HP Switch Software
Management and Configuration Guide

2615-8-PoE Switch
2915-8G-PoE Switch

Software version A.15.09
October 2012 Rev. B
© 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
5098-3647
October 2012 Rev. B

Applicable Products
HP 2615-8-PoE Switch J9565A
HP 2915-8G-PoE Switch J9562A

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.
Contents

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 ....................... 1-15
Menu: Viewing and Configuring TimeP ............................ 1-16
CLI: Viewing and Configuring TimeP ............................. 1-17
   Viewing the Current TimeP Configuration ..................... 1-18
   Configuring (Enabling or Disabling) the TimeP Mode ......... 1-19

SNTP Unicast Time Polling with Multiple SNTP Servers .......... 1-23
Displaying All SNTP Server Addresses Configured on the Switch . 1-23
Adding and Deleting SNTP Server Addresses ..................... 1-24
Menu: Operation with Multiple SNTP Server Addresses Configured .................................................. 1-24

SNTP Messages in the Event Log ...................................... 1-25

Port Status and Configuration

Viewing Port Status and Configuring Port Parameters .......... 2-1
   Menu: Port Status and Configuration ............................ 2-2
   Port Type ............................................................ 2-2
   Status of Ports ..................................................... 2-2
Flow Control .................................................. 2-3
Broadcast Limit .............................................. 2-3
Modes ............................................................... 2-3
Configuring Ports ............................................ 2-5
CLI: Viewing Port Status and Configuring Port Parameters ... 2-6
Viewing Port Status and Configuration .......................... 2-7
Viewing Port Utilization Statistics ................................. 2-9
Viewing Transceiver Status ...................................... 2-9
Enabling or Disabling Ports and Configuring Port Mode ........ 2-11
Enabling or Disabling Flow Control ............................... 2-12
Configuring Auto-MDIX ........................................... 2-14
Using Friendly (Optional) Port Names ............................. 2-17
Configuring and Operating Rules for Friendly Port Names ... 2-17
Configuring Friendly Port Names ................................ 2-18
Displaying Friendly Port Names with Other Port Data ........ 2-19
Uni-Directional Link Detection (UDLD) ......................... 2-22
Configuring UDLD ............................................... 2-24
Enabling UDLD .................................................. 2-25
Changing the Keepalive Interval ................................. 2-25
Changing the Keepalive Retries .................................. 2-26
Configuring UDLD for Tagged Ports .............................. 2-26
Viewing UDLD Information ........................................ 2-27
Configuration Warnings and Event Log Messages ............... 2-29

Power Over Ethernet (PoE+) Operation

Introduction to PoE+ .............................................. 3-1
Related Publications ............................................. 3-1
PoE Terminology .................................................. 3-2

PoE Operation ...................................................... 3-3
Configuration Options ........................................... 3-3
PD Support ......................................................... 3-4
Power Priority Operation ........................................ 3-5

Configuring PoE Operation ....................................... 3-5
Disabling or Re-Enabling PoE Port Operation .................... 3-6
Configuring the PoE Port Priority Level .............................................. 3-6
Enabling Support for Pre-Standard Devices ................................. 3-8
Controlling PoE Allocation .......................................................... 3-8
Manually Configuring PoE Power Levels ................................. 3-9
Changing the Threshold for Generating a Power Notice ........ 3-10
PoE with LLDP ................................................................. 3-11
  Overview ........................................................................... 3-11
  PoE Allocation ................................................................. 3-12
  Enabling Advertisement of Poe TLVs ................................. 3-13
  Displaying PoE When Using LLDP Information ............. 3-13
    Displaying LLDP Port Configuration ................................. 3-13
    Displaying Local Device Power Information ......................... 3-14
    Displaying Remote Power Information .............................. 3-14
Displaying the Global PoE Status ................................................. 3-17
  Displaying PoE Status on All Ports ........................................... 3-18
  Displaying the PoE Status on Specific Ports .................... 3-19
Planning and Implementing a PoE Configuration ....................... 3-22
  Assigning PoE Ports to VLANs ............................................. 3-22
  Applying Security Features to PoE Configurations .............. 3-22
  Assigning Priority Policies to PoE Traffic ................. 3-23
  PoE Event Log Messages .................................................. 3-23
    “Informational” PoE Event-Log Messages ...................... 3-23
    “Warning” PoE Event-Log Messages .............................. 3-24
Port Trunking
  Overview ........................................................................... 4-1
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
Trunk Group Operation Using LACP ............................................. 4-14
Default Port Operation ................................................. 4-17
LACP Notes and Restrictions ........................................... 4-18
Trunk Group Operation Using the “Trunk” Option .................. 4-22
How the Switch Lists Trunk Data ..................................... 4-22
Outbound Traffic Distribution Across Trunked Links ............... 4-23

Port Traffic Controls
Overview ................................................................. 5-1
Rate-Limiting ............................................................ 5-1
   All Traffic Rate-Limiting ........................................... 5-1
   Configuring Rate-Limiting ......................................... 5-2
   Displaying the Current Rate-Limit Configuration ............... 5-3
   Operating Notes for Rate-Limiting ............................... 5-4
   Configuring a Broadcast Limit on the Switch .................. 5-6
Jumbo Frames ............................................................. 5-7
   Terminology ......................................................... 5-7
   Operating Rules ..................................................... 5-8
   Configuring Jumbo Frame Operation ............................. 5-8
      Overview ......................................................... 5-9
      Viewing the Current Jumbo Configuration .................... 5-9
      Enabling or Disabling Jumbo Traffic on a VLAN ............... 5-11
   Configuring a Maximum Frame Size ............................. 5-11
      SNMP Implementation .......................................... 5-11
      Displaying the Maximum Frame Size ......................... 5-12
      Operating Notes for Maximum Frame Size .................... 5-12
      Operating Notes for Jumbo Traffic-Handling .................. 5-12
      Troubleshooting ............................................... 5-14

Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch ............................. 6-1
   SNMP Management Features ....................................... 6-2
   Configuring for SNMP version 1 and 2c Access to the Switch .... 6-2
   Configuring for SNMP Version 3 Access to the Switch ........... 6-3
   SNMP Version 3 Commands ........................................ 6-4
Enabling SNMPv3 .................................................. 6-5
SNMPv3 Users .................................................. 6-5
Group Access Levels ........................................... 6-9
SNMPv3 Communities ......................................... 6-9
Menu: Viewing and Configuring non-SNMP version 3 Communities ........................................... 6-11
CLI: Viewing and Configuring SNMP Community Names ........ 6-13
SNMP Notifications ............................................. 6-15
Supported Notifications ....................................... 6-15
General Steps for Configuring SNMP Notifications ............ 6-16
SNMPv1 and SNMPv2c Traps ..................................... 6-17
Configuring an SNMP Trap Receiver ........................... 6-17
Enabling SNMPv2c Informs ..................................... 6-19
Configuring SNMPv3 Notifications ............................ 6-20
Managing Network Security Notifications ..................... 6-24
Enabling Link-Change Traps .................................... 6-26
Configuring the Source IP Address for SNMP Notifications ... 6-27
Displaying SNMP Notification Configuration ................ 6-29
Advanced Management: RMON ................................ 6-31
CLI-Configured sFlow with Multiple Instances ................ 6-31
Terminology ...................................................... 6-31
Configuring sFlow ................................................ 6-32
Viewing sFlow Configuration and Status ....................... 6-32
LLDP (Link-Layer Discovery Protocol) .......................... 6-34
Terminology ...................................................... 6-36
General LLDP Operation ........................................ 6-37
LLDP-MED ......................................................... 6-38
Packet Boundaries in a Network Topology ...................... 6-38
Configuration Options ......................................... 6-38
Options for Reading LLDP Information Collected by the Switch ... 6-41
LLDP and LLDP-MED Standards Compatibility ................ 6-41
LLDP Operating Rules ........................................... 6-41
Configuring LLDP Operation ................................... 6-42
Viewing the Current Configuration ............................. 6-43
Configuring Global LLDP Packet Controls ..................... 6-45
Configuring SNMP Notification Support .............................. 6-49
Configuring Per-Port Transmit and Receive Modes .......... 6-50
Configuring Basic LLDP Per-Port Advertisement Content .... 6-51
Configuring Support for Port Speed and Duplex Advertisement .............................................. 6-53
LLDP-MED (Media-Endpoint-Discovery) ............................ 6-54
LLDP-MED Topology Change Notification ......................... 6-56
LLDP-MED Fast Start Control ........................................... 6-58
Advertising Device Capability, Network Policy, PoE Status and Location Data ................................. 6-58
Configuring Location Data for LLDP-MED Devices .......... 6-62
Displaying Advertisement Data ......................................... 6-67
Displaying Switch Information Available for Outbound Advertisement ................................................ 6-68
Displaying LLDP Statistics ................................................ 6-72
LLDP Operating Notes ...................................................... 6-74
LLDP and CDP Data Management ................................. 6-76
LLDP and CDP Neighbor Data ........................................... 6-76
CDP Operation and Commands ......................................... 6-78
MAC Limit Notification ..................................................... 6-82
Configuring the MAC Address Count Option .................. 6-82
Displaying Information About the mac-count-notify Option ................................. 6-82
MAC Address Table Change Notification ......................... 6-84
Configuring the MAC Address Table Change Option ....... 6-84
Additional mac-notify Options for Per-Port MAC Changes .... 6-85
Configuring the mac-notify Option at the Interface Context Level .................................................. 6-87
Displaying the mac-notify Traps Configuration Information ........................................... 6-87

File Transfers

Overview ................................................................. A-1

Downloading Switch Software ......................................... A-1
General Software Download Rules ................................ A-2
Using TFTP To Download Switch Software from a Server .... A-2
Menu: TFTP Download from a Server to Primary Flash .... A-3
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-11
Authentication .............................................. A-12
SCP/SFTP Operating Notes ................................. A-12
Troubleshooting SSH, SFTP, and SCP Operations .... A-14

Using Xmodem to Download Switch Software From a PC or UNIX Workstation ................................. A-15
  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-19

Using PCM+ to Update Switch Software .................. A-20

Copying Software Images ................................... A-21
  TFTP: Copying a Software Image to a Remote Host .... A-21
  Xmodem: Copying a Software Image from the Switch to a Serially Connected PC or UNIX Workstation ... A-21

Transferring Switch Configurations ....................... A-22
  TFTP: Copying a Configuration File to a Remote Host ... A-22
  TFTP: Copying a Configuration File from a Remote Host . A-23
  TFTP: Copying a Customized Command File to a Switch ... A-23
  Xmodem: Copying a Configuration File to a Serially Connected PC or UNIX Workstation ................. A-24
  Xmodem: Copying a Configuration File from a Serially Connected PC or UNIX Workstation ............... A-25

Transferring ACL Command Files .......................... A-26
  TFTP: Uploading an ACL Command File from a TFTP Server ... A-26
  Xmodem: Uploading an ACL Command File from a Serially Connected PC or UNIX Workstation .......... A-28

Copying Diagnostic Data to a Remote Host, PC or UNIX Workstation ................................. A-29
  Copying Command Output to a Destination Device ... A-29
Monitoring and Analyzing Switch Operation

Overview .................................................. B-1

Status and Counters Data ............................... B-1
  Menu Access To Status and Counters .............. B-3
  General System Information ......................... B-3
  Menu Access ........................................... B-3
  CLI Access to System Information ................. B-4

Task Monitor—Collecting Processor Data ........... B-5

Switch Management Address Information .......... B-6
  Menu Access ........................................... B-6
  CLI Access ............................................. B-7

Port Status ................................................ B-7
  Menu: Displaying Port Status ...................... B-7
  CLI Access ............................................. B-8

Viewing Port and Trunk Group Statistics and Flow Control Status . B-8
  Menu Access to Port and Trunk Statistics ........ B-9
  CLI Access to Port and Trunk Group Statistics .. B-10

Viewing the Switch's MAC Address Tables .......... B-11
  Menu Access to the MAC Address Views and Searches B-11
  CLI Access for MAC Address Views and Searches .. B-14

Spanning Tree Protocol (MSTP) Information ........ B-15
  CLI Access to MSTP Data ............................ B-15

Internet Group Management Protocol (IGMP) Status .... B-16

VLAN Information ........................................ B-16

Interface Monitoring Features ....................... B-18
  Menu: Configuring Port and Static Trunk Monitoring B-19
  CLI: Configuring Port and Static Trunk Monitoring B-21

Locating a Device ...................................... B-24
Troubleshooting

Overview ......................................................... C-1

Troubleshooting Approaches .................................. C-1

Browser or Telnet Access Problems .......................... C-2

Unusual Network Activity ................................. C-4

  General Problems ......................................... C-4
  802.1Q Prioritization Problems ......................... C-5
  ACL Problems ............................................. C-5
  IGMP-Related Problems .................................. C-10
  LACP-Related Problems .................................. C-10
  Port-Based Access Control (802.1X)-Related Problems  C-11
  QoS-Related Problems ................................... C-14
  Radius-Related Problems ................................ C-14
  Spanning-Tree Protocol (MSTP) and Fast-Uplink Problems  C-15
  SSH-Related Problems ................................ C-16
  TACACS-Related Problems ................................ C-17
  TimeP, SNTP, or Gateway Problems ...................... C-19
  VLAN-Related Problems ................................ C-20
  Fan Failure ................................................. C-23

Displaying Transceiver Information .......................... C-24

  CLI Support .............................................. C-25
  MIB Support ............................................ C-25
  Showing Transceiver Information ...................... C-25
    Information Displayed with the Detail Parameter . C-27
    Displaying Transceiver Information for Copper  
    Transceivers with VCT Support ..................... C-30
      Testing the Cable .................................. C-31
        Displaying Transceiver Information .......... C-31

Using the Event Log for Troubleshooting Switch Problems  ... C-34

  Event Log Entries ...................................... C-34
  Menu: Displaying and Navigating in the Event Log .... C-41
  CLI: Displaying the Event Log ........................ C-43
  CLI: Clearing Event Log Entries ..................... C-43
  CLI: Turning Event Numbering On or Off ............. C-44
Using Log Throttling to Reduce Duplicate Event Log and SNMP Messages ........................................ C-44
  Log Throttle Periods ........................................ C-45
  Example of Log Throttling ................................ C-45
  Example of Event Counter Operation .................. C-46
Reporting Information About Changes to the Running Configuration ................................................. C-47

Debug/Syslog Operation ........................................ C-48
  Debug/Syslog Messaging .................................... C-48
  Debug/Syslog Destination Devices ...................... C-48
  Debug/Syslog Configuration Commands ................. C-49
Configuring Debug/Syslog Operation ....................... C-50
  Displaying a Debug/Syslog Configuration .............. C-52
Debug Command ............................................... C-55
  Debug Messages ........................................... C-55
  Debug Destinations ....................................... C-58
Logging Command ............................................ C-59
  Configuring a Syslog Server ............................. C-60
Adding a Priority Description ............................. C-62
Configuring the Severity Level for Event Log Messages Sent to a Syslog Server ................................. C-63
  Configuring the System Module Used to Select the Event Log Messages Sent to a Syslog Server .......... C-64
Operating Notes for Debug and Syslog ..................... C-65

Diagnostic Tools .............................................. C-66
  Port Auto-Negotiation ..................................... C-66
  Ping and Link Tests ....................................... C-67
    CLI: Ping Test ........................................... C-67
    Link Tests ............................................... C-69
  Traceroute Command ...................................... C-69

Viewing Switch Configuration and Operation ................ C-73
  CLI: Viewing the Startup or Running Configuration File ............................................. C-73
  CLI: Viewing a Summary of Switch Operational Data ....................................................... C-73
  Saving show tech Command Output to a Text File ............................................................ C-74
  Customizing show tech Command Output ................. C-76
  CLI: Viewing More Information on Switch Operation ....................................................... C-79
Pattern Matching When Using the Show Command ............. C-79
CLI: Useful Commands for Troubleshooting Sessions ............. C-83
Restoring the Factory-Default Configuration .................. C-84
   CLI: Resetting to the Factory-Default Configuration .......... C-84
   Clear/Reset: Resetting to the Factory-Default Configuration .... C-84
Restoring a Flash Image .......................................... C-85
DNS Resolver .......................................................... C-87
   Terminology ....................................................... C-87
   Basic Operation .................................................. C-88
   Configuring and Using DNS Resolution
      with DNS-Compatible Commands .............................. C-90
   Configuring a DNS Entry ....................................... C-90
   Example Using DNS Names with Ping and Traceroute ........ C-92
   Viewing the Current DNS Configuration ...................... C-94
   Operating Notes .................................................. C-94
   Event Log Messages ............................................. C-95

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

Monitoring Resources

Viewing Information on Resource Usage ......................... E-1
   Policy Enforcement Engine ...................................... E-1
   Displaying Current Resource Usage ............................. E-2

When Insufficient Resources Are Available ..................... E-4

Daylight Savings Time on HP Switches

Power-Saving Features

Configuring Power-Saving ......................................... G-1
Index
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
Time Protocols
Selecting a Time Synchronization Protocol or Turning Off Time Protocol Operation

network broadcast address. Refer to the documentation provided with your SNTP server application.) Once the switch detects a particular 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

<table>
<thead>
<tr>
<th>SNTP Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view the SNTP time synchronization configuration</td>
<td>n/a</td>
<td>page 1-4</td>
<td>page 1-7</td>
<td></td>
</tr>
<tr>
<td>select SNTP as the time synchronization method</td>
<td>timep</td>
<td>page 1-5</td>
<td>page 1-9 ff.</td>
<td></td>
</tr>
<tr>
<td>disable time synchronization</td>
<td>timep</td>
<td>page 1-5</td>
<td>page 1-13</td>
<td></td>
</tr>
<tr>
<td>enable the SNTP mode (Broadcast, Unicast, or Disabled)</td>
<td>disabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>broadcast</td>
<td>n/a</td>
<td>page 1-5</td>
<td>page 1-10</td>
<td></td>
</tr>
<tr>
<td>unicast</td>
<td>n/a</td>
<td>page 1-5</td>
<td>page 1-11</td>
<td></td>
</tr>
<tr>
<td>none/disabled</td>
<td>n/a</td>
<td>page 1-5</td>
<td>page 1-14</td>
<td></td>
</tr>
<tr>
<td>configure an SNTP server address (for Unicast mode only)</td>
<td>none</td>
<td>page 1-5</td>
<td>page 1-11 ff.</td>
<td></td>
</tr>
<tr>
<td>change the SNTP server version (for Unicast mode only)</td>
<td>3</td>
<td>page 1-6</td>
<td>page 1-12</td>
<td></td>
</tr>
<tr>
<td>change the SNTP poll interval</td>
<td>720 seconds</td>
<td>page 1-6</td>
<td>page 1-13</td>
<td></td>
</tr>
<tr>
<td>change the server priority</td>
<td>n/a</td>
<td>—</td>
<td>page 1-11</td>
<td></td>
</tr>
</tbody>
</table>
Time Protocols
SNTP: Viewing, Selecting, and Configuring

Table 1-1. SNTP Parameters

<table>
<thead>
<tr>
<th>SNTP Parameter</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Sync Method</td>
<td>Used to select either SNTP, TIMEP, or None as the time synchronization method.</td>
</tr>
<tr>
<td>SNTP Mode</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td>The Default. SNTP does not operate, even if specified by the Menu interface Time Sync Method parameter or the CLI timesync command.</td>
</tr>
<tr>
<td>Unicast</td>
<td>Directs the switch to poll a specific server for SNTP time synchronization. Requires at least one server address.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>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.</td>
</tr>
<tr>
<td>Poll Interval (seconds)</td>
<td>In Unicast Mode: Specifies how often the switch polls the designated SNTP server for a time update. In Broadcast Mode: Specifies how often the switch polls the network broadcast address for a time update. Value between 30-720 seconds.</td>
</tr>
<tr>
<td>Server Address</td>
<td>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 1-23.</td>
</tr>
<tr>
<td>Server Version</td>
<td>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.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the order in which the configured servers are polled for getting the time. Value is between 1 and 3.</td>
</tr>
</tbody>
</table>

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
Time Protocols
SNTP: Viewing, Selecting, and Configuring

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.)

   ![Time Configuration Fields for SNTP with Broadcast Mode](image)

   - 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.

   ![Time Configuration Fields for SNTP with Broadcast Mode](image)
**Time Protocols**

**SNTP: Viewing, Selecting, and Configuring**

*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 1-23.

iii. Press \[v\] 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 1-23.

iv. Press \[>\] to move the cursor to the **Poll Interval** field, then go to step 6.

---

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Sync Method</td>
<td>SNTP</td>
</tr>
<tr>
<td>SNTP Mode</td>
<td>Unicast</td>
</tr>
<tr>
<td>Poll Interval (sec)</td>
<td>720</td>
</tr>
<tr>
<td>Tftp-enable</td>
<td>Yes</td>
</tr>
<tr>
<td>Time Zone</td>
<td>0</td>
</tr>
<tr>
<td>Daylight Time Rule</td>
<td>None</td>
</tr>
</tbody>
</table>

*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 1-23.

---

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

<table>
<thead>
<tr>
<th>SNTP Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snntp</td>
<td>1-7</td>
</tr>
<tr>
<td>[no] timesync</td>
<td>1-9 and ff., 1-13</td>
</tr>
<tr>
<td>snntp broadcast</td>
<td>1-10</td>
</tr>
<tr>
<td>snntp unicast</td>
<td>1-11</td>
</tr>
<tr>
<td>snntp server</td>
<td>1-11 and ff.</td>
</tr>
<tr>
<td>Protocol Version</td>
<td>1-9, 1-11</td>
</tr>
<tr>
<td>Priority</td>
<td>1-9, 1-11</td>
</tr>
<tr>
<td>poll-interval</td>
<td>1-13</td>
</tr>
<tr>
<td>no snntp</td>
<td>1-14</td>
</tr>
</tbody>
</table>

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

Viewing the Current SNTP Configuration

**Syntax: show snntp**

>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 snntp lists the following:
**Time Protocols**

SNTP: Viewing, Selecting, and Configuring

---

**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

<table>
<thead>
<tr>
<th>Priority</th>
<th>SNTP Server Address</th>
<th>Protocol Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2001:db8::215:60ff:fe79:8980</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>10.255.5.24</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>fe80::123%vlan10</td>
<td>3</td>
</tr>
</tbody>
</table>
```

---

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

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

```
HP Switch(config)# show sntp

SNTP Configuration

<table>
<thead>
<tr>
<th>Priority</th>
<th>SNTP Server Address</th>
<th>Protocol Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2001:db8::215:60ff:fe79:8980</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>10.255.5.24</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>fe80::123%vlan10</td>
<td>3</td>
</tr>
</tbody>
</table>
```

---

**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.
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 1-13).
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:

```plaintext
HP Switch(config)# show sntp
SNTP Configuration
  Time Sync Mode: TimeP
  SNTP Mode : disabled
  Poll Interval (sec) [720] : 720

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

5406_1(config)# show sntp
SNTP Configuration
  Time Sync Mode: Sntp
  SNTP Mode : Broadcast
  Poll Interval (sec) [720] : 720
```

**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 1-23.

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).
```
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
```

`show sntp` displays the changed server protocol version.

See also: If the poll interval command is not specified, the default poll interval is 720 seconds.

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

---

**Time Protocols**

SNTP: Viewing, Selecting, and Configuring

---

**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
```

`show sntp` displays the changed server protocol version.

---

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

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

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

<table>
<thead>
<tr>
<th>Priority</th>
<th>SNTP Server Address</th>
<th>Protocol Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2001:db8::215:60ff:fe79:8980</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>10.28.227.141</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>fe80::123%vlan10</td>
<td>3</td>
</tr>
</tbody>
</table>

---

Note: Protocol Version appears only when there is an IP address configured for an SNTP server.
Time Protocols
SNTP: Viewing, Selecting, and Configuring

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 inter-
val 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 synchroniza-
tion 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 Synchronization 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

<table>
<thead>
<tr>
<th>Priority</th>
<th>SNTP Server Address</th>
<th>Protocol Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2001:db8::215:60ff:fe79:8980</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>10.28.227.141</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>fe80::123%vlan10</td>
<td>3</td>
</tr>
</tbody>
</table>
```

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

Figure 1-11. Example of Disabling Time Synchronization by Disabling the SNTP Mode
TimeP: Viewing, Selecting, and Configuring

<table>
<thead>
<tr>
<th>TimeP Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view the TimeP time synchronization configuration</td>
<td>n/a</td>
<td>page 1-16</td>
<td>page 1-18</td>
<td>—</td>
</tr>
<tr>
<td>select TimeP as the time synchronization method</td>
<td>TIMEP</td>
<td>page 1-14</td>
<td>pages 1-20 ff.</td>
<td>—</td>
</tr>
<tr>
<td>disable time synchronization</td>
<td>timep</td>
<td>page 1-16</td>
<td>page 1-22</td>
<td>—</td>
</tr>
<tr>
<td>enable the TimeP mode</td>
<td>Disabled</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>DHCP</td>
<td>—</td>
<td>page 1-16</td>
<td>page 1-20</td>
<td>—</td>
</tr>
<tr>
<td>manual</td>
<td>—</td>
<td>page 1-16</td>
<td>page 1-21</td>
<td>—</td>
</tr>
<tr>
<td>none/disabled</td>
<td>—</td>
<td>page 1-16</td>
<td>page 1-22</td>
<td>—</td>
</tr>
<tr>
<td>change the SNTP poll interval</td>
<td>720 minutes</td>
<td>page 1-17</td>
<td>page 1-21</td>
<td>—</td>
</tr>
</tbody>
</table>

Table 1-2. TimeP Parameters

<table>
<thead>
<tr>
<th>SNTP Parameter</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Sync Method</td>
<td>Used to select either TIMEP (the default), SNTP, or None as the time synchronization method.</td>
</tr>
<tr>
<td>Timep Mode</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td>The Default. Timep does not operate, even if specified by the Menu interface Time Sync Method parameter or the CLI timesync command.</td>
</tr>
<tr>
<td>DHCP</td>
<td>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.</td>
</tr>
<tr>
<td>Manual</td>
<td>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.</td>
</tr>
<tr>
<td>Server Address</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

--- CONSOLE - MANAGER MODE ---

Switch Configuration - System Information

System Name : HPNetworking
System Contact :
System Location :

Inactivity Timeout (min) [0] : 0      MAC Age Time (sec) [300] : 300
Time Sync Method [None] : TIMEP
TimeP Mode [Disabled] : Disabled
Tftp-enable [Yes] : Yes
Time Zone [0] : 0
Daylight Time Rule [None] : None

Time Protocol Selection Parameter
  – TIMEP (the default)
  – SNTP
  – None

Actions->   Cancel     Edit     Save     Help

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.

   • Use the Space bar to select the Manual mode.
     i. Press [→] to move the cursor to the Server Address field.
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.

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, then [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

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show timep</td>
<td>1-18</td>
</tr>
<tr>
<td>[no] timesync</td>
<td>1-19 ff., 1-22</td>
</tr>
<tr>
<td>ip timep</td>
<td>1-19 ff., 1-22</td>
</tr>
<tr>
<td>dhcp</td>
<td>1-20</td>
</tr>
<tr>
<td>manual</td>
<td>1-21</td>
</tr>
<tr>
<td>server &lt;ip-addr&gt;</td>
<td>1-21</td>
</tr>
<tr>
<td>interval</td>
<td>1-21</td>
</tr>
<tr>
<td>no ip timep</td>
<td>1-22</td>
</tr>
</tbody>
</table>

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

**TimeP: Viewing, Selecting, and Configuring**

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] : Disabled
 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
 Server Address : 10.10.28.100
 Poll Interval (min) [720] : 720
```

**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.*
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
Timep Configuration
 Time Sync Mode: Sntp
 TimeP Mode [Disabled] : Disabled

HP Switch(config)# timesync timep
HP Switch(config)# ip timep dhcp
HP Switch(config)# show timep

Timep Configuration
 Time Sync Mode: Timep
 TimeP Mode [Disabled] : DHCP
 Server Address : 
 Poll Interval (min) [720] : 720
```

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 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.
```

```
Timep Configuration
Time Sync Mode: Timep
TimeP Mode [Disabled] : DHCP
Server Address : 10.28.227.141
Poll Interval (min) [720] : 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:

\[ \text{HP Switch(config)} \# \text{ip timep interval 60} \]

**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:

\[ \text{HP Switch(config)} \# \text{no timesync} \]

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 [Disabled] : DHCP
Poll Interval (min) [720] : 720
```

**Figure 1-18. Example of TimeP with Time Synchronization 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] : Disabled
```

**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

<table>
<thead>
<tr>
<th>Priority</th>
<th>SNTP Server Address</th>
<th>Protocol Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2001:db8::215:60ff:fe79:8980</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>10.255.5.24</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>fe80::123%vlan10</td>
<td>3</td>
</tr>
</tbody>
</table>

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.
Time Protocols

SNTP Messages in the Event Log
Port Status and Configuration

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
- Friendly Port Names
- Uni-directional Link Detection (UDLD)

Viewing Port Status and Configuring Port Parameters

Port Status and Configuration Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>viewing port status</td>
<td>n/a</td>
<td>page 2-2</td>
<td>page 2-6</td>
</tr>
<tr>
<td>viewing transceiver status</td>
<td>n/a</td>
<td>n/a</td>
<td>page 2-9</td>
</tr>
<tr>
<td>configuring ports</td>
<td></td>
<td>page 2-5</td>
<td>page 2-11</td>
</tr>
<tr>
<td>configuring HP auto-mdix</td>
<td></td>
<td></td>
<td>page 2-14</td>
</tr>
</tbody>
</table>

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 2-10).
Port Status and Configuration
Viewing Port Status and Configuring Port Parameters

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
3. Port Status

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Intrusion</th>
<th>Alert</th>
<th>Enabled</th>
<th>Status</th>
<th>Mode</th>
<th>MDI Mode</th>
<th>Ctrl</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>100FDx</td>
<td>Auto off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
Port Status and Configuration

Viewing Port Status and Configuring Port Parameters

- **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 traffic. Any broadcast 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 (data transfer operation) setting. Table 2-1 shows possible modes available, depending on the port type (copper or fiber) and port speed.
**Port Status and Configuration**
Viewing Port Status and Configuring Port Parameters

### Table 2-1. Supported Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Speed and Duplex Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-MDIX</td>
<td>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 <code>show interfaces brief</code> command or the menu commands &quot;1. Status and Counters&quot;, &quot;3. Port Status&quot;. This feature applies only to copper port switches using twisted-pair copper Ethernet cables.</td>
</tr>
<tr>
<td>MDI</td>
<td>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).</td>
</tr>
<tr>
<td>MDIX</td>
<td>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).</td>
</tr>
<tr>
<td>Auto-10</td>
<td>Allows the port to negotiate between half-duplex (HDx) and full-duplex (FDx) while keeping speed at 10 Mbps. 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.)</td>
</tr>
<tr>
<td>Auto-100</td>
<td>Uses 100 Mbps and negotiates with the port at the other end of the link for other port operation features.</td>
</tr>
<tr>
<td>Auto-10-100</td>
<td>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.</td>
</tr>
<tr>
<td>Auto-1000</td>
<td>Uses 1000 Mbps and negotiates with the port at the other end of the link for other port operation features.</td>
</tr>
<tr>
<td>10HDx</td>
<td>Uses 10 Mbps, Half-Duplex</td>
</tr>
<tr>
<td>100HDx</td>
<td>Uses 100 Mbps, Half-Duplex</td>
</tr>
<tr>
<td>10FDX</td>
<td>Uses 10 Mbps, Full-Duplex</td>
</tr>
<tr>
<td>100FDx</td>
<td>Uses 100 Mbps, Full-Duplex</td>
</tr>
<tr>
<td>1000FDx</td>
<td>Uses 1000 Mbps, Full-Duplex</td>
</tr>
<tr>
<td>10 GbE FDx</td>
<td>Uses 10 Gigabits/sec Full-Duplex</td>
</tr>
</tbody>
</table>

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

Viewing Port Status and Configuring Port Parameters

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

<table>
<thead>
<tr>
<th>10/100 Mbps</th>
<th>Gigabit</th>
<th>10 Gigabit</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/100 TX</td>
<td>10/100/1000-T</td>
<td>10GBASE-CX4</td>
</tr>
<tr>
<td>Modes</td>
<td>Settings</td>
<td>Modes</td>
</tr>
<tr>
<td>Auto</td>
<td>100FDx</td>
<td>Auto</td>
</tr>
<tr>
<td>10HDx</td>
<td>10HDx</td>
<td>Auto-10</td>
</tr>
<tr>
<td>100HDx</td>
<td>100HDx</td>
<td>Auto-100</td>
</tr>
<tr>
<td>10FDx</td>
<td>10FDx</td>
<td>Auto-1000</td>
</tr>
<tr>
<td>100FDx</td>
<td>100FDX</td>
<td>10HDx</td>
</tr>
<tr>
<td>Auto-10</td>
<td>10FDX</td>
<td>100HDx</td>
</tr>
<tr>
<td></td>
<td>1000FDx</td>
<td>1000FDx</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>100 Mbps</th>
<th>Gigabit</th>
<th>10 Gigabit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>10BASE-FX</td>
<td>1000BASE-SX</td>
</tr>
<tr>
<td></td>
<td>10BASE-BX10</td>
<td>1000BASE-LX</td>
</tr>
<tr>
<td>Modes</td>
<td>100HDx</td>
<td>Auto</td>
</tr>
<tr>
<td></td>
<td>100FDx</td>
<td>1000FDx</td>
</tr>
</tbody>
</table>

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.
Port Status and Configuration
Viewing Port Status and Configuring Port Parameters

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces brief</td>
<td>2-7</td>
</tr>
<tr>
<td>show interfaces config</td>
<td>2-7</td>
</tr>
<tr>
<td>show interfaces port-utilization</td>
<td>2-9</td>
</tr>
<tr>
<td>show tech transceivers</td>
<td>2-9</td>
</tr>
<tr>
<td>interface</td>
<td>2-11</td>
</tr>
<tr>
<td>disable/enable</td>
<td>2-11</td>
</tr>
<tr>
<td>speed-duplex</td>
<td>2-11</td>
</tr>
<tr>
<td>flow-control</td>
<td>2-12</td>
</tr>
<tr>
<td>auto-mdix</td>
<td>2-14</td>
</tr>
</tbody>
</table>
Port Status and Configuration

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
<table>
<thead>
<tr>
<th>Intrusion</th>
<th>MDI</th>
<th>Flow</th>
<th>Bcast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>Alert</td>
<td>Enabled</td>
<td>Status</td>
</tr>
<tr>
<td>---------------</td>
<td>-------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>1 100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
</tr>
<tr>
<td>2 100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
</tr>
<tr>
<td>3 100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
</tr>
<tr>
<td>4 100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
</tr>
<tr>
<td>5 100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
</tr>
<tr>
<td>6 100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
</tr>
</tbody>
</table>
```

**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
<table>
<thead>
<tr>
<th>Enabled Mode</th>
<th>Flow Ctrl MDI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>1 100/1000T</td>
<td>Yes</td>
</tr>
<tr>
<td>2 100/1000T</td>
<td>Yes</td>
</tr>
<tr>
<td>3 100/1000T</td>
<td>Yes</td>
</tr>
<tr>
<td>4 100/1000T</td>
<td>Yes</td>
</tr>
<tr>
<td>5 100/1000T</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Figure 2-4. Example of a show interfaces config Command Listing**
Port Status and Configuration
Viewing Port Status and Configuring Port Parameters

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
```

```
Status and Counters - Port Counters

<table>
<thead>
<tr>
<th>Port</th>
<th>Total Bytes</th>
<th>Total Frames</th>
<th>Errors Rx</th>
<th>Drops Tx</th>
<th>Flow Ctrl</th>
<th>Bca* Lim*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2,154,277</td>
<td>20,366</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Actions: Back | Show details | Reset | Help

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

Figure 2-5. Example of show int display Command with Dynamically Updating Output
Port Status and Configuration

Viewing Port Status and Configuring Port Parameters

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

Port Mode | Rx | Tx
|------- |----|-----|
|        | Kbits/sec | Pkts/sec | Util | Kbits/sec | Pkts/sec | Util
|------- |----------|----------|------|----------|----------|------|
| 1      | 0        | 0        | 0    | 0        | 0        | 0
| 2      | 0        | 0        | 0    | 0        | 0        | 0
| 3      | 0        | 0        | 0    | 0        | 0        | 0
| 4      | 0        | 0        | 0    | 0        | 0        | 0
| 5      | 0        | 0        | 0    | 0        | 0        | 0
| 6      | 0        | 0        | 0    | 0        | 0        | 0
| 7      | 624      | 86       | 0.62 | 496      | 0        | 0.49
```

Figure 2-6. 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.
Port Status and Configuration
Viewing Port Status and Configuring Port Parameters

- Display real-time status information about all installed transceivers, including non-operational transceivers.

Figure 2-7 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|
23     | ??      | ??     | non operational |      |

The following transceivers may not function correctly:
Port # | Message
-------|--------
23     | Self test failure.
```

Figure 2-7. 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 2-7), 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.
Port Status and Configuration
Viewing Port Status and Configuring Port Parameters

- Transceiver type not supported in this port.
- Transceiver type not supported in this software version.
- Not a 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
auto10 auto100 auto1000 auto100 >]
```

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.
Port Status and Configuration
Viewing Port Status and Configuring Port Parameters

Figure 2-8. Examples of Two Methods for Changing a Port Configuration

Refer to “Enabling or Disabling Flow Control” on page 2-12 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:
Port Status and Configuration
Viewing Port Status and Configuring Port Parameters

```
HP Switch(config)# int 7-11 flow-control
HP Switch(config)# show int brief

Status and Counters - Port Status

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Alert</th>
<th>Enabled</th>
<th>Status</th>
<th>Mode</th>
<th>MDI Mode</th>
<th>Flow Ctrl</th>
<th>Bcast Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>on</td>
<td>0</td>
</tr>
<tr>
<td>7-Trk1</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>on</td>
<td>0</td>
</tr>
<tr>
<td>8-Trk1</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>on</td>
<td>0</td>
</tr>
<tr>
<td>9-Trk2</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>on</td>
<td>0</td>
</tr>
<tr>
<td>10-Trk2</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>on</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
</tbody>
</table>

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

Status and Counters - Port Status

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Alert</th>
<th>Enabled</th>
<th>Status</th>
<th>Mode</th>
<th>MDI Mode</th>
<th>Flow Ctrl</th>
<th>Bcast Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Down</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>on</td>
<td>0</td>
</tr>
<tr>
<td>7-Trk1</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>on</td>
<td>0</td>
</tr>
<tr>
<td>8-Trk1</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>on</td>
<td>0</td>
</tr>
<tr>
<td>9-Trk2</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>on</td>
<td>0</td>
</tr>
<tr>
<td>10-Trk2</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>on</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>100/1000T</td>
<td>No</td>
<td>Yes</td>
<td>Up</td>
<td>1000FDx</td>
<td>Auto</td>
<td>off</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 2-9. Example of Configuring Flow Control for a Series of Ports

Disables per-port flow control on port 11.

Figure 2-10. Example Continued from Figure 2-9
Port Status and Configuration
Viewing Port Status and Configuring Port Parameters

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 “cross-over” 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.

---

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

<table>
<thead>
<tr>
<th>Status and Counters - Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7-Trk1</td>
</tr>
<tr>
<td>8-Trk1</td>
</tr>
<tr>
<td>9-Trk2</td>
</tr>
<tr>
<td>10-Trk2</td>
</tr>
<tr>
<td>11</td>
</tr>
</tbody>
</table>
Port Status and Configuration

Viewing Port Status and Configuring Port Parameters

- 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 2-4 shows the cabling requirements for the MDI/MDI-X settings.

### Table 2-4: Cable Types for Auto and Manual MDI/MDI-X Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>PC or Other MDI Device Type</th>
<th>Switch, Hub, or Other MDI-X Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual MDI</td>
<td>Crossover Cable</td>
<td>Straight-Through Cable</td>
</tr>
<tr>
<td>Manual MDI-X</td>
<td>Straight-Through Cable</td>
<td>Crossover Cable</td>
</tr>
<tr>
<td>Auto-MDI-X (The Default)</td>
<td>Either Crossover or Straight-Through Cable</td>
<td></td>
</tr>
</tbody>
</table>

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

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

`auto-mdix` 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.
Port Status and Configuration
Viewing Port Status and Configuring Port Parameters

**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* (**auto-mdix**), 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

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Enabled</th>
<th>Mode</th>
<th>Flow Ctrl</th>
<th>MDI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100/1000T</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td>Auto</td>
</tr>
<tr>
<td>2</td>
<td>100/1000T</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td>MDI</td>
</tr>
<tr>
<td>3</td>
<td>100/1000T</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td>MDIX</td>
</tr>
<tr>
<td>4</td>
<td>100/1000T</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td>Auto</td>
</tr>
<tr>
<td>5</td>
<td>100/1000T</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td>Auto</td>
</tr>
<tr>
<td>6</td>
<td>100/1000T</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td>Auto</td>
</tr>
</tbody>
</table>
```

**Figure 2-12. Example of Displaying the Current MDI Configuration**
Port Status and Configuration
Using Friendly (Optional) Port Names

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 2-19.)
Port Status and Configuration
Using Friendly (Optional) Port Names

- 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, not assigned 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 3 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 3:

```
HP Switch(config)# int 3 name Bill_Smith@10.25.101.73
HP Switch(config)# write mem
HP Switch(config)# show name 3
Port Names

Port : 3
    Type : 100/1000T
    Name : Bill_Smith@10.25.101.73
```

Figure 2-14. Example of Configuring a Friendly Port Name
Configuring the Same Name for Multiple Ports. Suppose that you want to use ports 5 through 8 as a trunked link to a server used by a drafting group. In this case you might configure ports 5 through 8 with the name “Draft-Server:Trunk”.

```
HP Switch(config)# int 5-8 name Draft-Server:Trunk
HP Switch(config)# write mem
HP Switch(config)# show name 5-8
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>6</td>
<td>100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>7</td>
<td>100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>8</td>
<td>100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
</tbody>
</table>

Figure 2-15. 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.
Port Status and Configuration
Using Friendly (Optional) Port Names

**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
<table>
<thead>
<tr>
<th>Port Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 100/1000T</td>
<td>not assigned</td>
</tr>
<tr>
<td>2 100/1000T</td>
<td>not assigned</td>
</tr>
<tr>
<td>3 100/1000T</td>
<td>Bill_Smith@10.25.101.73</td>
</tr>
<tr>
<td>4 100/1000T</td>
<td>not assigned</td>
</tr>
<tr>
<td>5 100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>6 100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>7 100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>8 100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>9 100/1000T</td>
<td>not assigned</td>
</tr>
<tr>
<td>10 100/1000T</td>
<td>not assigned</td>
</tr>
</tbody>
</table>
```

**Figure 2-16. Example of Friendly Port Name Data for All Ports on the Switch**

```
HP Switch(config)# show name
Port Names
<table>
<thead>
<tr>
<th>Port Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 100/1000T</td>
<td>not assigned</td>
</tr>
<tr>
<td>2 100/1000T</td>
<td>not assigned</td>
</tr>
<tr>
<td>3 100/1000T</td>
<td>Bill_Smith@10.25.101.73</td>
</tr>
<tr>
<td>4 100/1000T</td>
<td>not assigned</td>
</tr>
<tr>
<td>5 100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>6 100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>7 100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>8 100/1000T</td>
<td>Draft-Server:Trunk</td>
</tr>
<tr>
<td>9 100/1000T</td>
<td>not assigned</td>
</tr>
<tr>
<td>10 100/1000T</td>
<td>not assigned</td>
</tr>
</tbody>
</table>
```

**Figure 2-17. 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.
Port Status and Configuration
Using Friendly (Optional) Port Names

Syntax: show interface < port-number >

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

For example, if you configure port 1 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 1
Status and Counters - Port Counters for port 5

Name: O’Connor@10.25.101.43
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
Runt 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 2-18. 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 as:

```
Name: not assigned
```

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.)
Port Status and Configuration

Uni-Directional Link Detection (UDLD)

**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 ports with a friendly port name:

```
HP Switch(config)# int 6 name Print_Server
HP Switch(config)# write mem
HP Switch(config)# int 7 name Herbert_PC
Switch(config)#
HP Switch(config)# show config

Startup configuration:

; J9562A Configuration Editor; Created on release #A.15.XX

hostname "Switch 2520G-24-PoE"
savepower led
interface 6
   name "Print_Server"
exit
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address dhcp-bootp
exit
```

This command sequence saves the friendly port name for port 6 in the startup-config file. The name entered for port 7 is not saved because it was executed after write memory.

In this case, show config lists only port 6. Executing write mem after entering the name for port 7, and then executing show config again would result in a listing that includes both ports.

Listing includes friendly port name for port 6 only.

Figure 2-19. Example Listing of the Startup-Config File with a Friendly Port Name Configured (and Saved)

---

**Uni-Directional Link Detection (UDLD)**

Uni-directional Link Detection (UDLD) monitors a link between two HP 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 2-20 shows an 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 continues 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 unidirectional 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.
Port Status and Configuration
Uni-Directional Link Detection (UDLD)

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 switch series: 2600, 2800, 2900, 2910, 3400, 3500, 4200, 5300, 5400, 6200, 6400, 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)
Port Status and Configuration
Uni-Directional Link Detection (UDLD)

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 1, enter:

```
HP Switch(config)#interface 1 link-keepalive
```

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

```
HP Switch(config)#interface 1-4 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
```
Port Status and Configuration
Uni-Directional Link Detection (UDLD)

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 29 for potential problems).
Port Status and Configuration

Uni-Directional Link Detection (UDLD)

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

*Cleans 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
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Physical</th>
<th>Keepalive Status</th>
<th>Adjacent Switch</th>
<th>UDLD VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>up</td>
<td>up</td>
<td>00d9d-f9b700</td>
<td>200</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>up</td>
<td>up</td>
<td>01560-7b1600</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>down</td>
<td>off-line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Yes</td>
<td>up</td>
<td>failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>No</td>
<td>down</td>
<td>off-line</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 2-21. Example of Show Link-Keepalive Command

To display detailed UDLD information for specific ports, enter the `show link-keepalive statistics` command.
Port Status and Configuration
Uni-Directional Link Detection (UDLD)

Figure 2-22. 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 2-22 for an example).
Configuration Warnings and Event Log Messages

Warning Messages. The following table shows the warning messages that may be issued and their possible causes, when UDLD is configured for tagged ports.

<table>
<thead>
<tr>
<th>CLI Command Example</th>
<th>Warning Message</th>
<th>Possible Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-keepalive 6</td>
<td>Possible configuration problem detected on port 6. UDLD VLAN configuration does not match the port's VLAN configuration.</td>
<td>You have attempted to enable UDLD on a port that is a tagged only port, but did not specify a configuration for tagged UDLD control packets. In this example, the switch will send and receive the UDLD control packets untagged despite issuing this warning.</td>
</tr>
<tr>
<td>link-keepalive 7</td>
<td>Possible configuration problem detected on port 7. UDLD VLAN configuration does not match the port's VLAN configuration.</td>
<td>You have attempted to configure tagged UDLD packets on a port that does not belong to the specified VLAN. In this example, if port 7 belongs to VLAN 1 and 22, but the user tries to configure UDLD on port 7 to send tagged packets in VLAN 4, the configuration will be accepted. The UDLD control packets will be sent tagged in VLAN 4, which may result in the port being blocked by UDLD if the user does not configure VLAN 4 on this port.</td>
</tr>
<tr>
<td>no vlan 22 tagged 20</td>
<td>Possible configuration problem detected on port 18. UDLD VLAN configuration does not match the port's VLAN configuration.</td>
<td>You have attempted to remove a VLAN on port that is configured for tagged UDLD packets on that VLAN. In this example, if port 18, 19, and 20 are transmitting and receiving tagged UDLD packets for VLAN 22, but the user tries to remove VLAN 22 on port 20, the configuration will be accepted. In this case, the UDLD packets will still be sent on VLAN 20, which may result in the port being blocked by UDLD if the users do not change the UDLD configuration on this port.</td>
</tr>
</tbody>
</table>

Note: If you are configuring the switch via SNMP with the same problematic VLAN configuration choices, the above warning messages will also be logged in the switch's event log.

Event Log Messages. The following table shows the event log messages that may be generated once UDLD has been enabled on a port.

<table>
<thead>
<tr>
<th>Message</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>I 01/01/06 04:25:05 ports: port 4 is deactivated due to link failure.</td>
<td>A UDLD-enabled port has been blocked due to part of the link having failed.</td>
</tr>
<tr>
<td>I 01/01/06 06:00:43 ports: port 4 is up, link status is good.</td>
<td>A failed link has been repaired and the UDLD-enabled port is no longer blocked.</td>
</tr>
</tbody>
</table>
Port Status and Configuration
Uni-Directional Link Detection (UDLD)
Power Over Ethernet (PoE+) Operation

Introduction to PoE+

PoE technology allows IP telephones, wireless LAN access points, and other appliances to receive power and transfer data over ethernet LAN cabling. Using an available power supply of 382 watts, PoE can deliver up to 15.4 watts of power to 24 PoE ports over category 3 cabling. PoE+ can deliver up to 30 watts of power to 12 PoE+ ports over category 5 cabling. PoE+ also supports delivery of PoE power concurrently with 10/100/1000 Gbps of data transmission.

Additionally, PoE+ provides more power-management capability, allowing the switch to have more power available for more PDs. Power can be allocated exactly and automatically according to what the PD actually requires at a given time.

Related Publications

This chapter introduces general PoE operation, PoE configuration and monitoring commands, and Event Log messages related to PoE operation.

To help you plan and implement a PoE system in your network, refer to the PoE Planning and Implementation Guide, which is available on the HP Networking web site at www.HP.com/networking.

The latest version of any HP product guide is always on the HP Networking web site.
**Power Over Ethernet (PoE+) Operation**

**Introduction to PoE+**

---

### PoE Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Use in this Manual</th>
</tr>
</thead>
<tbody>
<tr>
<td>active PoE port</td>
<td>A PoE port connected to a PD requesting power.</td>
</tr>
<tr>
<td>DTE</td>
<td>Data Terminal Equipment</td>
</tr>
<tr>
<td>MPS</td>
<td>Maintenance Power Signature; the signal a PD sends to the switch to indicate that the PD is connected and requires power.</td>
</tr>
<tr>
<td>Oversubscribed</td>
<td>The state where there are more PDs requesting PoE power than can be accommodated.</td>
</tr>
<tr>
<td>PD</td>
<td>Powered Device. This is an IEEE 802.3at-compliant device that receives its power through a direct connection to a Gig-T PoE port in a PoE device. Examples of PDs include Voice-over-IP (VoIP) telephones, wireless access points, and remote video cameras.</td>
</tr>
<tr>
<td>PoE</td>
<td>Power-Over-Ethernet; the method by which PDs receive power (operates according to the 802.3af standard). Some pre-standard PoE devices are also supported; refer to the FAQs for your switch model.</td>
</tr>
<tr>
<td>PoE+</td>
<td>Power-over-Ethernet Plus; the method by which PDs receive power according to the 802.3at standard. It is backward compatible with devices using the 802.3af standard.</td>
</tr>
<tr>
<td>port-number priority</td>
<td>Refers to the type of power prioritization where, within a priority class, PoE 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 becomes oversubscribed.</td>
</tr>
<tr>
<td>priority class</td>
<td>Refers to the type of power prioritization that uses <strong>Low</strong> (the default), <strong>High</strong>, and <strong>Critical</strong> priority assignments to determine which groups of ports will receive power. Note that power priority rules apply only if PoE provisioning becomes oversubscribed.</td>
</tr>
<tr>
<td>PSE</td>
<td>Power-Sourcing Equipment. The PSE can supply 15.4 watts of PoE power to 24 PoE ports or 30 watts of power to 12 PoE+ ports.</td>
</tr>
</tbody>
</table>
Power Over Ethernet (PoE+) Operation

PoE Operation

Note

You can connect either a PoE device (PD) or a non-PoE device to a port configured for PoE operation.

Using the commands described in this chapter, you can:

- Configure a non-default power threshold for SNMP and Event Log reporting of PoE consumption on all PoE ports on the switch.
- Specify the port priority you want to use for provisioning PoE power in the event that the PoE resources become oversubscribed.
- Enable or disable PoE operation on individual ports.
- Monitor PoE status and performance.

A PSE detects the power needed by a PD before supplying that power, a detection phase referred to as “searching”. If the PSE can’t supply the required amount of power, it does not supply any power. A PSE will not supply any power to a PD unless the PSE has at least 15.4W available. For example, if a PSE has a maximum available power of 382W and is already supplying 378W, and is then connected to a PD requiring 10W, the PSE will not supply power to the PD.

Note

The PSE output maximum is limited to a higher value than 15.4W. This may affect how much power must be in reserve before a detected PD is supplied with power. For example, if the maximum is 20W, then 20W must be currently available for a detected PD to be supplied with power. This can reduce the number of PDs that can be powered by the switch.

Configuration Options

In the default configuration, all Gig-T ports in an HP switch covered in this guide are configured to support PoE operation. You can:

- Disable or re-enable per-port PoE operation on individual ports to help control power usage and avoid oversubscribing PoE resources.
Power Over Ethernet (PoE+) Operation

PoE Operation

- Configure per-port priority for allocating power in case power is oversubscribed. Power for some lower-priority ports is dropped to support the demand on other, higher-priority ports.
- Configure a global power threshold. This setting acts as a trigger for sending a notice when the PoE power consumption crosses the configured global threshold level. (Crossing the threshold level in either direction—PoE power usage either increasing or decreasing—triggers the notice.) The default setting is 80%.

Note

The ports support standard networking links and PoE links. You can connect either a non-PoE device or a PD to a port enabled for PoE without reconfiguring the port.

PD Support

The internal power supply for the switches covered in this guide provides up to 382 watts of power. Depending on the amount of power the power supply device delivers to PoE ports, there may or may not always be enough power available to connect and support PoE operation on all 24 Gig-T ports. When a new PD connects to a PoE port and there is not enough power left to allocate to that port:

- If the new PD connects to a port “X” having a higher PoE priority than another port “Y” that is already supporting another PD, then the power is removed from port “Y” and delivered to port “X”. In this case the PD on port “Y” loses power and the PD on port “X” receives power.
- If the new PD connects to a port “X” having a lower priority than all other PoE ports currently providing power to PDs, then power is not supplied to port “X” until one or more PDs using higher priority ports are removed.

In the default configuration (usage), when a PD connects to a PoE port and begins operating, the port retains only enough PoE power to support the PD’s operation. Unused power becomes available for supporting other PD connections. However, if you configure the poe-allocate-by option to either value or class, then all of the power configured is allocated to the port.

Disconnecting a PD from a PoE port causes the switch to stop providing PoE power to that port and makes the power available to any other PoE ports that have PDs connected and waiting for power. If the PD demand for power becomes greater than the PoE power available, then power is transferred from the lower-priority ports to the higher-priority ports. (Ports not currently providing power to PDs are not affected.)
Power Priority Operation

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 ports enabled for PoE.

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. See “Configuring the PoE Port Priority Level” on page 3-6.

- 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 Gig-T ports. The default priority for all ports is **Low** and the default power notification threshold is **80** (%). Using the CLI, you can perform the functions shown in table 3-1.

<table>
<thead>
<tr>
<th>Function</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the PoE priority level on individual PoE ports</td>
<td>interface &lt;port-list&gt; power-over-ethernet [critical</td>
</tr>
<tr>
<td>Disable or re-enable PoE operation on individual PoE ports</td>
<td>[no] interface &lt;port-list&gt; power-over-ethernet</td>
</tr>
<tr>
<td>Change the threshold for generating a power level notice</td>
<td>power-over-ethernet threshold &lt;1-99&gt;</td>
</tr>
</tbody>
</table>
Power Over Ethernet (PoE+) Operation
Configuring PoE Operation

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 are initially enabled for PoE operation at **Low** priority. If you configure a higher priority, this priority is retained until you change it.)

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. For example, to cycle the power on a PoE device connected to port 1:

```
HP Switch(config)# no interface 1 power-over-ethernet
HP Switch(config)# interface 1 power-over-ethernet
```

Configuring the PoE Port Priority Level

Using a **priority class** method, you can assign a power priority of **Low** (the default), **High**, or **Critical** to each enabled PoE port.

**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 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 shows some examples of PoE priority configuration.

<table>
<thead>
<tr>
<th>Port</th>
<th>Priority Setting</th>
<th>Configuration Command(^1) and Resulting Operation with PDs connected to Ports 3 Through 24</th>
</tr>
</thead>
</table>
| 3 - 17 | Critical | In this example, the following CLI command sets ports 3-17 to Critical:  
   HP Switch(config)# interface 3-17 power-over-ethernet critical  
   The Critical 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-priority ports, then power is allocated to these ports in ascending order, beginning with the lowest-numbered port in the class, which, in this case, is port 3. |
| 19 - 22 | High | In this example, the following CLI command sets ports 19-22 to High:  
   HP Switch(config)# interface 19-22 power-over-ethernet high  
   The High priority class receives power only if all PDs on ports with a Critical priority setting are receiving 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-priority ports, then power is allocated to these ports in ascending order, beginning, in this example, with port 18, until all available power is in use. |
| 23 - 24 | Low | In this example, the CLI command sets ports 23-24 to Low\(^2\):  
   HP Switch(config)# interface 23-24 power-over-ethernet 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 (port 23, in this case), until all available power is in use. |
| 1 - 2 | - n/a - | In this example, the CLI command disables PoE power on ports 1-2:  
   HP Switch(config)# no interface 1-2 power-over-ethernet  
   There is no priority setting for the ports in this example. |

\(^1\) For a listing of PoE configuration commands, with descriptions, refer to “Configuring PoE Operation” on page 3-5.  
\(^2\) In the default PoE configuration, the ports are already set to the Low priority. In this case, the command is not necessary.
Power Over Ethernet (PoE+) Operation
Configuring PoE Operation

Enabling Support for Pre-Standard Devices

The HP switches covered in this guide are automatically backward compatible with 802.3af devices, and can also support some pre-802.3af devices. For a list of the devices supported, refer to the FAQs for your switch model.

**Syntax:**

```
[no] power-over-ethernet pre-std-detect
```

Detections and powers pre-802.3af standard devices.

**Note:** This is enabled by default.

Controlling PoE Allocation

The default option for PoE allocation is **usage**, which is what a PD attached to the port is allocated. You can specify 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. The power supplied to the PD at the output of the PSE is separated into 4 classes. Classes and their ranges are shown in table 3-3. These are approximately the minimum power amounts to be supplied by the PSE. Actual PD needs may be within some range for each class.

**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.
Power Over Ethernet (PoE+) Operation
Configuring PoE Operation

Table 3-3. Power Classes and Their Values

<table>
<thead>
<tr>
<th>Power Class</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Depends on cable type and PoE architecture. Requires a minimum of 30W. 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).</td>
</tr>
<tr>
<td>1</td>
<td>Requires at least 4 watts at the PSE.</td>
</tr>
<tr>
<td>2</td>
<td>Requires at least 7 watts at the PSE.</td>
</tr>
<tr>
<td>3</td>
<td>15.4 watts</td>
</tr>
<tr>
<td>4</td>
<td>reserved: can be power value beyond the class 3 limit. Depends on cable type and PoE architecture.</td>
</tr>
</tbody>
</table>

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 in 1 watt increments, by using the `value` option.

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:
**Power Over Ethernet (PoE+) Operation**

**Configuring PoE Operation**

<table>
<thead>
<tr>
<th>HP Switch(config)# show power-over-ethernet 6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status and Counters - Port Power Status for port 6</strong></td>
</tr>
<tr>
<td><strong>Power Enable</strong> : Yes</td>
</tr>
<tr>
<td><strong>Priority</strong> : low</td>
</tr>
<tr>
<td><strong>AllocateBy</strong> : value</td>
</tr>
<tr>
<td><strong>Detection Status</strong> : Delivering</td>
</tr>
<tr>
<td><strong>Over Current Cnt</strong> : 0</td>
</tr>
<tr>
<td><strong>Power Denied Cnt</strong> : 0</td>
</tr>
<tr>
<td><strong>Voltage</strong> : 55.1 V</td>
</tr>
<tr>
<td><strong>Power</strong> : 19.1 W</td>
</tr>
</tbody>
</table>

**Figure 3-1. Example Displaying PoE Allocation by Value**

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

<table>
<thead>
<tr>
<th>HP Switch(config)# int 7 PoE-value 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Switch(config)# show power-over-ethernet 7</td>
</tr>
<tr>
<td><strong>Status and Counters - Port Power Status for port 7</strong></td>
</tr>
<tr>
<td><strong>Power Enable</strong> : Yes</td>
</tr>
<tr>
<td><strong>Priority</strong> : low</td>
</tr>
<tr>
<td><strong>AllocateBy</strong> : value</td>
</tr>
<tr>
<td><strong>Detection Status</strong> : Other Fault</td>
</tr>
<tr>
<td><strong>Over Current Cnt</strong> : 0</td>
</tr>
<tr>
<td><strong>Power Denied Cnt</strong> : 2</td>
</tr>
<tr>
<td><strong>Voltage</strong> : 0 V</td>
</tr>
<tr>
<td><strong>Power</strong> : 0 W</td>
</tr>
</tbody>
</table>

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

**Changing the Threshold for Generating a Power Notice**

You can generate a power usage notice at a specified threshold by entering this command.
Power Over Ethernet (PoE+) Operation

PoE with LLDP

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.

Syntax: power-over-ethernet threshold < 1 - 99 >

This command specifies the PoE usage level (as a percentage of the PoE power available) at which the switch generates a power usage notice. This notice appears as an SNMP trap and a corresponding Event Log message, and occurs when the power consumption crosses the configured threshold value. That is, the switch generates a notice whenever the power consumption either exceeds or drops below the specified percentage of the total PoE power available.

This command configures the notification threshold for PoE power usage on a global basis.

If the switch is configured for debug logging, it also sends the Event Log message to the configured debug destination(s).
Power Over Ethernet (PoE+) Operation
PoE with LLDP

PoE Allocation

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
```

<table>
<thead>
<tr>
<th>PoE</th>
<th>Power</th>
<th>LLDP</th>
<th>Power</th>
<th>Alloc</th>
<th>PoE</th>
<th>Configured</th>
<th>Detection</th>
<th>Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Enable</td>
<td>Detect</td>
<td>Priority</td>
<td>By</td>
<td>Val</td>
<td>Type</td>
<td>Status</td>
<td>Class</td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
<td>-------</td>
<td>----------</td>
<td>----</td>
<td>-----</td>
<td>------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>1</td>
<td>Yes</td>
<td>enabled</td>
<td>low</td>
<td>usage</td>
<td>5</td>
<td>Phone-1</td>
<td>Delivering</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>usage</td>
<td>17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>usage</td>
<td>17</td>
<td></td>
<td>Searching</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>usage</td>
<td>17</td>
<td></td>
<td>Searching</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>usage</td>
<td>17</td>
<td></td>
<td>Searching</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>value</td>
<td>17</td>
<td></td>
<td>Searching</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Yes</td>
<td>enabled</td>
<td>low</td>
<td>value</td>
<td>5</td>
<td>Phone-2</td>
<td>Delivering</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>value</td>
<td>17</td>
<td></td>
<td>Searching</td>
<td>0</td>
</tr>
</tbody>
</table>

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

3-12
Power Over Ethernet (PoE+) Operation

PoE with LLDP

Enabling Advertisement of Poe TLVs

To initiate the advertisement of power with PoE TLVs, the following command is configured with the `poeplus_config` option.

**Syntax:** `lldp config <port-list> dot3TlvEnable poeplus_config`

*Enables advertisement of data link layer power using PoE TLVs. The TLV is processed only after the physical layer and the data link layer are enabled. The TLV informs the PSE about the actual power required by the device.*

Displaying PoE When Using LLDP Information

Displaying LLDP Port Configuration

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
* poeplus_config

IpAddress Advertised:
```

Figure 3-4. Example of LLDP Port Configuration Information with PoE
Power Over Ethernet (PoE+) Operation
PoE with LLDP

Displaying Local Device Power Information

To view information about local PoE devices and power usage, use this command.

Syntax: show lldp info local-device <port-list>

Displays detailed information about local PoE devices.

| Port | 1 |
| PortType | local |
| PortId | 1 |
| PortDesc | 1 |
| Poe Device Type | Type2 PSE |
| Power Source | Primary |
| Requested Power Value | 15 Watts |
| Actual Power Value | 15 Watts |
| Acknowledgement | Not part of ack/nack cycle |
| Lost Communication | 0 |

Figure 3-5. Example of LLDP Local Device Information

Displaying Remote Power Information

To view information about remote PoE devices and power usage, use this command.

Syntax: show lldp info remote-device <port-list>

Displays detailed information about remote PoE devices.
### Power Over Ethernet (PoE+) Operation

#### PoE with LLDP

**Figure 3-6. Example of LLDP Remote Device Information**

```
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 : HP Switch
System Descr : HP J9562A Switch, revision A.15.XX
PortDescr : 23

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

Remote Management Address
Type : ipv4
Address : 10.0.10.10

Poe Plus Information Detail

Poe Device Type : Type2 PD
Power Source : Only PSE
Power Priority : High
Requested Power Value : 10 Watts
Actual Power Value : 10 Watts
Acknowledgement : Not part of ack/nack cycle
```
Power Over Ethernet (PoE+) Operation
PoE with LLDP

Possible values for the PoE information are shown in table 3-4.

Table 3-4. Values for Displayed PoE Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poe Device Type</td>
<td>• Type2 PSE</td>
</tr>
<tr>
<td></td>
<td>• Type2 PD</td>
</tr>
<tr>
<td></td>
<td>• Type1 PSE</td>
</tr>
<tr>
<td></td>
<td>• Type1 PD</td>
</tr>
<tr>
<td>Local Power Source</td>
<td>• Unknown</td>
</tr>
<tr>
<td>(from where the PSE is sourcing power to PD)</td>
<td>• Primary</td>
</tr>
<tr>
<td></td>
<td>• Backup</td>
</tr>
<tr>
<td></td>
<td>• Reserved</td>
</tr>
<tr>
<td>Remote Power Source</td>
<td>• Unknown</td>
</tr>
<tr>
<td>(from where the PD is acquiring power)</td>
<td>• Only PSE</td>
</tr>
<tr>
<td></td>
<td>• Only Local</td>
</tr>
<tr>
<td></td>
<td>• PSE and Local</td>
</tr>
<tr>
<td>Power Priority Values</td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• High</td>
</tr>
<tr>
<td></td>
<td>• Low</td>
</tr>
<tr>
<td>Acknowledgement Values</td>
<td>• Not part of ack/nack cycle</td>
</tr>
<tr>
<td>For a PSE (local), this value is the response by the PSE to the request from the PD. For a PD (remote), this value is the response by the PD to the request from the PSE.</td>
<td>• Acknowledge</td>
</tr>
<tr>
<td></td>
<td>• Non Acknowledge</td>
</tr>
<tr>
<td></td>
<td>• Loss of Communication</td>
</tr>
</tbody>
</table>
Displaying the Global PoE Status

Syntax:  show power-over-ethernet [brief | ethernet <port-list> | all]]

Displays the switch's global PoE power status.

brief: Displays PoE information for each port. See “Displaying PoE Status on All Ports” on page 3-18.

<port-list>: Displays PoE information for the ports in <port-list>. See “Displaying the PoE Status on Specific Ports” on page 3-19.

For example, show power-over-ethernet displays data similar to that in figure 3-7.

```
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 Provided Power:  382 W
Total Failover Power:  0 W
Total Redundancy Power:  0 W
Total Redundancy Power:  0 W
Total Allocated Power:  376 W +/- 6W
```

Figure 3-7. Example of Show Power-Over-Ethernet Output
Power Over Ethernet (PoE+) Operation
Displaying the Global PoE Status

Displaying PoE Status on All Ports

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

Displays the following port power status:

- **Port:** Lists all PoE-capable ports on the switch.
- **Power Enable:** Shows *Yes* for ports enabled to support PoE (the default) and *No* for ports on which PoE is disabled.
- **LLDP Detect:** Displays if the port is enabled or disabled for allocating PoE power based on the link-partner’s capabilities via LLDP *(enabled, disabled)*. Not all PoE devices support LLDP, so PoE information is ignored by default.
- **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 3-5.)*
- **Alloc by:** Displays how PoE is allocated *(usage, class, value)*
- **PoE Value:** The maximum amount of PoE power allocated for that port (expressed in watts).
- **Configured Type:** If configured, shows the user-specified identifier for the port. If not configured, the field is empty.
- **Detection Status:**
  - **Searching:** The port is trying to detect a PD connection.
  - **Delivering:** The port is delivering power to a PD.
  - **Disabled:** On the indicated port, either PoE support is disabled or PoE power is enabled but the PSE does not have enough power available to supply the port’s power needs.
  - **Fault:** The switch detects a problem with the connected PD.
- **Power Class:** Shows the 802.3at physical layer power class of the PD detected on the indicated port. Classes include:
  
<table>
<thead>
<tr>
<th>Class</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Depends on cable type and PoE architecture</td>
</tr>
<tr>
<td>1</td>
<td>4 watts</td>
</tr>
<tr>
<td>2</td>
<td>7 watts</td>
</tr>
<tr>
<td>3</td>
<td>15.4 watts</td>
</tr>
<tr>
<td>4</td>
<td>reserved—can be power value beyond the class 3 limit. Depends on cable type and PoE architecture.</td>
</tr>
</tbody>
</table>

- **Other fault:** The switch has detected an internal fault that prevents it from supplying power on that port.
Power Over Ethernet (PoE+) Operation
Displaying the Global PoE Status

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

<table>
<thead>
<tr>
<th>PoE Port</th>
<th>Power Enable</th>
<th>LLDP Detect</th>
<th>Power Priority</th>
<th>Alloc By</th>
<th>Configured Val</th>
<th>Detection Status</th>
<th>Power Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>enabled</td>
<td>low</td>
<td>usage</td>
<td>5</td>
<td>Phone-1</td>
<td>Delivering</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>usage</td>
<td>17</td>
<td>Searching</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>usage</td>
<td>17</td>
<td>Searching</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>usage</td>
<td>17</td>
<td>Searching</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>usage</td>
<td>17</td>
<td>Searching</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>value</td>
<td>17</td>
<td>Searching</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>value</td>
<td>17</td>
<td>Searching</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Yes</td>
<td>disabled</td>
<td>low</td>
<td>value</td>
<td>17</td>
<td>Searching</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 3-8. 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. Note that for ports on which power is disabled, this is the only field displayed by `show power-over-ethernet <port-list>`.

- **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 3-5.)

- **Allocate by:** How PoE is allocated (**usage**, **class**, **value**)

- **Detection Status:**
  - **Searching:** The port is available to support a PD.
  - **Delivering:** The port is delivering power to a PD.
  - **Disabled:** PoE power is enabled on the port but the PSE does not have enough power available to supply the port’s power needs.
  - **Fault:** The switch detects a problem with the connected PD.
  - **Other Fault:** The switch has detected an internal fault that prevents it from supplying power on that port.

- **Over Current Cnt:** Shows the number of times a connected PD has attempted to draw more than 33 watts if PoE is configured by **usage**, otherwise it is based on the **class** or by the limit configured on the port (**value**). Each occurrence generates an Event Log message.
Syntax: show power-over-ethernet <port-list>  (Continued)

- **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 dV, being delivered to PDs.
- **Power**: The total power, in mW, 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**: If configured, shows the user-specified identifier for the port. If not configured, the field is empty.
- **Value**: The maximum amount of PoE power allocated for that port (expressed in watts).
- **Power Class**: Shows the power class of the PD detected on the indicated port. Classes include:
  
  0: Depends on cable type and PoE architecture
  1: 0.44w to 3.84w
  2: 3.84w to 6.49w
  3: 6.49w to 12.95w
  4: reserved: can be power value beyond the class 3 limit. Depends on cable type and PoE architecture

- **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 "PoE 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 ports 6 and 7, you would use `show power-over-ethernet 6-7` to display the data:

```
HP Switch(config)# show power-over-ethernet 6-7

Status and Counters - Port Power Status for port 6
Power Enable : Yes
Priority : low
AllocateBy : value
Detection Status : Delivering
Over Current Cnt : 0
Power Denied Cnt : 0
Voltage : 55.1 V
Power : 15 W

Status and Counters - Port Power Status for port 7
Power Enable : yes
Priority : low
AllocateBy : value
Detection Status : Searching
Over Current Cnt : 0
Power Denied Cnt : 0
Voltage : 0 V
Power : 0 W
```

Figure 3-9. Example of Show Power-Over-Ethernet `<port-list>` Output
Planning and Implementing a PoE Configuration

This section provides an overview of some considerations for planning a PoE application. For additional information on this topic, refer to the *HP PoE Planning and Implementation Guide* which is available on the HP Networking web site at [www.hp.com/networking](http://www.hp.com/networking).

Some of the elements you may want to consider for a PoE installation include:

- Port assignments to VLANs
- Use of security features
- Power requirements

This section can help you to plan your PoE installation. If you use multiple VLANs in your network, or if you have concerns about network security, you should read the first two topics. If your PoE installation comes close to (or is likely to exceed) the system’s ability to supply power to all devices that may request it, then you should also read the third topic. (If it is unlikely that your installation will even approach a full utilization of the PoE power available, then you may find it unnecessary to spend much time on calculating PoE power scenarios.)

Assigning PoE Ports to VLANs

If your network includes VLANs, you may want to assign various PoE 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 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.
Power Over Ethernet (PoE+) Operation
Planning and Implementing a PoE Configuration

- **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:
  - Local username and password
  - TACACS+
  - RADIUS Authentication and Accounting
  - 802.1X Authentication

For more information on security options, refer to the latest edition of the *Access Security Guide* for your switch. (The HP Networking web site offers the latest version of all HP product publications.

Assigning Priority Policies to PoE Traffic

You can use the configurable QoS (Quality of Service) features in the switch to create prioritization policies for traffic moving through PoE ports. Table 3-5 lists the available classifiers and their order of precedence.

**Table 3-5. Classifiers for Prioritizing Outbound Packets**

<table>
<thead>
<tr>
<th>Priority</th>
<th>QoS Classifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UDP/TCP Application Type (port)</td>
</tr>
<tr>
<td>2</td>
<td>Device Priority (destination or source IP address)</td>
</tr>
<tr>
<td>3</td>
<td>IP Type of Service (ToS) field (IP packets only)</td>
</tr>
<tr>
<td>4</td>
<td>VLAN Priority</td>
</tr>
<tr>
<td>5</td>
<td>Incoming source-port on the switch</td>
</tr>
<tr>
<td>6</td>
<td>Incoming 802.1p priority (present in tagged VLAN environments)</td>
</tr>
</tbody>
</table>

For more on this topic, refer to the chapter titled “Quality of Service: Managing Bandwidth More Effectively” in the *Advanced Traffic Management Guide* for your switch.

PoE Event Log Messages

PoE operation generates these Event Log messages. You can also configure the switch to send these messages to a configured debug destination (terminal device or SyslogD server).

**“Informational” PoE Event-Log Messages**
## Power Over Ethernet (PoE+) Operation
Planning and Implementing a PoE Configuration

### Message

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>I <code>&lt;MM/DD/YY&gt;</code> <code>&lt;HH:MM:SS&gt;</code> <code>&lt;ports&gt;</code></td>
<td>Message header, with severity, date, system time. For more information on Event Log operation, including severity indicators, refer to “Using the Event Log for Troubleshooting Switch Problems” on page C-34.</td>
</tr>
<tr>
<td>port <code>&lt;port-id&gt;</code> applying power to PD</td>
<td>A PoE device is connected to the indicated port and receiving power.</td>
</tr>
<tr>
<td>port <code>&lt;port-id&gt;</code> PD detected</td>
<td>The switch has detected a PoE device connected to the indicated port.</td>
</tr>
</tbody>
</table>

### “Warning” PoE Event-Log Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>W <code>&lt;MM/DD/YY&gt;</code> <code>&lt;HH:MM:SS&gt;</code> chassis</td>
<td>Message header, with severity, date, system time. For more information on Event Log operation, including severity indicators, refer to “Using the Event Log for Troubleshooting Switch Problems” on page C-34.</td>
</tr>
<tr>
<td>Port <code>&lt;port-id&gt;</code> PD Denied power due to insufficient power allocation.</td>
<td>There is insufficient power available to power the PD on the indicated port and the port does not have sufficient PoE priority to take power from another active PoE port.</td>
</tr>
<tr>
<td>Port <code>&lt;port-id&gt;</code> PD Invalid Signature indication</td>
<td>The switch has detected a non-802.3af-compliant device on the indicated port. This message appears for all non-802.3af devices connected to the port, such as other switches, PC-NICs, etc.</td>
</tr>
<tr>
<td>Port <code>&lt;port-id&gt;</code> PD MPS Absent indication</td>
<td>The switch no longer detects a device on <code>&lt;port-id&gt;</code>. The device may have been disconnected, powered down, or stopped functioning.</td>
</tr>
<tr>
<td>Port <code>&lt;port-id&gt;</code> PD Other Fault indication</td>
<td>There is a problem with the PD connected to the port.</td>
</tr>
<tr>
<td>Port <code>&lt;port-id&gt;</code> PD Over Current indication</td>
<td>The PD connected to <code>&lt;port-id&gt;</code> has requested more than 15.4 watts of power. This may indicate a short-circuit or other problem in the PD.</td>
</tr>
<tr>
<td>50v Power Supply is faulted. Failures:x</td>
<td>Internal power supply has faulted.</td>
</tr>
<tr>
<td>50v Power Supply is OK. Failures:x</td>
<td>Internal power supply is now OK.</td>
</tr>
<tr>
<td>FET bad on port <code>&lt;port-id&gt;</code></td>
<td>External FET (Field Effect Transistor) on the port has gone bad and cannot deliver power.</td>
</tr>
</tbody>
</table>
Port Trunking

Overview

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

Port Status and Configuration Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>viewing port trunks</td>
<td>n/a</td>
<td>page 4-7</td>
<td>page 4-9</td>
</tr>
<tr>
<td>configuring a static trunk group</td>
<td>none</td>
<td>page 4-7</td>
<td>page 4-12</td>
</tr>
<tr>
<td>configuring a dynamic LACP trunk group</td>
<td>disabled</td>
<td>—</td>
<td>page 4-13</td>
</tr>
</tbody>
</table>

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 back-bone 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 an 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 4-14
- Trunk: Non-Protocol—page 4-22

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 4-14.)

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.
Port Trunking
Trunk Configuration Methods

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

<table>
<thead>
<tr>
<th>Trunking Method</th>
<th>LACP</th>
<th>Trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Static</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 4-2. Trunk Configuration Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Trunking Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACP (802.3ad)</td>
<td>Provides dynamic and static LACP trunking options.</td>
</tr>
<tr>
<td></td>
<td>• Dynamic LACP — Use the switch-negotiated dynamic LACP trunk when:</td>
</tr>
<tr>
<td></td>
<td>-- The port on the other end of the trunk link is configured for Active or Passive LACP.</td>
</tr>
<tr>
<td></td>
<td>-- 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.</td>
</tr>
<tr>
<td></td>
<td>• Static LACP — Use the manually configured static LACP trunk when:</td>
</tr>
<tr>
<td></td>
<td>-- The port on the other end of the trunk link is configured for a static LACP trunk</td>
</tr>
<tr>
<td></td>
<td>-- You want to configure non-default spanning tree or IGMP parameters on an LACP trunk group.</td>
</tr>
<tr>
<td></td>
<td>-- 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.)</td>
</tr>
<tr>
<td></td>
<td>-- You want to use a monitor port on the switch to monitor traffic on an LACP trunk.</td>
</tr>
</tbody>
</table>

For more information, refer to “Trunk Group Operation Using LACP” on page 4-14.

<table>
<thead>
<tr>
<th>Trunk (non-protocol)</th>
<th>Provides manually configured, static-only trunking to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Most HP switches and routing switches not running the 802.3ad LACP protocol.</td>
</tr>
<tr>
<td></td>
<td>• Windows NT and HP-UX workstations and servers</td>
</tr>
<tr>
<td></td>
<td>Use the Trunk option when:</td>
</tr>
<tr>
<td></td>
<td>-- The device to which you want to create a trunk link is using a non-802.3ad trunking protocol</td>
</tr>
<tr>
<td></td>
<td>-- 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.</td>
</tr>
<tr>
<td></td>
<td>-- You want to use a monitor port on the switch to monitor traffic on a trunk.</td>
</tr>
</tbody>
</table>

Refer to “Trunk Group Operation Using the “Trunk” Option” on page 4-22.
Port Trunking
Trunk Configuration Methods

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 4-14.

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 4-23.
Port Trunking
Trunk Configuration Methods

**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 Spanning Tree 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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Cost</th>
<th>Priority</th>
<th>State</th>
<th>Designated Bridge</th>
</tr>
</thead>
<tbody>
<tr>
<td>C3</td>
<td>10G/1000T</td>
<td>5</td>
<td>128</td>
<td>Forwarding</td>
<td>0018e1-11274c0</td>
</tr>
<tr>
<td>C4</td>
<td>10G/1000T</td>
<td>5</td>
<td>128</td>
<td>Forwarding</td>
<td>0060b0-683e00</td>
</tr>
<tr>
<td>C5</td>
<td>10G/1000T</td>
<td>5</td>
<td>128</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>C6</td>
<td>10G/1000T</td>
<td>5</td>
<td>128</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Trk1</td>
<td>1</td>
<td>64</td>
<td></td>
<td>Forwarding</td>
<td>001e7-603c00</td>
</tr>
</tbody>
</table>

**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 4-14.

**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 2-11.)

**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.

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.
Port Trunking
Menu: Viewing and Configuring a Static Trunk Group

- 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.)

---

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Enabled</th>
<th>Mode</th>
<th>Flow Ctrl</th>
<th>Group</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>10/100TX</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>C2</td>
<td>10/100TX</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>C3</td>
<td>10/100TX</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>C4</td>
<td>10/100TX</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td></td>
<td>-</td>
</tr>
<tr>
<td>C5</td>
<td>10/100TX</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td>Trnk</td>
<td>Trunk</td>
</tr>
<tr>
<td>C6</td>
<td>10/100TX</td>
<td>Yes</td>
<td>Auto</td>
<td>Disable</td>
<td>Trnk</td>
<td>Trunk</td>
</tr>
</tbody>
</table>

Actions-> Cancel Hit Save Help

Select whether the port is part of a trunk or Mesh.

Use arrow keys to change field selection, <Space> to toggle field choices, and <Enter> to go to Actions.

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-34) to verify that the trunked ports are operating properly.

---

**CLI: Viewing and Configuring Port Trunk Groups**

**Trunk Status and Configuration Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show trunks</td>
<td></td>
</tr>
<tr>
<td>show lacp</td>
<td>4-10</td>
</tr>
<tr>
<td>trunk</td>
<td>4-12</td>
</tr>
<tr>
<td>interface &lt; port-list &gt; lacp</td>
<td>4-13</td>
</tr>
</tbody>
</table>

**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.*
Port Trunking
CLI: Viewing and Configuring Port Trunk Groups

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:

```
Switch> show trunks e 5-7
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Type</th>
<th>Group Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Print-Server-Trunk</td>
<td>10/100TX</td>
<td>Trk1</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>10/100TX</td>
<td>Trk2</td>
</tr>
</tbody>
</table>

Port 5 appears with an example of a name that you can optionally assign using the Friendly Port Names feature. (Refer to “Using Friendly (Optional) Port Names” on page 2-17.)

Port 6 does not appear in this listing because it is not assigned to a static trunk.

```
Switch> show trunks
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Type</th>
<th>Group Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Print-Server-Trunk</td>
<td>10/100TX</td>
<td>Trk1</td>
</tr>
<tr>
<td>5</td>
<td>Print-Server-Trunk</td>
<td>10/100TX</td>
<td>Trk1</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>10/100TX</td>
<td>Trk2</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>10/100TX</td>
<td>Trk2</td>
</tr>
</tbody>
</table>

**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.

```
Switch> show trunks
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Type</th>
<th>Group Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Print-Server-Trunk</td>
<td>10/100TX</td>
<td>Trk1</td>
</tr>
<tr>
<td>5</td>
<td>Print-Server-Trunk</td>
<td>10/100TX</td>
<td>Trk1</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>10/100TX</td>
<td>Trk2</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>10/100TX</td>
<td>Trk2</td>
</tr>
</tbody>
</table>

**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.)

<table>
<thead>
<tr>
<th>PORT NUMB</th>
<th>LACP ENABLED</th>
<th>TRUNK GROUP</th>
<th>STATUS</th>
<th>PARTNER STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active</td>
<td>Trk1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Active</td>
<td>Trk1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Active</td>
<td>3</td>
<td>Down</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>Passive</td>
<td>4</td>
<td>Down</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>Passive</td>
<td>5</td>
<td>Down</td>
<td>No</td>
</tr>
<tr>
<td>6</td>
<td>Passive</td>
<td>6</td>
<td>Down</td>
<td>No</td>
</tr>
</tbody>
</table>

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 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”.

<table>
<thead>
<tr>
<th>PORT NUMB</th>
<th>LACP ENABLED</th>
<th>TRUNK GROUP</th>
<th>STATUS</th>
<th>PARTNER STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>8</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>9</td>
<td>Active</td>
<td>Dyn1</td>
<td>Standby</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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 2-11.)

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:

<table>
<thead>
<tr>
<th>Trunk Type</th>
<th>Trunk Group Membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACP</td>
<td>Yes</td>
</tr>
<tr>
<td>Trunk</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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 *TrkX* 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.

![Dynamic LACP Trunk Group Diagram](image)

**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.
Port Trunking
Trunk Group Operation Using LACP

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.

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...
Port Trunking
Trunk Group Operation Using LACP

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:

<table>
<thead>
<tr>
<th>Trunk Display Method</th>
<th>Static LACP Trunk</th>
<th>Dynamic LACP Trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI show lacp command</td>
<td>Included in listing.</td>
<td>Included in listing.</td>
</tr>
<tr>
<td>CLI show trunk command</td>
<td>Included in listing.</td>
<td>Not included.</td>
</tr>
<tr>
<td>Port/Trunk Settings screen in menu interface</td>
<td>Included in listing.</td>
<td>Not included</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>LACP Port Trunk Configuration</th>
<th>Operation</th>
</tr>
</thead>
</table>
| Dynamic LACP                  | This option automatically establishes an 802.3ad-compliant trunk group, with **LACP** for the port Type parameter and **DynX** 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.) **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.

Under the following conditions, the switch automatically establishes a dynamic LACP port trunk group and assigns a port Group name:

- The ports on both ends of each link have compatible mode settings (speed and duplex).
- 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:

```
Switch 1
Port X:
  LACP Enable: Active
Port Y:
  LACP Enable: Active

Switch 2
Port A:
  LACP Enable: Active
Port B:
  LACP Enable: Passive
```

Either of the above link configurations allow a dynamic LACP trunk link. **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.

Displaying Dynamic LACP Trunk Data: To list the configuration and status for a dynamic LACP trunk, use the CLI `show lacp` command.

**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.
Port Trunking
Trunk Group Operation Using LACP

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:

Switch> show lacp

Table 4-5. LACP Port Status Data

<table>
<thead>
<tr>
<th>Status Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Numb</td>
<td>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.</td>
</tr>
</tbody>
</table>
| LACP Enabled| **Active**: The port automatically sends LACP protocol packets.  
**Passive**: The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.  
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.  
**Note**: In the default switch configuration, LACP is disabled for all ports. |
Port Trunking
Trunk Group Operation Using LACP

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:
Port Trunking

Trunk Group Operation Using LACP

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).

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).
Port Trunking
Trunk Group Operation Using LACP

- 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

<table>
<thead>
<tr>
<th>PORT NUMB</th>
<th>LACP ENABLED</th>
<th>TRUNK GROUP</th>
<th>PORT STATUS</th>
<th>LACP PARTNER STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Active</td>
<td>Dyn1</td>
<td>Up</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>Active</td>
<td>Dyn1</td>
<td>Blocked</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>Active</td>
<td>Dyn1</td>
<td>Blocked</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>Active</td>
<td>7</td>
<td>Down</td>
<td>No</td>
</tr>
<tr>
<td>8</td>
<td>Active</td>
<td>8</td>
<td>Down</td>
<td>No</td>
</tr>
</tbody>
</table>
```

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:
Port Trunking
Trunk Group Operation Using LACP

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 (TrkX) 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.

<table>
<thead>
<tr>
<th>Interface Option</th>
<th>Dynamic LACP Trunk Group</th>
<th>Static LACP Trunk Group</th>
<th>Static Non-Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu Interface</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI <code>show trunk</code></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI <code>show interfaces</code></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI <code>show lacp</code></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>CLI <code>show spanning-tree</code></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI <code>show igmp</code></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
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
Port Trunking
Outbound Traffic Distribution Across Trunked Links

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](image)

<table>
<thead>
<tr>
<th>Source:</th>
<th>Destination:</th>
<th>Link:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node A</td>
<td>Node W</td>
<td>1</td>
</tr>
<tr>
<td>Node B</td>
<td>Node X</td>
<td>2</td>
</tr>
<tr>
<td>Node C</td>
<td>Node Y</td>
<td>3</td>
</tr>
<tr>
<td>Node D</td>
<td>Node Z</td>
<td>1</td>
</tr>
<tr>
<td>Node A</td>
<td>Node Y</td>
<td>2</td>
</tr>
<tr>
<td>Node B</td>
<td>Node W</td>
<td>3</td>
</tr>
</tbody>
</table>

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.
Port Traffic Controls

Overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate-Limiting</td>
<td>None</td>
<td>n/a</td>
<td>5-1</td>
<td>n/a</td>
</tr>
<tr>
<td>Jumbo Packets</td>
<td>Disabled</td>
<td>n/a</td>
<td>5-7</td>
<td>n/a</td>
</tr>
</tbody>
</table>

This chapter includes:

- **Rate-Limiting**: Enables a port to limit the amount of bandwidth a user or device may utilize for traffic on the switch.
- **Jumbo Frames**: Enables ports operating at 1 Gbps or 10 Gbps speeds to accept inbound frames of up to 9220 bytes when configured for jumbo traffic.

Rate-Limiting

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-limit all</td>
<td>none</td>
<td>n/a</td>
<td>page 5-2</td>
<td>n/a</td>
</tr>
<tr>
<td>show rate-limit all</td>
<td>n/a</td>
<td>n/a</td>
<td>page 5-3</td>
<td>n/a</td>
</tr>
</tbody>
</table>

All Traffic Rate-Limiting

Rate-limiting for all traffic operates on a per-port basis to allow only the specified bandwidth to be used for inbound or outbound traffic. When traffic exceeds the configured limit, it is dropped. This effectively sets a usage level on a given port, and is a tool for enforcing maximum service level commitments granted to network users. This feature operates on a per-port level and is not configurable on port trunks. Note that rate-limiting is designed to be applied at the network edge to limit traffic from non-critical users or to enforce service agreements such as those offered by Internet Service Providers (ISPs) to provide only the bandwidth for which a customer has paid.
Port Traffic Controls
Rate-Limiting

Note
Rate-limiting also can be applied by a RADIUS server during an authentication client session. For further details, refer to the chapter titled “RADIUS Authentication and Accounting” in the Access Security Guide for your switch.

Caution
Rate-limiting is intended for use on edge ports in a network. It is not recommended for use on links to other switches, routers, or servers within a network, or for use in the network core. Doing so can interfere with applications the network requires to function properly.

Configuring Rate-Limiting
The rate-limit all command controls the rate of traffic sent or received on a port by setting a limit on the bandwidth available. It includes options for:

- Rate-limiting on either inbound or outbound traffic.
- Specifying the traffic rate as either a percentage of bandwidth, or in terms of bits per second.

Syntax:  

```plaintext
[int <port-list> rate-limit all in <percent <0-100> | kbps < 0-10000000>>
```

Configures a traffic rate limit (on non-trunked ports) on the link. The "no" form of the command disables rate-limiting on the specified ports.

(Default: Disabled.)

Options include:

- in — Specifies a traffic rate limit on inbound traffic passing through that port, or on outbound traffic.
- percent or kbps — Specifies the rate limit as a percentage of total available bandwidth, or in kilobits per second.

Notes:
- Rate-limiting does not apply to trunked ports.
Port Traffic Controls
Rate-Limiting

- **Kbps rate-limiting** is done in segments of 1% of the lowest corresponding media speed. For example, if the media speed is 100 Kbps, the value would be 1 Mbps. A 1-100 Kbps rate-limit is implemented as a limit of 100 Kbps; a limit of 100-199 Kbps is also implemented as a limit of 100 Kbps, a limit of 200-299 Kbps is implemented as a limit of 200 Kbps, and so on.

- **Percentage limits** are based on link speed. For example, if a 100 Mbps port negotiates a link at 100 Mbps and the inbound rate-limit is configured at 50%, then the traffic flow through that port is limited to no more than 50 Mbps. Similarly, if the same port negotiates a 10 Mbps link, then it allows no more than 5 Mbps of inbound traffic.

Configuring a rate limit of 0 (zero) on a port blocks all traffic on that port. However, if this is the desired behavior on the port, HP recommends using the `<port-list> disable` command instead of configuring a rate limit of 0.

You can configure a rate limit from either the global configuration level or from the port context level. For example, either of the following commands configures an inbound rate limit of 60% on ports 3 - 5:

```plaintext
HP Switch(config)# int 3-5 rate-limit all in percent 60
HP Switch(eth-3-5)# rate-limit all in percent 60
```

**Note**: You must execute a `write mem` to save the rate-limiting configuration to the start-up config file.

Displaying the Current Rate-Limit Configuration

The `show rate-limit all` command displays the per-port rate-limit configuration.

**Syntax**: `show rate-limit all [port-list]`

Without `[port-list]`, this command lists the rate-limit configuration for all ports on the switch. With `[port-list]`, this command lists the rate-limit configuration for the specified port(s). This command operates the same way in any CLI context.

For example, if you wanted to view the rate-limiting configuration:
Operating Notes for Rate-Limiting

- **Rate-limiting operates on a per-port basis**, regardless of traffic priority. Rate-limiting is available on all types of ports (other than trunked ports) on the switches covered in this guide, and at all port speeds configurable for these devices.

- **Rate-limiting is not allowed on trunked ports**: Rate-limiting is not supported on ports configured in a trunk group. Configuring a port for rate-limiting and then adding it to a trunk suspends rate-limiting on the port while it is in the trunk. Attempting to configure rate-limiting on a port that already belongs to a trunk generates the following message:
  
  ```
  <port-list>: Operation is not allowed for a trunked port.
  ```

- **Rate-limiting is visible as an outbound forwarding rate**: Because inbound rate-limiting is performed on packets during packet-processing, it is not shown via the inbound drop counters. Instead, this limit is verifiable as the ratio of outbound traffic from an inbound rate-limited port versus the inbound rate.

- **Operation with other features**: Configuring rate-limiting on a port where other features affect port queue behavior (such as flow control) can result in the port not achieving its configured rate-limiting maximum. For example, in a situation where flow control is configured on a rate-limited port, there can be enough “back pressure” to hold high-priority inbound traffic from the upstream device or application to a rate that is lower than the configured rate limit. In this case, the inbound traffic flow does not reach the configured rate and lower priority traffic is not forwarded into the switch fabric from the rate-limited port. (This behavior is termed “head-of-line blocking” and is a well-known problem with flow-control.) In another type of situation, an outbound port can become oversubscribed by traffic received from multiple rate-limited ports. In this case, the actual rate for traffic on the rate-limited ports may be lower than configured because the total traffic load requested to the outbound port exceeds the port’s bandwidth, and thus some requested traffic may be held off on inbound.

---

Figure 5-1. Example of Listing the Rate-Limit Configuration

<table>
<thead>
<tr>
<th>Port</th>
<th>Limit</th>
<th>Mode</th>
<th>Radius Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No-override</td>
</tr>
<tr>
<td>2</td>
<td>500</td>
<td>kbps</td>
<td>No-override</td>
</tr>
<tr>
<td>3</td>
<td>50</td>
<td>%</td>
<td>No-override</td>
</tr>
<tr>
<td>4</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No-override</td>
</tr>
</tbody>
</table>
**Port Traffic Controls**

**Rate-Limiting**

- **Traffic filters on rate-limited ports**: Configuring a traffic filter on a port does not prevent the switch from including filtered traffic in the bandwidth-use measurement for rate-limiting when it is configured on the same port. For example, ACLs, source-port filters, protocol filters, and multicast filters are all included in bandwidth usage calculations.

- **Monitoring (Mirroring) rate-limited interfaces**: If monitoring is configured, packets dropped by rate-limiting on a monitored interface will still be forwarded to the designated monitor port. (Monitoring shows what traffic is inbound on an interface, and is not affected by “drop” or “forward” decisions.)

- **Optimum rate-limiting operation**: Optimum rate-limiting occurs with 64-byte packet sizes. Traffic with larger packet sizes can result in performance somewhat below the configured bandwidth. This is to ensure the strictest possible rate-limiting of all sizes of packets.

---

### Note on Testing Rate-Limiting

Rate-limiting is applied to the available bandwidth on a port, and not to any specific applications running through the port. If the total bandwidth requested by all applications is less than the configured maximum rate, then no rate-limit can be applied. This situation occurs with a number of popular throughput-testing applications, as well as most regular network applications. Consider the following example that uses the minimum packet size:

The total available bandwidth on a 100 Mbps port “X” (allowing for Inter-packet Gap—IPG), with no rate-limiting restrictions, is:

\[
(((100,000,000 \text{ bits}) / 8) / 84) \times 64 = 9,523,809 \text{ bytes per second}
\]

where:

- The divisor (84) includes the 12-byte IPG, 8-byte preamble, and 64-bytes of data required to transfer a 64-byte packet on a 100 Mbps link.
- Calculated “bytes-per-second” includes packet headers and data. This value is the maximum “bytes-per-second” that 100 Mbps can support for minimum-sized packets.

Suppose port “X” is configured with a rate limit of 50% (4,761,904 bytes). If a throughput-testing application is the only application using the port, and transmits 1 Mbyte of data through the port, it uses only 10.5% of the port’s available bandwidth, and the rate-limit of 50% has no effect. This is because the maximum rate permitted (50%) exceeds the test application’s bandwidth usage (126,642-164,062 bytes, depending upon packet size, which is only 1.3-1.7% of the available total). Before rate-limiting can occur, the test application’s bandwidth usage must exceed 50% of the port’s total available bandwidth. That is, to test the rate-limit setting, the following must be true:

\[
\text{bandwidth usage} > (0.50 \times 9,523,809)
\]
Port Traffic Controls  
Rate-Limiting

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

**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.
Jumbo Frames

The Maximum Transmission Unit (MTU) is the maximum size IP frame the switch can receive for Layer 2 frames inbound on a port. The switch drops any inbound frames 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 frames of up to 9220 bytes (including four bytes for a VLAN tag) when configured for jumbo traffic. You can enable inbound jumbo frames 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 frames 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 frames that do not exceed 1522 bytes are allowed inbound on that port.)

Terminology

**Jumbo Frame**: An IP frame exceeding 1522 bytes in size. The maximum Jumbo frame 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 frames from external devices. If the switch is in a meshed domain, then all meshed ports (operating at 1 Gbps or higher) on the switch will accept jumbo traffic from other devices in the mesh.

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

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

- **Required Port Speed**: This feature allows inbound and outbound jumbo frames on ports operating at speeds of 1 gigabit or higher. At lower port speeds, only standard (1522-byte or smaller) frames are allowed, regardless of the jumbo configuration.

- **Switch Meshing**: If you enable jumbo traffic on a VLAN, then all meshed ports on the switch will be enabled to support jumbo traffic. (On a given meshed switch, every meshed port operating at 1 Gbps or higher becomes a member of every VLAN configured on the switch.)

- **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 frames 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 “Configuring a Maximum Frame Size” on page 5-11.

Configuring Jumbo Frame Operation

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlans</td>
<td>5-10</td>
</tr>
<tr>
<td>show vlans ports &lt; port-list &gt;</td>
<td>5-10</td>
</tr>
<tr>
<td>show vlans &lt; vid &gt;</td>
<td>5-11</td>
</tr>
<tr>
<td>jumbo</td>
<td>5-11</td>
</tr>
<tr>
<td>jumbo max-frame-size</td>
<td>5-11</td>
</tr>
</tbody>
</table>
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 frames 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 frames on one or more VLANs statically configured in the switch. (All ports belonging to a jumbo-enabled VLAN can receive jumbo frames.

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 “Configuring a Maximum Frame Size” on page 5-11.) See Figure 5-2, below.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>Status</th>
<th>Voice</th>
<th>Jumbo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Port-based</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>VLAN5</td>
<td>Port-based</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>22</td>
<td>VLAN22</td>
<td>Port-based</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Figure 5-2. Example Listing of Static VLANs To Show Jumbo Status Per VLAN
Port Traffic Controls
Jumbo Frames

Syntax: show vlans ports < port-list>

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 5-3.)

Figure 5-3. 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 5-4. Example of Listing the Port Membership and Jumbo Status for a VLAN

5-10
Enabling or Disabling Jumbo Traffic on a VLAN

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

Configures the specified VLAN to allow jumbo frames 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 frames through any other VLAN statically configured on the switch, regardless of whether the other VLAN is enabled for jumbo frames. 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.)

Configuring a Maximum Frame Size

You can globally set a maximum frame size for Jumbo frames that will support values from 1518 bytes to 9216 bytes for untagged frames.

**Syntax:** `jumbo max-frame-size <size>`

Sets the maximum frame size for Jumbo frames. The range is from 1518 bytes to 9216 bytes.

**Note:** The `jumbo max-frame-size` is set on a GLOBAL level.

**Default:** 9216 bytes

SNMP Implementation

**Jumbo Maximum Frame Size.**

The maximum frame size for Jumbos is supported with the following proprietary MIB object:

`hpSwitchMaxFrameSize OBJECT-TYPE`

This is the value of the global `max-frame-size` supported by the switch. The default value is set to 9216 bytes.
Port Traffic Controls
Jumbo Frames

Displaying the Maximum Frame Size

Use the `show jumbos` command to display the globally configured untagged maximum frame size for the switch.

```
HP Switch(config)# show jumbos
Jumbos Global Values
Configured : MaxFrameSize : 9216      Ip-MTU : 9198
In Use     : MaxFrameSize : 9216      Ip-MTU : 9198
```

Figure 5-5. Displaying the Maximum Frame Size and IP MTU Values

Operating Notes for Maximum Frame Size

- When you set a maximum frame size for Jumbo frames, it must be on a global level. You cannot use the `jumbo max-frame-size` command on a per-port or per-VLAN basis.

- The original way to configure Jumbo frames remains the same, which is per-VLAN, but you cannot set a maximum frame size per-VLAN.

- Jumbo support must be enabled for a VLAN from the CLI or through SNMP.

- Setting the maximum frame size does not require a reboot.

- When you upgrade to a version of software that supports setting the maximum frame size from a version that did not, the `max-frame-size` value is set automatically to 9216 bytes.

- Configuring a Jumbo maximum frame size on a VLAN allows frames up to `max-frame-size` even though other VLANs of which the port is a member are not enabled for Jumbo support.

Operating Notes for Jumbo Traffic-Handling

- HP does not recommend configuring a voice VLAN to accept jumbo frames. Voice VLAN frames are typically small, and allowing a voice VLAN to accept jumbo frame traffic can degrade the voice transmission performance.

- You can configure the default, primary, and/or (if configured) the management VLAN to accept jumbo frames 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 frames 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 frames of up to 9220 bytes in length.
A port receiving frames exceeding the applicable MTU drops such frames, causing the switch to generate an Event Log message and increment the “Giant Rx” counter (displayed by `show interfaces <port-list>`).

- The switch allows flow control and jumbo frame capability to co-exist on a port.
- 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 WebAgent, and also increments the switch’s “Giant Rx” counter.
- If you do not want all ports in a given VLAN to accept jumbo frames, 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 frames 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 frames 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:

<table>
<thead>
<tr>
<th>Ports</th>
<th>VLAN 100</th>
<th>VLAN 200</th>
<th>VLAN 300</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jumbo-Enabled?</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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 frames 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 frames can forward them to the ports in the VLAN that do not have jumbo capability.
Port Traffic Controls
Jumbo Frames

Figure 5-6. Forwarding Jumbo Frames Through Non-Jumbo Ports

Jumbo frames can also be forwarded out non-jumbo ports when the jumbo frames 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.

- Jumbo Traffic in a Switch Mesh Domain. Note that if a switch belongs to a meshed domain, but does not have any VLANs configured to support jumbo traffic, then the meshed ports on that switch will drop any jumbo frames they receive from other devices. In this regard, if a mesh domain includes any HP 1600M/2400M/2424M/4000M/8000M switches along with the switches covered in this guide configured to support jumbo traffic, only the switches covered in this guide will receive jumbo frames. The other switch models in the mesh will drop such frames. For more information on switch meshing, refer to the chapter titled “Switch Meshing” in the Advanced Traffic Management Guide for your switch.

Troubleshooting

A VLAN is configured to allow jumbo frames, but one or more ports drops all inbound jumbo frames. 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 frames. 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 frames. 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 frames”
messages in the Event Log. The switches 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 frames received on the jumbo VLAN to non-jumbo ports. Refer to “Outbound Jumbo Traffic” on page 5-13.
Port Traffic Controls
Jumbo Frames
Configuring for Network Management Applications

Using SNMP Tools To Manage the Switch

You can manage the switch via SNMP from a network management station running an application such as PCM or PCM+. For more on PCM and PCM+, visit the HP Networking web site at www.hp.com/networking, click on Network Management.

This section includes:

■ An overview of SNMP management for the switch
■ Configuring the switches for:
  • SNMP Communities (page 6-9)
  • Trap Receivers and Authentication Traps (page 6-15)
■ Advanced management information through RMON Support (page 6-31)

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 Networking 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 6-9)
- Security via authentication and privacy for SNMP Version 3 access
- Event reporting via SNMP
  - Version 1 traps
  - RMON: groups 1, 2, 3, and 9
- PCM/PCM+ 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 Networking web site at:

www.hp.com/networking

Configuring for SNMP version 1 and 2c Access to the Switch

SNMP access requires an IP address and subnet mask configured on the switch. (See “Configuring IP Configuration” in the Basic Operation Guide.) If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address. (See “DHCP/Bootp Operation” in the 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 6-9.)
2. Configure the appropriate trap receivers. (Refer to “SNMP Notifications” on page 6-15.)

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.
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

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. (See “IP Configuration” in the Basic Operation Guide.) If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address. (See “DHCP/Bootp Operation” in the 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 6-4)
2. Configure the appropriate SNMP users (Refer to “SNMPv3 Users” on page 6-5)
3. Configure the appropriate SNMP communities. (Refer to “SNMPv3 Communities” on page 6-9.)
4. Configure the appropriate trap receivers. (Refer to “SNMP Notifications” on page 6-15.)

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 SNMPv3 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:**

- `snmpv3 enable`
  
  Enable and disable the switch for access from SNMPv3 agents. This includes the creation of the initial user record.

- `snmpv3 only`
  
  Enables or disables restrictions to access from only SNMPv3 agents. When enabled, the switch will reject all non-SNMPv3 messages.

- `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 6-1 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.

```
HP Switch(config)# snmpv3 enable
SNMPv3 Initialization process.
Creating user 'initial'
Authentication Protocol: MD5
Enter authentication password: ********
Privacy protocol is DES
Enter privacy password: ********
User 'initial' is created
Would you like to create a user that uses SHA? y
Enter user name: templateSHA
Authentication Protocol: SHA
Enter authentication password: ********
Privacy protocol is DES
Enter privacy password: ********
User creation is done. SHMPv3 is now functional.
Would you like to restrict SHMPv1 and SNMPv2c messages to have read only access (you can set this later by the command 'snmp restrict-access'): n
```

**Figure 6-1. 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:
Configuring for Network Management Applications
Using SNMP Tools To Manage 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 6-6).

2. Assign users to Security Groups based on their security model with the `snmpv3 group` command (see “Assigning Users to Groups” on page 6-8).

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.

```
HP Switch(config)# snmpv3 user NetworkAdmin
```

```
HP Switch(config)# snmpv3 user NetworkMgr auth md5 authpass priv privpass
```

Add user Network Admin with no authentication or privacy.
Add user Network Mgr with authentication and privacy.
MD5 authentication is enabled and the password is set to “authpass”.
Privacy is enabled and the password is set to “privpass”.

```
HP Switch(config)# show snmpv3 user
```

Status and Counters - SNMP v3 Global Configuration Information

<table>
<thead>
<tr>
<th>User Name</th>
<th>Auth. Protocol</th>
<th>Privacy Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>initial</td>
<td>MD5</td>
<td>CFB AES-128</td>
</tr>
<tr>
<td>NetworkAdmin</td>
<td>MD5</td>
<td>CBC-DES</td>
</tr>
</tbody>
</table>

Figure 6-2. Adding SNMPv3 Users and Displaying SNMPv3 Configuration
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

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(vlan-1)# show snmpv3 user

Status and Counters – SNMPv3 Global Configuration Information
User Name     Auth. Protocol     Privacy Protocol
-------------- ----------- ---------------------
initial       MD5            CFB AES-128
NetworkAdmin  MD5            CBC-DES
```

Figure 6-3.  Example of Management Station Information
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

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 6-9.

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 6-9.

```
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.

---

**Figure 6-4. Example of Assigning Users to Groups**

**SNMPv3 Group Commands**

<table>
<thead>
<tr>
<th>Security Name</th>
<th>Security Model</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CommunityManagerReadOnly</td>
<td>ver1</td>
<td>ComManagerR</td>
</tr>
<tr>
<td>CommunityManagerReadWrite</td>
<td>ver1</td>
<td>ComManagerRW</td>
</tr>
<tr>
<td>CommunityOperatorReadOnly</td>
<td>ver1</td>
<td>ComOperatorRW</td>
</tr>
<tr>
<td>CommunityOperatorReadWrite</td>
<td>ver1</td>
<td>ComOperatorRW</td>
</tr>
<tr>
<td>CommunityOperatorReadOnly</td>
<td>ver2c</td>
<td>ComOperatorRW</td>
</tr>
<tr>
<td>CommunityManagerReadWrite</td>
<td>ver2c</td>
<td>ComManagerRW</td>
</tr>
<tr>
<td>CommunityOperatorReadOnly</td>
<td>ver2c</td>
<td>ComOperatorRW</td>
</tr>
<tr>
<td>CommunityOperatorReadWrite</td>
<td>ver2c</td>
<td>ComOperatorRW</td>
</tr>
<tr>
<td>NetworkMgr</td>
<td>ver3</td>
<td>ManagerPriv</td>
</tr>
<tr>
<td>NetworkAdmin</td>
<td>ver3</td>
<td>OperatorNoAuth</td>
</tr>
</tbody>
</table>

Pre-assigned groups for access by Version 2c and version 1 management applications

Add NetworkAdmin to operator noauth group

Add NetworkMgr to managerpriv group
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.

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Group Access Type</th>
<th>Group Read View</th>
<th>Group Write View</th>
</tr>
</thead>
<tbody>
<tr>
<td>managerpriv</td>
<td>Ver3 Must have Authentication and Privacy</td>
<td>ManagerReadView</td>
<td>ManagerWriteView</td>
</tr>
<tr>
<td>managerauth</td>
<td>Ver3 Must have Authentication</td>
<td>ManagerReadView</td>
<td>ManagerWriteView</td>
</tr>
<tr>
<td>operatorauth</td>
<td>Ver3 Must have Authentication</td>
<td>OperatorReadView</td>
<td>DiscoveryView</td>
</tr>
<tr>
<td>operatormauth</td>
<td>Ver3 No Authentication</td>
<td>OperatorReadView</td>
<td>DiscoveryView</td>
</tr>
<tr>
<td>commanagerrw</td>
<td>Ver2c or Ver1</td>
<td>ManagerReadView</td>
<td>ManagerWriteView</td>
</tr>
<tr>
<td>commanagerr</td>
<td>Ver2c or Ver1</td>
<td>ManagerReadView</td>
<td>DiscoveryView</td>
</tr>
<tr>
<td>comoperatorrw</td>
<td>Ver2c or Ver1</td>
<td>OperatorReadView</td>
<td>DiscoveryView</td>
</tr>
<tr>
<td>comoperatorr</td>
<td>Ver2c or Ver1</td>
<td>OperatorReadView</td>
<td>DiscoveryView</td>
</tr>
</tbody>
</table>

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, hpSwitchIpTftpMode, vacmContextTable, vacmAccessTable, vacmViewTreeFamilyTable, 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 commnities 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 6-9. This mapping will happen automatically based on the communities access privileges, but special mappings can be added with the `snmpv3 community` command.
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

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 6-9.

tag <tag_value>
This is used to specify which target address may have access by way of this index reference.

Figure 6-5 shows the assigning of the Operator community on MgrStation1 to the CommunityOperatorReadWrite group. Any other Operator only has an access level of CommunityOperatorReadOnly.

```
Add mapping to allow write access for Operator community on MgrStation1

HP Switch(config)# snmpv3 Community index 30 name Operator sec-name CommunityManagerReadWrite tag MgrStation1
HP Switch(config)# show snmpv3 community

snmpCommunityTable [rfc2576]

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Community Name</th>
<th>Security Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>public</td>
<td></td>
<td>CommunityManagerReadWrite</td>
</tr>
<tr>
<td>2</td>
<td>Operator</td>
<td>Operator</td>
<td>CommunityOperatorReadOnly</td>
</tr>
<tr>
<td>3</td>
<td>Manager</td>
<td>Manager</td>
<td>CommunityManagerReadWrite</td>
</tr>
<tr>
<td>30</td>
<td>Operator</td>
<td>Operator</td>
<td>CommunityManagerReadWrite</td>
</tr>
</tbody>
</table>

Two Operator Access Levels
```

Figure 6-5. Assigning a Community to a Group Access Level
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

SNMP Community Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>show SNMP communities</td>
<td>n/a</td>
<td>page 6-11</td>
<td>page 6-13</td>
<td>—</td>
</tr>
<tr>
<td>configure identity information</td>
<td>none</td>
<td>—</td>
<td>page 6-14</td>
<td></td>
</tr>
<tr>
<td>configure community names</td>
<td>public</td>
<td>page 6-11</td>
<td>page 6-14</td>
<td>—</td>
</tr>
<tr>
<td>MIB view for a community name (operator, manager)</td>
<td>manager</td>
<td>“”</td>
<td>“”</td>
<td></td>
</tr>
<tr>
<td>write access for default community name</td>
<td>unrestricted</td>
<td>“”</td>
<td>“”</td>
<td></td>
</tr>
</tbody>
</table>

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
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

Note: This screen gives an overview of the SNMP communities that are currently configured. All fields in this screen are read-only.

2. Press [A] (for Add) to display the following screen:

![Figure 6-6. The SNMP Communities Screen (Default Values)]

Add and Edit options are used to modify the SNMP options. See Figure 8-2.

Note: This screen gives an overview of the SNMP communities that are currently configured. All fields in this screen are read-only. 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.

3. Enter the name you want in the Community Name field, and use the Space bar to select values for 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

<table>
<thead>
<tr>
<th>Community Name Commands</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp-server [&lt;community-string&gt;]</td>
<td>6-13</td>
</tr>
<tr>
<td>[no] snmp-server</td>
<td>6-14</td>
</tr>
<tr>
<td>[community &lt;community-str&gt;]</td>
<td>6-14</td>
</tr>
<tr>
<td>[host &lt;community-str&gt; &lt;ip-addr&gt;]</td>
<td>6-17</td>
</tr>
<tr>
<td>[enable traps &lt;authentication&gt;]</td>
<td>6-25</td>
</tr>
<tr>
<td>[enable traps link-change &lt;port-list&gt;]</td>
<td>6-26</td>
</tr>
</tbody>
</table>

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 6-15).

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 6-8. Example of the SNMP Community Listing with Two Communities](image)

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:

<table>
<thead>
<tr>
<th>Community</th>
<th>Access Level</th>
<th>Type of Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>red-team</td>
<td>manager (Access to all MIB objects.)</td>
<td>unrestricted (read/write)</td>
</tr>
<tr>
<td>blue-team</td>
<td>operator (Access to all MIB objects except the CONFIG MIB.)</td>
<td>restricted (read-only)</td>
</tr>
</tbody>
</table>

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
  - Instrumentation monitoring
  - Link-Layer Discovery Protocol (LLDP)
  - Ping tests
  - Power over Ethernet (POE): port toggle, power limit
  - RMON
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

- **Advance Traffic Management Guide:**
  - Loop protection
  - Spanning Tree (STP, RSTP, MSTP)

- **Access Security Guide:**
  - MAC lockdown
  - MAC lockout
  - Uni-Directional Link Detection (UDLD)

**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 6-17
   - “Configuring an SNMP Trap Receiver” on page 6-17
   - “Enabling SNMPv2c Informs” on page 6-19
   
   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 6-20

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 6-26

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 6-27
   - “Displaying SNMP Notification Configuration” on page 6-29
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 the public community name. These traps cannot be redirected to other communities. If you change or delete the default public community name, these traps are not sent.

- **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.
Configuring for Network Management Applications
Using SNMP Tools To Manage 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`.

```plaintext
[<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 6-1, “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.

```plaintext
[<inform>]
```

(Optional) Configures the switch to send SNMPv2 inform requests when certain events occur. See “Enabling SNMPv2c Informs” on page 6-19 for more information.

---

**Table 6-1. Security Levels for Event Log Messages Sent as Traps**

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (default)</td>
<td>Sends no event log messages.</td>
</tr>
<tr>
<td>All</td>
<td>Sends all event log messages.</td>
</tr>
<tr>
<td>Non-Info</td>
<td>Sends all event log messages that are not for information only.</td>
</tr>
<tr>
<td>Critical</td>
<td>Sends only event log messages for critical error conditions.</td>
</tr>
<tr>
<td>Debug</td>
<td>Sends only event log messages needed to troubleshoot network- and switch-level problems.</td>
</tr>
</tbody>
</table>
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

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 \texttt{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 ([<\texttt{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 \texttt{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 \texttt{<ipv4-addr | ipv6-addr> <community name> inform [retries <count>] [timeout <interval>]\]

\textit{Enables (or disables) the inform option for SNMPv2c on the switch and allows you to configure options for sending SNMP inform requests.}
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

**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:

```console
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   Type  Retry  Timeout
  ---------------   ----------   --------  ----   ------  ------
  15.255.134.252    public      None     trap   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
```

**Figure 6-9. 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 6-4).

   When SNMPv3 is enabled, the switch supports:
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

- 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 6-5). 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 6-8).

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`
<parms_name> must match the `params`
<parms_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>]`n
```

(Optional) Number of times a notification is
retransmitted if no response is received. Range: `1-255`.
Default: `3`.

---

6-22
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

**Syntax:**  

```
[no] snmpv3 targetaddress <ipv4-addr | ipv6-addr> <name>  
---Continued---
[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
```

6. 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 > [noauth | 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:

```
HP Switch(config)# snmpv3 notify MyNotification tagvalue not_tag
HP Switch(config)# snmpv3 targetaddress not_addr params not_parms 15.255.123.109
filter not-info taglist not_tag
HP Switch(config)# snmpv3 params not_parms user NetworkMgr sec-model ver3
message-processing ver3 priv
```

The tag _name value in `snmpv3 notify` command matches the tag _name value in the `snmpv3 targetaddress` command.

*Params _name value in the `snmpv3 targetaddress` command matches the params _name value in the `snmpv3 params` command.*

Configuring the security model `ver3` requires you to configure message processing `ver3` and a security service level.

**Figure 6-10. 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 6-15 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 6-17
- “Configuring SNMPv3 Notifications” on page 6-20

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
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

To enable or disable notification/traps for network security failures and other security events, enter the **snmp-server enable traps** command.

**Syntax:**

```
```

*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.)*

- **arp-protect** sends a trap if ARP packets are received with an invalid source or destination MAC address, an invalid IP address, or an invalid IP-to-MAC binding.
- **auth-server-fail** sends a trap if the connection with a RADIUS or TACACS+ authentication server fails.
- **dhcp-snooping** sends a trap if DHCP packets are received from an untrusted source or if DHCP packets contain an invalid IP-to-MAC binding.
- **dyn-ip-lockdown:** sends a trap if the switch is out of hardware resources needed to program a dynamic IP lockdown rule.
- **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 a trap when a 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-34.

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 6-13.
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

Figure 6-11. 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:**

```plaintext
[no] snmp-server response-source [dst-ip-of-request | <ipv4-addr | ipv6-addr> | loopback<0-7>]
```

- **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.
- **<ipv4-addr | ipv6-addr>:** User-defined interface IP address that is used as the source IP address in an SNMP response PDU. Both IPv4 and IPv6 addresses are supported.
- **loopback <0-7>:** IP address configured for the specified loopback interface that is used as the source IP address in an SNMP response PDU. If multiple loopback IP addresses are configured, the lowest alphanumeric address is used.

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:

```bash
HP Switch(config)# snmp-server response-source dst-ip-of-request
```
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

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 | loopback<0-7>]
```

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.

- `loopback <0-7>`: IP address configured for the specified loopback interface that is used as the source IP address in a generated trap PDU. If multiple loopback IP addresses are configured, the lowest alphanumeric address is used.

**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.
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

<table>
<thead>
<tr>
<th>SNMP Communities</th>
<th>MIB View</th>
<th>Write Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>public</td>
<td>Manager</td>
<td>Unrestricted</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trap Receivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Change Traps Enabled on Ports [All] : All</td>
</tr>
</tbody>
</table>

Excluded MIBs

<table>
<thead>
<tr>
<th>Snmp Response Pdu Source-IP Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection Policy : dstIpOfRequest</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trap Pdu Source-IP Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection Policy : Configured IP</td>
</tr>
<tr>
<td>Ip Address : 10.10.10.10</td>
</tr>
</tbody>
</table>

Figure 6-12. 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.*
Configuring for Network Management Applications
Using SNMP Tools To Manage the Switch

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
ARP Protection                      enabled
DHCP Snooping                       enabled

Address                  Community    Events   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
...
```

**Figure 6-13. 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 PCM network management software. For more on PCM, visit the HP web site at www.hp.com/Networking

Navigate to Network management.

CLI-Configured sFlow with Multiple Instances

Up to three distinct sFlow instances can be configured via the CLI. 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 for Network Management Applications
Using SNMP Tools To Manage the Switch

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;A.15.XX
  Agent Address 10.0.10.228
```

**Figure 6-14. 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 6-15. 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
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Sampling</th>
<th>Dropped</th>
<th>Polling</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes(2)</td>
<td>1234567890</td>
<td>---</td>
</tr>
<tr>
<td>2</td>
<td>---</td>
<td>---</td>
<td>Yes(1)</td>
</tr>
<tr>
<td>3</td>
<td>No(1)</td>
<td>898703</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>Yes(3)</td>
<td>0</td>
<td>No(3)</td>
</tr>
</tbody>
</table>

Table 6-2. LLDP and LLDP-MED Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the switch’s LLDP configuration</td>
<td>n/a</td>
<td>—</td>
<td>page 6-42</td>
<td>—</td>
</tr>
<tr>
<td>Enable or disable LLDP on the switch</td>
<td>Enabled</td>
<td>—</td>
<td>page 6-38</td>
<td>—</td>
</tr>
<tr>
<td>Change the transmit interval (refresh-interval) for LLDP packets</td>
<td>30 seconds</td>
<td>—</td>
<td>page 6-46</td>
<td>—</td>
</tr>
</tbody>
</table>

**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 Networking 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.
Configuring for Network Management Applications

LLDP (Link-Layer Discovery Protocol)

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 6-54.

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 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).
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-54.

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 6-38)

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 6-54.

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 6-38).

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 6-38).
Configuring for Network Management Applications

LLDP (Link-Layer Discovery Protocol)

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 6-50). 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 6-49).

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 6-51).

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Configuration Options</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time-to-Live</td>
<td>See note 1.</td>
<td>120 Seconds</td>
<td>The length of time an LLDP neighbor retains the advertised data before discarding it.</td>
</tr>
<tr>
<td>Chassis Type(^a,b)</td>
<td>N/A</td>
<td>Always Enabled</td>
<td>Indicates the type of identifier used for Chassis ID.</td>
</tr>
<tr>
<td>Chassis ID(^b)</td>
<td>N/A</td>
<td>Always Enabled</td>
<td>Uses base MAC address of the switch.</td>
</tr>
<tr>
<td>Port Type(^3,b)</td>
<td>N/A</td>
<td>Always Enabled</td>
<td>Uses “Local”, meaning assigned locally by LLDP.</td>
</tr>
</tbody>
</table>
### Configuring for Network Management Applications

#### LLDP (Link-Layer Discovery Protocol)

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Configuration Options</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Id⁵</td>
<td>N/A</td>
<td>Always Enabled</td>
<td>Uses port number of the physical port. In the switches covered in this guide, this is an internal number reflecting the reserved port position in the chassis. For more information on this numbering scheme, refer to figures D-2 and D-3 in Appendix D, “MAC Address Management”.</td>
</tr>
<tr>
<td>Remote Management Address⁴⁄⁶</td>
<td>N/A</td>
<td>Always Enabled</td>
<td>Shows the network address type.</td>
</tr>
<tr>
<td>Type⁴⁄⁶</td>
<td>Default or Configured</td>
<td></td>
<td>Uses a default address selection method unless an optional address is configured. See “Remote Management Address” on page 6-40.</td>
</tr>
<tr>
<td>Address⁴</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Name⁶</td>
<td>Enable/Disable</td>
<td>Enabled</td>
<td>Uses the switch’s assigned name.</td>
</tr>
<tr>
<td>System Description⁶</td>
<td>Enable/Disable</td>
<td>Enabled</td>
<td>Includes switch model name and running software version, and ROM version.</td>
</tr>
<tr>
<td>Port Description⁶</td>
<td>Enable/Disable</td>
<td>Enabled</td>
<td>Uses the physical port identifier.</td>
</tr>
<tr>
<td>System capabilities supported⁶</td>
<td>Enable/Disable</td>
<td>Enabled</td>
<td>Identifies the switch’s primary capabilities (bridge, router).</td>
</tr>
<tr>
<td>System capabilities enabled⁶</td>
<td>Enable/Disable</td>
<td>Enabled</td>
<td>Identifies the primary switch functions that are enabled, such as routing.</td>
</tr>
</tbody>
</table>

¹The Packet Time-to-Live value is included in LLDP data packets. (Refer to “Changing the Time-to-Live for Transmitted Advertisements” on page 6-47.)
²Subelement of the Chassis ID TLV.
³Subelement of the Port ID TLV.
⁴Subelement of the Remote-Management-Address TLV.
⁵Subelement of the System Capability TLV.
⁶Populated 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 6-41.

**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 6-42).
- 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 the 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 6-54.)

LLDP Operating Rules

(For additional information specific to LLDP-MED operation, refer to “LLDP-MED (Media-Endpoint-Discovery)” on page 6-54.)

**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...
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-51). (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 6-54.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lldp config</td>
<td>6-45</td>
</tr>
<tr>
<td>[no] lldp run</td>
<td>6-46</td>
</tr>
<tr>
<td>lldp refresh-interval</td>
<td>6-46</td>
</tr>
<tr>
<td>lldp holdtime-multiplier</td>
<td>6-47</td>
</tr>
<tr>
<td>lldpTxDelay</td>
<td>6-47</td>
</tr>
<tr>
<td>lldpReinitDelay</td>
<td>6-48</td>
</tr>
<tr>
<td>lldp enable-notification</td>
<td>6-49</td>
</tr>
<tr>
<td>lldp notificationinterval</td>
<td>6-50</td>
</tr>
<tr>
<td>lldp admin-status &lt; txonly</td>
<td>rxonly</td>
</tr>
<tr>
<td>lldp config &lt; port-list &gt; IpAddrEnable</td>
<td>6-51</td>
</tr>
<tr>
<td>lldp config &lt; port-list &gt; basicTlvEnable</td>
<td>6-52</td>
</tr>
<tr>
<td>lldp config &lt; port-list &gt; dot3TlvEnable &lt; macphy_config &gt;</td>
<td>6-53</td>
</tr>
</tbody>
</table>

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 6-50.

For example, **show lldp config** produces the following display when the switch is in the default LLDP configuration:
### Configuring for Network Management Applications

**LLDP (Link-Layer Discovery Protocol)**

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

LLDP Global Configuration

- 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 Port Configuration

<table>
<thead>
<tr>
<th>Port</th>
<th>AdminStatus</th>
<th>NotificationEnabled</th>
<th>Med Topology</th>
<th>Trap Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tx_Rx</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tx_Rx</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Tx_Rx</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Tx_Rx</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Tx_Rx</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Tx_Rx</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Tx_Rx</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Tx_Rx</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: This value corresponds to the `lldp refresh-interval` command (page 6-46).

Figure 6-17. Example of Viewing the General LLDP Configuration
```
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-49. For information on the other configurable settings displayed by this command, refer to “Configuring Per-Port Transmit and Receive Modes” on page 6-50.

```
HP Switch(config)# show lldp config 1
LLDP Port Configuration Detail
Port: 1
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

IpAddress Advertised:
```

These fields appear when medtlvenable is enabled on the switch, which is the default setting.

This field appears when dot3tlvenable is enabled on the switch, which is the default setting.

The blank IpAddress field indicates that the default IP address will be advertised from this port. (Refer to page 6-51: “Configuring a Remote Management Address for Outbound LLDP Advertisements”)

**Figure 6-18. 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 \((4 \times \text{delay-interval})\). (The default delay-interval is 2). For example, with the default delay-interval, the lowest refresh-interval you can use is 8 seconds \((4 \times 2 = 8)\). Thus, if you want a refresh-interval of 5 seconds, you must first change the delay interval to 1 (that is, \(4 \times 1 < 5\)). If you want to change the delay-interval, use the setmib command.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

**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).

```
HP Switch(config)# setmib lldpTxDelay.0 -i B
lldpTxDelay.0: Inconsistent value.
HP Switch(config)# lldp refresh-interval 32
HP Switch(config)# setmib lldpTxDelay.0 -i B
lldpTxDelay.0 = 8
```

**Figure 6-19. 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 6-15.

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 for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-70.

**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 switch
- SNMP Power over Ethernet (PoE) status and troubleshooting support
- 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
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

Figure 6-20. Example of LLDP-MED Network Elements

**LLDP-MED Endpoint Support.** LLDP-MED on the switches covered in this guide inter-operates 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
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)

LLDP-MED operation also requires the port speed and duplex TLV (**dot3TlvEnable; page 6-53**), 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.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-75.)
- the LLDP-MED class of the device detected on the port (“LLDP-MED Endpoint Device Classes” on page 6-56.)

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 6-15.

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.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-62**
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 6-53.

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 >`
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-62.)
  - 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.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-59

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.
**Configuring for Network Management Applications**

**LLDP (Link-Layer Discovery Protocol)**

**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 6-70.

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 3, “Power Over Ethernet (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
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

- **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 > . . . ]
```

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](http://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—
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 6-4 on page 6-66.

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.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

Table 6-4. Some Location Codes Used in CA-TYPE Fields*

<table>
<thead>
<tr>
<th>Location Element</th>
<th>Code</th>
<th>Location Element</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>national subdivision</td>
<td>1</td>
<td>street number</td>
<td>19</td>
</tr>
<tr>
<td>regional subdivision</td>
<td>2</td>
<td>additional location data</td>
<td>22</td>
</tr>
<tr>
<td>city or township</td>
<td>3</td>
<td>unit or apartment</td>
<td>26</td>
</tr>
<tr>
<td>city subdivision</td>
<td>4</td>
<td>floor</td>
<td>27</td>
</tr>
<tr>
<td>street</td>
<td>6</td>
<td>room number</td>
<td>28</td>
</tr>
<tr>
<td>street suffix</td>
<td>18</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*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:

<table>
<thead>
<tr>
<th>Description</th>
<th>CA-Type</th>
<th>CA-VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>national subdivision</td>
<td>1</td>
<td>CA</td>
</tr>
<tr>
<td>city</td>
<td>3</td>
<td>Widgitville</td>
</tr>
<tr>
<td>street</td>
<td>6</td>
<td>Main</td>
</tr>
<tr>
<td>street number</td>
<td>19</td>
<td>1433</td>
</tr>
<tr>
<td>unit</td>
<td>26</td>
<td>Suite 4-N</td>
</tr>
<tr>
<td>floor</td>
<td>27</td>
<td>4</td>
</tr>
<tr>
<td>room number</td>
<td>28</td>
<td>N4-3</td>
</tr>
</tbody>
</table>
Configuring for Network Management Applications

LLDP (Link-Layer Discovery Protocol)

Figure 6-21 shows the commands for configuring and displaying the data.

```
HP Switch(config)# lldp config 2 medportlocation civic-addr US 2 1 CA 3 Widgitville 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 6-21. Example of a Civic Address Configuration

Displaying Advertisement Data

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lldp info local-device</td>
<td>below</td>
</tr>
<tr>
<td>walkmib lldpXdot3LocPortOperMauType</td>
<td></td>
</tr>
<tr>
<td>show lldp info remote-device</td>
<td>6-70</td>
</tr>
<tr>
<td>walkmib lldpXdot3RemPortAutoNegAdvertisedCap</td>
<td></td>
</tr>
<tr>
<td>show lldp info stats</td>
<td>6-72</td>
</tr>
</tbody>
</table>
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-22 on page 6-69.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

Figure 6-22. Example of Displaying the Global and Per-Port Information Available for Outbound Advertisements

```
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-E2520G-24-PoE
System Description : HP J9562A Switch, revision A.15.XX
System Capabilities Supported:bridge
System Capabilities Enabled:bridge

Management Address :
  Type:ipv4
  Address:

LLDP Port Information

<table>
<thead>
<tr>
<th>Port</th>
<th>PortType</th>
<th>PortId</th>
<th>PortDesc</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>local</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>local</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>local</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>local</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>local</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
```

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 6-40.

Figure 6-23. Example of the Default Per-Port Information Content for Ports 1 and 2

```
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
```

6-69
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-70.

**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 6-3 on page 6-39.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

Figure 6-24. Example of a Global Listing of Discovered Devices

```
HP Switch(config)# show lldp info remote

LLDP Remote Devices Information

<table>
<thead>
<tr>
<th>LocalPort</th>
<th>ChassisId</th>
<th>PortId</th>
<th>PortDescr</th>
<th>SysName</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00 11 85 35 3b 80</td>
<td>6</td>
<td>6</td>
<td>HP Switch 2650</td>
</tr>
<tr>
<td>2</td>
<td>00 11 85 cf 66 60</td>
<td>8</td>
<td>8</td>
<td>HP Switch 2650</td>
</tr>
</tbody>
</table>
```

Figure 6-25. Example of an LLDP-MED Listing of an Advertisement Received

```
HP Switch(config)# show lldp info remote-device 1

LLDP Remote Device Information Detail

Local Port : 1
ChassisType : mac-address
ChassisId   : 00 11 85 35 3b 80
PortType    : local
PortId      : 6
SysName     : HP Switch 2650
System Descr: HP J4899B Switch 2650, revision H.08.106, ROM H.08....
PortDescr   : 6

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

Remote Management Address
```
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-74.

Neighbor Entries AgeOut Count: Shows the number of LLDP neighbors dropped on all ports due to Time-to-Live expiring.

— Continued —
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

— 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 6-74. 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.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

Figure 6-26. Example of a Global LLDP Statistics Display

<table>
<thead>
<tr>
<th>Port</th>
<th>NumFramesRecvd</th>
<th>NumFramesSent</th>
<th>NumFramesDiscarded</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7301</td>
<td>7223</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>21</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>252</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>446</td>
<td>226</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Context: 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 6-27. 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.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

**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 6-47.

**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 (number) identity. To match the port’s external port number to the internal port number appearing in an SNMP trap, use the `walkmib ifDescr` command, as shown in the following figure:
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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:

```bash
HP Switch# walkmib ifDescr
ifDescr.1 = 1
ifDescr.2 = 2
ifDescr.3 = 3
.
.
ifDescr.23 = 23
ifDescr.24 = 24
```

Figure 6-28. Matching Internal Port Numbers to External Port Numbers
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

- 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.

<table>
<thead>
<tr>
<th>Protocol State</th>
<th>Packet Generation</th>
<th>Inbound Data Management</th>
<th>Inbound Packet Forwarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP Enabled¹</td>
<td>n/a</td>
<td>Store inbound CDP data.</td>
<td>No forwarding of inbound CDP packets.</td>
</tr>
<tr>
<td>CDP Disabled</td>
<td>n/a</td>
<td>No storage of CDP data from neighbor devices.</td>
<td>Floods inbound CDP packets from connected devices to outbound ports.</td>
</tr>
<tr>
<td>LLDP Enabled¹</td>
<td>Generates and transmits LLDP packets out all ports on the switch.</td>
<td>Store inbound LLDP data.</td>
<td>No forwarding of inbound LLDP packets.</td>
</tr>
<tr>
<td>LLDP Disabled</td>
<td>No packet generation.</td>
<td>No storage of LLDP data from neighbor devices.</td>
<td>No forwarding of inbound LLDP packets.</td>
</tr>
</tbody>
</table>
Configuring for Network Management Applications

LLDP (Link-Layer Discovery Protocol)

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.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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 6-29. Example of Show CDP with the Default CDP Configuration
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

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.

```plaintext
[[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.

```plaintext
[detai[[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 6-30 lists CDP devices that the switch has detected by receiving their CDP packets.

<table>
<thead>
<tr>
<th>Port</th>
<th>Device ID</th>
<th>Platform</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Accounting (0030c1-7fcc40)</td>
<td>J4812A HP Switch...</td>
<td>S</td>
</tr>
<tr>
<td>2</td>
<td>Research1-1 (0060b0-889e43)</td>
<td>J4121A HP Switch...</td>
<td>S</td>
</tr>
<tr>
<td>4</td>
<td>Support (0060b0_761a45)</td>
<td>J4121A HP Switch...</td>
<td>S</td>
</tr>
<tr>
<td>7</td>
<td>Marketing (0030c5_33dc59)</td>
<td>J4313A HP Switch...</td>
<td>S</td>
</tr>
<tr>
<td>12</td>
<td>Mgmt NIC (099a05-09df9b)</td>
<td>NIC Model X666</td>
<td>H</td>
</tr>
<tr>
<td>12</td>
<td>Mgmt NIC (099a05-09df11)</td>
<td>NIC Model X666</td>
<td>H</td>
</tr>
</tbody>
</table>

Figure 6-30. 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
```
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

MAC Limit Notification

The MAC Address Count feature provides a way to notify the switch management system when the number of MAC addresses learned on a switch port exceeds the permitted configurable number.

Configuring the MAC Address Count Option

To enable the `mac-count-notify` option, enter this command in global config context.

```
Syntax:  [no] snmp-server enable traps mac-count-notify
Sends a trap when the number of MAC addresses learned on the specified ports exceeds the configured `<learned-count>` value.
```

To configure the `mac-count-notify` option on a port or ports, enter this command. When the configured number of MAC addresses is exceeded (the `learned-count`), a trap is sent.

```
Syntax:  [no] mac-count-notify traps <port-list> [learned-count>
    Configures `mac-count-notify` traps on the specified ports (or all) for the entire switch.
    The `no` form of the command disables `mac-count-notify` traps.
    `<learned-count>`: The number of MAC addresses learned before sending a trap. Values range between 1-128.
    Default: 32
```

```
HP Switch(config)# mac-count-notify traps 5-7 50
```

**Figure 6-31. Configuring mac-count-notify traps on Ports 5-7**

Displaying Information About the `mac-count-notify` Option

Use the `show mac-count-notify traps [port-list]` command to display information about the configured value for sending a trap, the current count, and if a trap has been sent.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

HP Switch(config)# show mac-count-notify traps

Mac-count-notify Enabled : Yes

<table>
<thead>
<tr>
<th>Port</th>
<th>Count for sending Trap</th>
<th>Count</th>
<th>Trap Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>50</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>50</td>
<td>2</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>50</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 6-32. Example of Information Displayed for show mac-count-notify traps Command

The interface context can be used to configure the value for sending a trap.

HP Switch(config)# interface 5
HP Switch(eth-5)# mac-count-notify traps 35

Figure 6-33. Example of Configuring mac-count-notify traps from the Interface Context

The show snmp-server traps command displays whether the MAC Address Count feature is enabled or disabled.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

Figure 6-34. Example of Information About SNMP Traps, Including MAC Address Count Being Enabled/Disabled

The notify option is enabled.

MAC Address Table Change Notification

When enabled, this feature allows the generation of SNMP traps for each MAC address table change. Notifications can be generated for each device that connects to a port and for devices that are connected through another device (daisy-chained).

Configuring the MAC Address Table Change Option

The `snmp-server enable traps mac-notify` command globally enables the generation of SNMP trap notifications upon MAC address table changes.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

Syntax: [no] snmp-server enable traps mac-notify [mac-move | trap-interval <0-120>]

Globally enables or disables generation of SNMP trap notifications.

trap-interval: The time interval (in seconds) that trap notifications are sent. A value of zero disables the interval and traps are sent as events occur. If the switch is busy, notifications can be sent prior to the configured interval. Notifications may be dropped in extreme instances and a system warning is logged.

The range is 0-120 seconds. Default: 30 seconds.

mac-move: Configures the switch to capture data for MAC addresses that are moved from one port to another port. The snmp-server enable traps mac-notify command must have been enabled in order for this information to be sent as an SNMP notification.

Switch(config)# snmp-server enable traps mac-notify trap-interval 60

Figure 6-35. Example of trap-interval Option

Switch(config)# snmp-server enable traps mac-notify mac-move

Figure 6-36. Example of mac-move Option

Additional mac-notify Options for Per-Port MAC Changes

Use the following command to configure SNMP traps for learned or removed MAC addresses on a per-port basis.

Note

The switch will capture learned or removed events on the selected ports, but will not send an SNMP trap unless mac-notify has been enabled with the snmp-server enable traps mac-notify command.
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

Syntax:  [no] mac-notify traps <port-list> [learned | removed]

When this command is executed without the learned or removed option, it enables or disables the capture of both learned and removed MAC address table changes for the selected ports in <port-list>.

<port-list>: Configures MAC address table changes capture on the specified ports. Use all to capture changes for all ports on the switch.

learned: Enables the capture of learned MAC address table changes on the selected ports.

removed: Enables the capture of removed MAC address table changes on the selected ports.

Switch(config)# mac-notify traps 5-6 learned
Switch(config)# show mac-notify traps 5-6

Mac Notify Trap Information
Mac-notify Enabled : Yes
Mac-move Enabled : Yes
Trap-interval : 60

Port   MAC Addresses trap learned/removed
------- -------------------------------
5      Learned
6      Learned

Figure 6-37. Example of Configuring Traps on a Per-Port Basis for Learned MAC Addresses
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

Figure 6-38. Example of Configuring Traps on a Per-Port Basis for Removed MAC Addresses

Configuring the mac-notify Option at the Interface Context Level

You can also execute the `mac-notify traps` command from the interface context.

```
Switch(config)# int 11
Switch(int-11)# mac-notify traps learned
```

Figure 6-39. Example of the Interface Context for mac-notify traps Command

Displaying the mac-notify Traps Configuration Information

Use the `show mac-notify traps` command to display information about SNMP trap configuration for MAC Address Table changes.

**Syntax:**
```
show mac-notify traps [port-list]
```

*Displays SNMP trap information for all ports, or each port in the port-list.*
Configuring for Network Management Applications
LLDP (Link-Layer Discovery Protocol)

Figure 6-40. Example of Information for SNMP Trap Configuration

The configured **mac-notify** commands are displayed in the **show running-configuration** output.

Example of Running Config File With mac-notify Parameters Configured
File Transfers

Overview

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, and upload command files for configuring Access Control Lists (ACLs). It contains the following information:

- Downloading switch software (begins on this page)
- Copying software images (page A-21)
- Transferring switch configurations (begins on page A-22)
- Uploading ACL command files (begins on page A-26)
- Copying diagnostic data (begins on page A-29)

---

Downloading Switch Software

HP periodically provides switch software updates through the HP Networking 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:

<table>
<thead>
<tr>
<th>Software Download Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP</td>
<td>n/a</td>
<td>page A-3</td>
<td>page A-5</td>
<td>—</td>
</tr>
<tr>
<td>Xmodem</td>
<td>n/a</td>
<td>page A-15</td>
<td>page A-16</td>
<td>—</td>
</tr>
<tr>
<td>Switch-to-Switch</td>
<td>n/a</td>
<td>page A-18</td>
<td>page A-19</td>
<td>—</td>
</tr>
<tr>
<td>Software Update Manager in PCM+</td>
<td>Refer to the documentation provided with PCM+</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
File Transfers
Downloading Switch Software

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-21.

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-85.

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 Networking web site at [www.hp.com/networking/support](http://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)](image)

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 following screen then appears:

![Figure A-2. Example of the Download OS (Software) Screen During a Download](image)
File Transfers
Downloading Switch Software

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 [5] (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.

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](image)

Press any key to continue.
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-34.
- 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 HP website.

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.
File Transfers
Downloading Switch Software

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:

   ```
   HP Switch# copy tftp flash 10.28.227.103 k0800.swi
   The primary OS Image will be deleted, continue [y/n]? y
   01431K
   Dynamic counter continually displays the number of bytes transferred.
   This message means that the image you want to upload will replace the image currently in primary flash.
   ```

   **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.*

4. To confirm that the software downloaded correctly, execute **show system** and check the Firmware revision line.

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).
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.
File Transfers
Downloading Switch Software

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.
File Transfers
Downloading Switch Software

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 15.22.22.03

- 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
\---core
  |   port_1-24.core  core-dump for ports 1-24 (stackable switches only)
  |   port_25-48.core core-dump for ports 25-48 (stackable switches only)
```

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
ssh: sftp session from ::ffff:10.0.12.35 W 01/01/90 00:06:26
sftp read error Bad file number, session aborted I 01/01/90 00:09:54
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
```
File Transfers
Downloading Switch Software

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
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.

4. To confirm that the software downloaded correctly:

   Switch> show system

   Check the Firmware revision line. It should show the software version that you downloaded in the preceding steps.

**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 [5] (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 <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:

```
HP Switch# copy tftp flash 10.29.227.13 flash
Device will be rebooted, do you want to continue [y/n]? y
00107K
```

![Figure A-7. Switch-To-Switch, from Primary in Source to Either Flash in Destination](image)
File Transfers
Downloading Switch Software

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:

```bash
HP Switch# copy tftp flash 10.29.227.13 flash /os/secondary secondary
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 PCM+ to Update Switch Software

PCM+ 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.

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**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use TFTP to copy from a remote host to a config file.</td>
<td>A-23</td>
</tr>
<tr>
<td>Use TFTP to copy a config file to a remote host.</td>
<td>A-24</td>
</tr>
<tr>
<td>Use Xmodem to copy a configuration from a serially connected host to a config file.</td>
<td>A-24</td>
</tr>
<tr>
<td>Use Xmodem to copy a config file to a serially connected host.</td>
<td>A-25</td>
</tr>
</tbody>
</table>

Using the CLI commands described in this section, you can copy switch configurations to and from a switch, or copy a software image to configure or replace an ACL in the switch configuration.

**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 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 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`. 

---

A-23
File Transfers
Transferring Switch Configurations

If no custom file is found, a message displays stating “No SHOW-TECH file found.”

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 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 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. To do so, use one of the following commands:

Syntax: boot system flash [ primary | secondary ]
        boot system flash [ config < filename >

Switches boot from the designated configuration file.

Syntax: reload

Reboots from the flash image currently in use.
Transferring ACL Command Files

This section describes how to upload and execute a command file to the switch for configuring or replacing an Access Control List (ACL) in the switch configuration. Such files should contain only ACE (Access Control Entry) commands. For more on this general topic, including an example of an ACL command file created offline, refer to the section titled “Editing ACLs and Creating an ACL Offline” in the “Access Control Lists (ACLs)” chapter of the latest Access Security Guide for your switch.

TFTP: Uploading an ACL Command File from a TFTP Server

Syntax: copy tftp command-file < ip-addr > < filename.txt > < unix | pc >

where:

- `<ip-addr>` = The IP address of a TFTP server available to the switch
- `<filename.txt>` = A text file containing ACL commands and stored in the TFTP directory of the server identified by `<ip-addr>`
- `<unix | pc>` = The type of workstation used for serial, Telnet, or SSH access to the switch CLI

This command copies and executes the named text file from the specified TFTP server address and executes the ACL commands in the file. Depending on the ACL commands used, this action does one of the following in the running-config file:

- Creates a new ACL.
- Replaces an existing ACL. (Refer to “Creating an ACL Offline” in the “Access Control Lists (ACLs)” chapter in the latest Access Security Guide for your switch.)
- Adds to an existing ACL.

For example, suppose you:

1. Created an ACL command file named `vlan10_in.txt` to update an existing ACL.
2. Copied the file to a TFTP server at 18.38.124.16.
Using a PC workstation, you then execute the following from the CLI to upload the file to the switch and implement the ACL commands it contains:

```
HP Switch(config)# copy tftp command-file 18.38.124.16 vlan10_in.txt pc
```

The switch displays this message:

```
Running configuration may change, do you want to continue [y/n]?
```

To continue with the upload, press the [Y] key. To abort the upload, press the [N] key. Note that if the switch detects an illegal (non-ACL) command in the file, it bypasses the illegal command, displays a notice as shown in figure A-11, and continues to implement the remaining ACL commands in the file.

```
HP Switch(config)# copy tftp command-file 10.38.124.18 vlan10_in.txt pc
Running configuration may change, do you want to continue [y/n]? y
1. ip access-list extended "155"
2. deny tcp 0.0.0.0 255.255.255.255 10.10.10.2 0.0.0.0 eq 23 log
3. permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
4. show running
Command files are limited to access-list commands.
5. exit
HP Switch(config)# show running
Running configuration:
```
hostname "HP-E2520G-24-PoE"
cdp run
ip default-gateway 10.38.248.1
logging 10.38.227.2
snmp-server community "public" unrestricted
ip access-list extended "155"
deny tcp 0.0.0.0 255.255.255.255 10.10.10.2 0.0.0.0 eq 23 log
permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit
```

Figure A-11. Example of Using the Copy Command to Download and Configure an ACL
Xmodem: Uploading an ACL Command File from a Serially Connected PC or UNIX Workstation

Syntax: copy xmodem command-file < unix | pc >

Uses Xmodem to copy and executes an ACL command from a PC or Unix workstation. Depending on the ACL commands used, this action does one of the following in the running-config file:

- Creates a new ACL.
- Replaces an existing ACL. (Refer to “Creating an ACL Offline” in the “Access Control Lists (ACLs)” chapter in the latest Access Security Guide for your switch.)
- Adds to an existing ACL.
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.*
File Transfers
Copying Diagnostic Data to a Remote Host, PC or UNIX Workstation

For example, to use Xmodem to copy the output of show config to a serially connected PC:

```
HP Switch(config)# copy command-output "show config" xmodem pc
Press 'Enter' and start XMODEM on your host...
Transfer complete
```

Figure A-12. 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 | sftp | xmodem>
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:

```
HP Switch(config)# copy event-log xmodem pc
Press 'Enter' and start XMODEM on your host...
Transfer complete
```

Figure A-13. 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:

```
At this point, press [Enter] and start the Xmodem command sequence in your terminal emulator.

HP Switch(config)# copy crash-data xmodem pc
Press 'Enter' and start XMODEM on your host...
Transfer complete
```

**Figure A-14. Example of Copying Switch Crash Data Content to a PC**

Copying Crash Log 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 Crash Log to a file in a PC connected to the switch:

```
At this point, press [Enter] and start the Xmodem command sequence in your terminal emulator.

HP Switch(config)# copy crash-log xmodem
Press 'Enter' and start XMODEM on your host...
Transfer complete
```

**Figure A-15. Example of sending a Crash Log to a File on an Attached PC**
File Transfers
Copying Diagnostic Data to a Remote Host, PC or UNIX Workstation
Monitoring and Analyzing Switch Operation

Overview

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-8).
- **Event Log**: Lists switch operating events (“Using the Event Log for Troubleshooting Switch Problems” on page C-34).
- **Alert Log**: Lists network occurrences detected by the switch—in the Status | Overview screen of the WebAgent.
- **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 6-2.)
- **Port monitoring (mirroring)**: Copy all traffic from the specified ports to a designated monitoring port (page B-18).
- **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-66.

Status and Counters Data

This section describes the status and counters screens available through the switch console interface and/or the WebAgent.
Monitoring and Analyzing Switch Operation
Status and Counters Data

**Note** You can access all console screens from the WebAgent via Telnet to the console. Telnet access to the switch is available in the Device View window under the **Configuration** tab.

<table>
<thead>
<tr>
<th>Status or Counters Type</th>
<th>Interface</th>
<th>Purpose</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menu Access to Status and Counters</td>
<td>Menu</td>
<td>Access menu interface for status and counter data.</td>
<td>B-3</td>
</tr>
<tr>
<td>General System Information</td>
<td>Menu, CLI</td>
<td>Lists switch-level operating information.</td>
<td>B-3</td>
</tr>
<tr>
<td>Management Address Information</td>
<td>Menu, CLI</td>
<td>Lists the MAC address, IP address, and IPX network number for each VLAN or, if no VLANs are configured, for the switch.</td>
<td>B-6</td>
</tr>
<tr>
<td>Port Status</td>
<td>Menu, CLI,</td>
<td>Displays the operational status of each port.</td>
<td>B-7</td>
</tr>
<tr>
<td>Port Address Table</td>
<td>Menu, CLI,</td>
<td>Summarizes port activity and lists per-port flow control status.</td>
<td>B-8</td>
</tr>
<tr>
<td>Port and Trunk Statistics and Flow Control Status</td>
<td>Menu, CLI,</td>
<td></td>
<td>B-8</td>
</tr>
<tr>
<td>VLAN Information</td>
<td>Menu, CLI</td>
<td>Lists the MAC addresses of nodes the switch has detected on specific VLANs, with the corresponding switch port.</td>
<td>B-11</td>
</tr>
<tr>
<td>VLAN Information</td>
<td>Menu, CLI</td>
<td>Lists the MAC addresses that the switch has learned from the selected port.</td>
<td>B-11</td>
</tr>
<tr>
<td>IGMP Status</td>
<td>Menu, CLI</td>
<td>Lists IGMP groups, reports, queries, and port on which querier is located.</td>
<td>B-16</td>
</tr>
<tr>
<td>STP Information</td>
<td>Menu, CLI</td>
<td>Lists Spanning Tree Protocol data for the switch and for individual ports. If VLANs are configured, reports on a per-VLAN basis.</td>
<td>B-15</td>
</tr>
<tr>
<td>VLAN Information</td>
<td>Menu, CLI</td>
<td>For each VLAN configured in the switch, lists 802.1Q VLAN ID and up/down status.</td>
<td>B-16</td>
</tr>
</tbody>
</table>
Menu Access To Status and Counters

Beginning at the Main Menu, display the Status and Counters menu by selecting:

1. Status and Counters

![Status and Counters Menu](image)

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
Monitoring and Analyzing Switch Operation
Status and Counters Data

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.
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*
Monitoring and Analyzing Switch Operation
Status and Counters Data

Figure B-4. Example of the task-monitor cpu Command and show cpu Output

```
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
```

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

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>MAC Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>00:01:e7-00:90:08</td>
<td>16.29.227.101</td>
</tr>
<tr>
<td>VLAN-52</td>
<td>00:01:e7-00:90:08</td>
<td>Disabled</td>
</tr>
<tr>
<td>VLAN-53</td>
<td>00:01:e7-00:90:08</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

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.
Monitoring and Analyzing Switch Operation
Status and Counters Data

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 WebAgent 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
Monitoring and Analyzing Switch Operation
Status and Counters Data

Figure B-6. Example of Port Status on the Menu Interface

CLI Access

Syntax:
show interfaces brief

Viewing Port and Trunk Group Statistics and Flow Control Status

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>viewing port and trunk statistics for all ports, and flow control status</td>
<td>n/a</td>
<td>page B-9</td>
<td>page B-10</td>
</tr>
<tr>
<td>viewing a detailed summary for a particular port or trunk</td>
<td>n/a</td>
<td>page B-9</td>
<td>page B-10</td>
</tr>
<tr>
<td>resetting counters</td>
<td>n/a</td>
<td>page B-9</td>
<td>page B-10</td>
</tr>
</tbody>
</table>

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.
Monitoring and Analyzing Switch Operation
Status and Counters Data

The menu interface and the WebAgent 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

<table>
<thead>
<tr>
<th>Port</th>
<th>Total Bytes</th>
<th>Total Frames</th>
<th>Errors Rx</th>
<th>Drops Tx</th>
<th>Flow Ctrl</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>192,972</td>
<td>323</td>
<td>0</td>
<td>0</td>
<td>off</td>
</tr>
<tr>
<td>A2</td>
<td>659,316</td>
<td>671</td>
<td>0</td>
<td>0</td>
<td>off</td>
</tr>
<tr>
<td>A3-Port1</td>
<td>296,163</td>
<td>503</td>
<td>0</td>
<td>0</td>
<td>off</td>
</tr>
<tr>
<td>A4-Port1</td>
<td>286,134</td>
<td>501</td>
<td>0</td>
<td>0</td>
<td>off</td>
</tr>
<tr>
<td>C1</td>
<td>859,363</td>
<td>514</td>
<td>0</td>
<td>0</td>
<td>off</td>
</tr>
<tr>
<td>C2</td>
<td>674,574</td>
<td>1693</td>
<td>0</td>
<td>0</td>
<td>off</td>
</tr>
<tr>
<td>C3</td>
<td>26,554</td>
<td>246</td>
<td>0</td>
<td>0</td>
<td>off</td>
</tr>
<tr>
<td>C4</td>
<td>119,184</td>
<td>276</td>
<td>0</td>
<td>0</td>
<td>off</td>
</tr>
</tbody>
</table>

Actions: Back Show details Reset Help

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.
Monitoring and Analyzing Switch Operation
Status and Counters Data

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-9.)

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-9.)*
To reset the port counters to zero, you must reboot the switch.

Viewing the Switch’s MAC Address Tables

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>viewing MAC addresses on all ports on a specific VLAN</td>
<td>n/a</td>
<td>page B-11</td>
<td>page B-14</td>
</tr>
<tr>
<td>viewing MAC addresses on a specific port</td>
<td>n/a</td>
<td>page B-13</td>
<td>page B-14</td>
</tr>
<tr>
<td>searching for a MAC address</td>
<td>n/a</td>
<td>page B-13</td>
<td>page B-14</td>
</tr>
</tbody>
</table>

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.

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:
Monitoring and Analyzing Switch Operation
Status and Counters Data

---
CONSOL...E ADDRESS MODE --
Status and Counters - Address Table

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Located on Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>000001-123456</td>
<td>A1</td>
</tr>
<tr>
<td>000001-678901</td>
<td>A2</td>
</tr>
<tr>
<td>000001-908765</td>
<td>A3</td>
</tr>
</tbody>
</table>

Actions=> Jack  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

![Prompt for Selecting the Port To Search]

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.**

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:

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:

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 : 080009-21ae84
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

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Cost</th>
<th>Prio</th>
<th>Designated Bridge</th>
<th>Hello Time</th>
<th>PtP</th>
<th>Edge</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 100/1000T</td>
<td>Auto</td>
<td>128</td>
<td>Forwarding</td>
<td>000883-028300 9</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>2 100/1000T</td>
<td>Auto</td>
<td>128</td>
<td>Blocked</td>
<td>0001e7-948300 9</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>3 100/1000T</td>
<td>Auto</td>
<td>128</td>
<td>Forwarding</td>
<td>000883-02a700 2</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>4 100/1000T</td>
<td>Auto</td>
<td>128</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure B-12. Output from show spanning-tree Command
Monitoring and Analyzing Switch Operation
Status and Counters Data

Internet Group Management Protocol (IGMP) Status

The switch uses the CLI to display the following IGMP status on a per-VLAN basis:

<table>
<thead>
<tr>
<th>Show Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp</td>
<td>Global command listing IGMP status for all VLANs configured in the switch:</td>
</tr>
<tr>
<td></td>
<td>• VLAN ID (VID) and name</td>
</tr>
<tr>
<td></td>
<td>• Active group addresses per VLAN</td>
</tr>
<tr>
<td></td>
<td>• Number of report and query packets per group</td>
</tr>
<tr>
<td></td>
<td>• Querier access port per VLAN</td>
</tr>
<tr>
<td>show ip igmp &lt;vlan-id&gt;</td>
<td>Per-VLAN command listing above IGMP status for specified VLAN (VID)</td>
</tr>
<tr>
<td>show ip igmp group &lt;ip-addr&gt;</td>
<td>Lists the ports currently participating in the specified group, with port type, Access type, Age Timer data and Leave Timer data.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Show Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlan</td>
<td>Lists:</td>
</tr>
<tr>
<td></td>
<td>• Maximum number of VLANs to support</td>
</tr>
<tr>
<td></td>
<td>• Existing VLANs</td>
</tr>
<tr>
<td></td>
<td>• Status (static or dynamic)</td>
</tr>
<tr>
<td></td>
<td>• Primary VLAN</td>
</tr>
</tbody>
</table>
Monitoring and Analyzing Switch Operation
Status and Counters Data

For example, suppose that your switch has the following VLANs:

<table>
<thead>
<tr>
<th>Ports</th>
<th>VLAN</th>
<th>VLANID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-12</td>
<td>DEFAULT_VLAN</td>
<td>1</td>
</tr>
<tr>
<td>13-14</td>
<td>VLAN-33</td>
<td>33</td>
</tr>
<tr>
<td>15-20</td>
<td>VLAN-44</td>
<td>44</td>
</tr>
</tbody>
</table>

The next three figures show how you could list data on the above VLANs.

**Figure B-14. Example of VLAN Listing for the Entire Switch**

```
HP Switch(config)# show vlan
Status and Counters - VLAN Information

Maximum VLANs to support : 256
Primary VLAN : DEFAULT_VLAN
Management VLAN :

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>Status</th>
<th>Voice</th>
<th>Jumbo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Static</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>33</td>
<td>VLAN-33</td>
<td>Static</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>44</td>
<td>VLAN-44</td>
<td>Static</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```

**Figure B-15. Example of VLAN Listing for Specific Ports**

```
HP Switch(config)# show vlan ports 1-2
Status and Counters - VLAN Information - for ports 1,2

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>Status</th>
<th>Voice</th>
<th>Jumbo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Static</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>33</td>
<td>VLAN-33</td>
<td>Static</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```
Monitoring and Analyzing Switch Operation

Interface Monitoring Features

You can designate monitoring of inbound and outbound traffic on:

- **Ports and static trunks**: Allows monitoring of individual ports, groups of contiguous ports, and static port trunks.
- **Static VLANs**: Allows traffic monitoring on one static VLAN.

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

---

Figure B-16. Example of Port Listing for an Individual VLAN

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>display monitoring configuration</td>
<td>disabled</td>
<td>page B-19</td>
<td>page B-21</td>
</tr>
<tr>
<td>configure the monitor port(s)</td>
<td>ports: none</td>
<td>page B-19</td>
<td>page B-22</td>
</tr>
<tr>
<td>selecting or removing ports</td>
<td>none selected</td>
<td>page B-19</td>
<td>page B-23</td>
</tr>
</tbody>
</table>

---
Monitoring and Analyzing Switch Operation
Interface Monitoring Features

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-17. 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.
Monitoring and Analyzing Switch Operation
Interface Monitoring Features

Figure B-18. How To Select a Monitoring Port

5. Use the Space bar to select the port to use for monitoring.
6. Highlight the Monitor field and use the Space bar to select the interfaces to monitor:
   - **Ports**: Use for monitoring ports or static trunks.
   - **VLAN**: Use for monitoring a VLAN.
7. Do one of the following:
   - If you are monitoring ports or static trunks go to step 8.
   - If you are monitoring a VLAN:
     i. Press [Tab] or the down arrow key to move to the VLAN field.

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Action</th>
<th>Port</th>
<th>Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>10/100TX</td>
<td></td>
<td>A10</td>
<td>10/100TX</td>
<td></td>
</tr>
<tr>
<td>A2</td>
<td>10/100TX</td>
<td></td>
<td>A11</td>
<td>10/100TX</td>
<td></td>
</tr>
<tr>
<td>A3</td>
<td>10/100TX</td>
<td></td>
<td>A12</td>
<td>10/100TX</td>
<td></td>
</tr>
<tr>
<td>A4</td>
<td>10/100TX</td>
<td></td>
<td>A13</td>
<td>10/100TX</td>
<td></td>
</tr>
<tr>
<td>A5</td>
<td>10/100TX</td>
<td></td>
<td>A14</td>
<td>10/100TX</td>
<td></td>
</tr>
<tr>
<td>A6</td>
<td>10/100TX</td>
<td></td>
<td>A15</td>
<td>10/100TX</td>
<td></td>
</tr>
<tr>
<td>A7</td>
<td>10/100TX</td>
<td></td>
<td>A20</td>
<td>10/100TX</td>
<td></td>
</tr>
<tr>
<td>A8</td>
<td>10/100TX</td>
<td>Trk1 Trunk</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
ii. Use the Space bar to select the VLAN you want to monitor.

iii. Go to step 10.

8. 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.

9. 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.)

10. When you finish selecting ports to monitor, press **[Enter]**, then press **[S]** (for **Save**) to save your changes and exit from the screen.

11. Return to the Main Menu.

**CLI: Configuring Port and Static Trunk Monitoring**

**Port and Static Trunk Monitoring Commands Used in This Section**

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show monitor</td>
<td>B-22</td>
</tr>
<tr>
<td>mirror-port</td>
<td>B-22</td>
</tr>
<tr>
<td>monitor</td>
<td>B-23</td>
</tr>
</tbody>
</table>

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:
Monitoring and Analyzing Switch Operation
Interface Monitoring Features

Figure B-19. Example of Monitored Port Listing

Configuring the Monitor Port.

Syntax:  \texttt{[no]} mirror-port [<port-num>]

\textit{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:

\texttt{HP Switch(config)# mirror-port 6}

To turn off monitoring:

\texttt{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, static trunks, or VLANs as monitoring sources. You can also use either level to remove monitoring sources.

**Syntax:**

```
[no] interface < monitor-list > monitor
```

*< 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.

**Note**

Individual ports and static trunks can be monitored at the same time. However, if you configure the switch to monitor a VLAN, all other interfaces are removed from monitoring. Also, you can configure only one VLAN at a time for monitoring.

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
- Trunks 1 and 2

```
HP Switch(config)# int 6-9, 14 trk2, monitor
```

**Figure B-20. Examples of Selecting Ports and Static Trunks as Monitoring Sources**

To monitor a VLAN:

```
HP Switch(config)# vlan 20 monitor
```

```
HP Switch(config)# show monitor
Network Monitoring Port
  Mirror Port: 6
  Monitoring Sources:
    VLAN_20
```

**Figure B-21. Example of Configuring VLAN Monitoring**
Monitoring and Analyzing Switch Operation
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.

```plaintext
HP Switch(eth-1-3,5)# no int 5 monitor
HP Switch(eth-1-3,5)# no monitor

HP Switch(config)# no int 5 monitor
HP Switch(config)# no int 1-3,5 monitor

These two commands show how to disable monitoring at the interface context level for a single port or all ports in an interface context level.

These two commands show how to disable monitoring at the global config level for a single port or a group of ports.
```

Figure B-22. Examples of Removing Ports as Monitoring Sources

## 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.*

```plaintext
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
Monitoring and Analyzing Switch Operation
Locating a Device
Troubleshooting

Overview

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 Networking 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 Networking web site for software updates that may have solved your problem: www.hp.com/networking/support

- 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.
Troubleshooting
Browser or Telnet Access Problems

- 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 PCM to help isolate problems and recommend solutions.
- Use the Port Utilization Graph and Alert Log in the WebAgent included in the switch to help isolate problems. These tools are available through the WebAgent:
  - 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. 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 WebAgent:
- 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 WebAgent 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 WebAgent 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:

- Off subnet management stations can lose Telnet access if you enable routing without first configuring a static (default) route. That is, the switch uses the IP default gateway only while operating as a Layer 2 device. While routing is enabled on the switch, the IP default gateway is not used. You can avoid this problem by using the ip route command to configure a static (default) route before enabling routing. For more information, refer to the chapter titled “IP Routing Features” in the Multicast and Routing Guide for your switch.

- 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 PCM. 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.
Troubleshooting
Unusual Network Activity

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.

ACL Problems

ACLs are properly configured and assigned to VLANs, but the switch is not using the ACLs to filter IP layer 3 packets.

1. The switch may be running with IP routing disabled. To ensure that IP routing is enabled, execute `show running` and look for the IP routing statement in the resulting listing. For example:
Troubleshooting
Unusual Network Activity

Figure C-1. Indication that Routing Is Enabled

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname &quot;HPswitch&quot;</td>
<td>Indicates that routing is enabled; a requirement for ACL operation. (There is an exception. Refer to the Note, below.)</td>
</tr>
<tr>
<td>ip routing</td>
<td></td>
</tr>
<tr>
<td>ip default-gateway 10.33.248.1</td>
<td></td>
</tr>
<tr>
<td>logging 10.28.227.2</td>
<td></td>
</tr>
<tr>
<td>snmp-server community &quot;public&quot; Unrestricted</td>
<td></td>
</tr>
<tr>
<td>ip access-list extended &quot;Controls for VLAN 20&quot;</td>
<td></td>
</tr>
<tr>
<td>permit tcp 0.0.0.0 255.255.255.255 10.10.20.98 0.0.0.0 eq 80</td>
<td></td>
</tr>
<tr>
<td>permit tcp 0.0.0.0 255.255.255.255 10.10.20.21 0.0.0.0 eq 80</td>
<td></td>
</tr>
<tr>
<td>deny tcp 0.0.0.0 255.255.255.255 10.10.20.1 0.0.0.255 eq 80</td>
<td></td>
</tr>
<tr>
<td>deny tcp 10.10.20.1? 0.0.0.0 10.10.10.100 0.0.0.0 eq 20 log</td>
<td></td>
</tr>
<tr>
<td>deny tcp 10.10.20.20 0.0.0.0 10.10.10.100 0.0.0.0 eq 20 log</td>
<td></td>
</tr>
<tr>
<td>deny tcp 10.10.20.43 0.0.0.0 10.10.10.100 0.0.0.0 eq 20 log</td>
<td></td>
</tr>
<tr>
<td>permit ip 10.10.20.1 0.0.0.255 10.10.10.100 0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>deny ip 10.10.30.1 0.0.0.255 10.10.10.100 0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>permit ip 10.10.30.1 0.0.0.255 10.10.10.1 0.0.0.255</td>
<td></td>
</tr>
</tbody>
</table>

Note

If an ACL assigned to a VLAN includes an ACE referencing an IP address on the switch itself as a packet source or destination, the ACE screens traffic to or from this switch address regardless of whether IP routing is enabled. This is a security measure designed to help protect the switch from unauthorized management access.

If you need to configure IP routing, execute the `ip routing` command.

2. ACL filtering on the switches covered in this guide applies only to routed packets and packets having a destination IP address (DA) on the switch itself. Also, the switch applies assigned ACLs only at the point where traffic enters or leaves the switch on a VLAN. Ensure that you have correctly applied your ACLs (“in” and/or “out”) to the appropriate VLAN(s).

The switch does not allow management access from a device on the same VLAN.

The implicit `deny any` function that the switch automatically applies as the last entry in any ACL always blocks packets having the same DA as the switch’s IP address on the same VLAN. That is, bridged packets with the switch itself...
as the destination are blocked as a security measure. To preempt this action, edit the ACL to include an ACE that permits access to the switch’s DA on that VLAN from the management device.

**Error (Invalid input) when entering an IP address.**

When using the “host” option in the command syntax, ensure that you are not including a mask in either dotted decimal or CIDR format. Using the “host” option implies a specific host device and therefore does not permit any mask entry.

```
HP Switch(config)# access-list 6 permit host 10.28.100.100  Correct.
HP Switch(config)# access-list 6 permit host 10.28.100.100 255.255.255.255  Incorrect. No mask needed to specify a single host.
HP Switch(config)# access-list 6 permit host 10.28.100.100/32  Invalid input: 10.28.100.100/32
```

**Figure C-2. Examples of Correctly and Incorrectly Specifying a Single Host**

Apparent failure to log all “Deny” Matches.

Where the `log` statement is included in multiple ACEs configured with a “deny” option, a large volume of “deny” matches generating logging messages in a short period of time can impact switch performance. If it appears that the switch is not consistently logging all “deny” matches, try reducing the number of logging actions by removing the `log` statement from some ACEs configured with the “deny” action.

The switch does not allow any routed access from a specific host, group of hosts, or subnet.

The implicit `deny any` function that the switch automatically applies as the last entry in any ACL may be blocking all access by devices not specifically permitted by an entry in an ACL affecting those sources. If you are using the ACL to block specific hosts, a group of hosts, or a subnet, but want to allow any access not specifically permitted, insert `permit any` as the last explicit entry in the ACL.

The switch is not performing routing functions on a VLAN

Two possible causes of this problem are:

- Routing is not enabled. If `show running` indicates that routing is not enabled, use the `ip routing` command to enable routing.
Troubleshooting
Unusual Network Activity

- On a switch covered in this guide, an ACL may be blocking access to the VLAN. Ensure that the switch’s IP address on the VLAN is not blocked by one of the ACE entries in an ACL applied to that VLAN. A common mistake is to either not explicitly permit the switch’s IP address as a DA or to use a wildcard ACL mask in a deny statement that happens to include the switch’s IP address. For an example of this problem, refer to the section titled “General ACL Operating Notes” in the “Access Control Lists (ACLs)” chapter of the latest Access Security Guide for your switch.

Routing Through a Gateway on the Switch Fails

Configuring a “deny” ACE that includes a gateway address can block traffic attempting to use the gateway as a next-hop.

Remote Gateway Case. For example, configuring ACL “101” (below) and applying it outbound on VLAN 1 in Figure C-4 includes the router gateway (10.0.8.1) needed by devices on other networks. This can prevent the switch from sending ARP and other routing messages to the gateway router to support traffic from authorized remote networks.

```plaintext
In Figure C-4, this ACE denies access to the 10 Net’s 10.0.8.1 router gateway needed by the 20 Net. (Subnet mask is 255.255.255.0.)

HP Switch(config)# access-list config
ip access-list extended "101"
   deny ip 0.0.0.0 255.255.255.255 10.0.8.30 0.0.0.255
   permit ip 0.0.0.0 255.255.255.255 0.0.0.00 255.255.255.255
exit
```

Figure C-3. Example of ACE Blocking an Entire Subnet
Troubleshooting
Unusual Network Activity

To avoid inadvertently blocking the remote gateway for authorized traffic from another network (such as the 20 Net in this example):

1. Configure an ACE that specifically permits authorized traffic from the remote network.
2. Configure narrowly defined ACEs to block unwanted IP traffic that would otherwise use the gateway. Such ACEs might deny traffic for a particular application, particular hosts, or an entire subnet.
3. Configure a “permit any” ACE to specifically allow any IP traffic to move through the gateway.

Local Gateway Case. If you use the switch as a gateway for traffic you want routed between subnets, use these general steps to avoid blocking the gateway for authorized applications:

1. Configure gateway security first for routing with specific permit and deny statements.
2. Permit authorized traffic.
3. Deny any unauthorized traffic that you have not already denied in step 1.
Troubleshooting
Unusual Network Activity

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 WebAgent:** If you can access the WebAgent, 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, HP recommends that you either disable the port or disconnect it from the LAN.
Port-Based Access Control (802.1X)-Related Problems

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-14.

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.
Troubleshooting
Unusual Network Activity

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
Access Authenticator Authentication
Port Status Control State Backend State
----- ------ -------- -------------- --------------
9  Open   FU       Force Auth     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.

```
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] : Yes
Access Authenticator Authentication
Port Status Control State Backend State
----- ------ -------- -------------- --------------
9  Closed FU       Force Unauth     Idle
```

Figure C-5. 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
Troubleshooting
Unusual Network Activity

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.

```
HP Switch(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

  Server IP Addr  Port  Port  CoA  Window  Encryption Key
  -------------- ---- ---- ---- ------ ---------------
   10.33.18.119  1812 1813            119-only-key
```

Figure C-6. 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.
Troubleshooting
Unusual Network Activity

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.
Troubleshooting
Unusual Network Activity

Spanning-Tree Protocol (MSTP) and Fast-Uplink Problems

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.
Troubleshooting
Unusual Network Activity

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.
Troubleshooting
Unusual Network Activity

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.
Troubleshooting
Unusual Network Activity

VLAN-Related Problems

Monitor Port. When using the monitor port in a multiple VLAN environment, the switch handles broadcast, multicast, and unicast traffic output from the monitor port as follows:

- If the monitor port is configured for tagged VLAN operation on the same VLAN as the traffic from monitored ports, the traffic output from the monitor port carries the same VLAN tag.
- If the monitor port is configured for untagged VLAN operation on the same VLAN as the traffic from the monitored ports, the traffic output from the monitor port is untagged.
- If the monitor port is not a member of the same VLAN as the traffic from the monitored ports, traffic from the monitored ports does not go out the monitor port.

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-8. 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-9. Example of Duplicate MAC Address](image-url)

**Disabled Overlapping Subnet Configuration.** Previous software versions allowed configuration of VLAN IP addresses in overlapping subnets, which can cause incorrect routing of packets and result in IP communication failure. As of software version K.15.09, overlapping subnet configurations are no longer allowed. An overlapping subnet is determined by the configuration order. The subnet that is configured first is valid, but any subsequent IP addresses that overlap are not allowed.
Troubleshooting
Unusual Network Activity

When the switch is booted into software version K.15.09 or later, and the configuration file includes overlapping subnets, the following occurs:

- The event log provides an error message in the format:
  
ip: VLANx : IP initialization failed for vlan x.

  For a multinetted VLAN (multiple IP addresses assigned to the VLAN), only the IP addresses that are overlapping subnets are removed. The other IP addresses on the VLAN are retained and function correctly. The error message can be somewhat misleading; the IP addresses on the VLAN that are not overlapping are initialized correctly.

- The output of the `show ip` command correctly indicates that the overlapping IP address does not exist on the VLANs that have error messages in the event log.

- The output of the `show running-config` command incorrectly indicates that the overlapping IP address is configured. For example, in figure C-10, the IP address shown in VLAN6 is not actually configured on the VLAN; it has been removed.

```
HP Switch(config)# show running-config
.
.
vlan 5
  name "VLAN5"
  ip address 11.22.33.1 255.0.0.0
  exit
vlan 6
  name "VLAN6"
  ip address 11.23.34.1 255.255.255.0
  exit
```

**Figure C-10. Example of an IP Address that is not Actually Configured on the VLAN**

The information is retained in the config file to allow you to boot up the switch and have it function as it did when it was configured with earlier software that allows overlapping subnets.

If you attempt to remove the overlapping subnet from the VLAN, the switch displays an error message similar to:

The IP address <ip-address> is not configured on this VLAN
This occurs because the overlapping IP address has been removed and is not visible to the switch. To resolve this:

- Enter the `show ip` command to determine which addresses are visible to the switch.
- Remove the erroneous IP addresses from the config file by entering the `no ip address` command to remove all the IP addresses from the specific VLAN. Be sure to document the other valid IP addresses on that VLAN so they can be restored after removing the erroneous IP addresses from the config file.

If you go back to a software version prior to K.15.09 before removing the overlapping IP address, the prior software version enables the overlapping IP subnet.

**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.

HP recommends that you replace a failed fan tray assembly within one minute of removing it.
Troubleshooting
Displaying Transceiver Information

Displaying Transceiver Information

This feature provides the ability to view diagnostic monitoring information for transceivers with Diagnostic Optical Monitoring (DOM) support. The following table indicates the support level for specific transceivers:

<table>
<thead>
<tr>
<th>Product #</th>
<th>Description</th>
<th>Support*</th>
</tr>
</thead>
<tbody>
<tr>
<td>J8436A</td>
<td>10GbE X2-SC SR Optic</td>
<td>V</td>
</tr>
<tr>
<td>J8437A</td>
<td>10GbE X2-SC LR Optic</td>
<td>V</td>
</tr>
<tr>
<td>J8440B</td>
<td>10GbE X2-CX4 Xcver</td>
<td>NA</td>
</tr>
<tr>
<td>J8440C</td>
<td>10GbE X2-CX4 Xcver</td>
<td>NA</td>
</tr>
<tr>
<td>J4858A</td>
<td>Gigabit-SX-LC Mini-GBIC</td>
<td>V</td>
</tr>
<tr>
<td>J4858B</td>
<td>Gigabit-SX-LC Mini-GBIC</td>
<td>V</td>
</tr>
<tr>
<td>J4858C</td>
<td>Gigabit-SX-LC Mini-GBIC</td>
<td>V (some)</td>
</tr>
<tr>
<td>J9054B</td>
<td>100-FX SFP-LC Transceiver</td>
<td>N</td>
</tr>
<tr>
<td>J8177C</td>
<td>Gigabit 1000Base-T Mini-GBIC</td>
<td>NA</td>
</tr>
<tr>
<td>J9150A</td>
<td>10GbE SFP+ SR Transceiver</td>
<td>D</td>
</tr>
<tr>
<td>J9151A</td>
<td>10GbE SFP+ LR Transceiver</td>
<td>D</td>
</tr>
<tr>
<td>J9152A</td>
<td>10GbE SFP+ LRM Transceiver</td>
<td>D</td>
</tr>
<tr>
<td>J9153A</td>
<td>10GbE SFP+ ER Transceiver</td>
<td>D</td>
</tr>
<tr>
<td>J9144A</td>
<td>10GbE X2-SC LRM Transceiver</td>
<td>D</td>
</tr>
<tr>
<td>J8438A</td>
<td>10GbE X2-SC ER Transceiver</td>
<td>D</td>
</tr>
</tbody>
</table>

*Support indicators:
- V - Validated to respond to DOM requests
- N - No support of DOM
- D - Documented by the component suppliers as supporting DOM.
- NA - Not applicable to the transceiver (copper transceiver)

**Note**
Not all transceivers support Digital Optical Monitoring. If DOM appears in the Diagnostic Support field of the `show interfaces transceiver detail` command, or the `hpicfTransceiverMIB hpicfXcvrDiagnostics MIB` object, DOM is supported for that transceiver.
Troubleshooting
Displaying Transceiver Information

CLI Support

Enter this command to display information about the transceivers in the switch.

**Syntax:**  `show interfaces transceiver [port-list] [detail]`

*Displays information about the transceivers. If a port is specified, displays information for the transceiver in that port.*

*[detail]: Displays detailed transceiver information.*

MIB Support

The hpicfTransceiver MIB is available for displaying transceiver information.

Showing Transceiver Information

The transceiver information displayed depends on the **show** command executed.

The output for **show interfaces transceiver [port-list]** is shown in Figure C-11. You can specify multiple ports, separated by commas, and the information for each transceiver will display.

```
HP Switch(config)# show interfaces transceiver 21
Transceiver Technical information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Product Number</th>
<th>Serial Number</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>1000SX</td>
<td>J4858B</td>
<td>PAD45CP</td>
<td></td>
</tr>
</tbody>
</table>
```

**Figure C-11. Example of Output for a Specified Transceiver**

If there is no transceiver in the port specified in the command, the output displays as shown in Figure C-12.
Troubleshooting
Displaying Transceiver Information

When no ports are specified, information for all transceivers found is displayed.

You can specify all for port-list as shown in Figure C-14.

Figure C-12. Example of Output When No Transceiver is Present in Specified Interface

Figure C-13. Example of Output When No Ports are Specified

Figure C-14. Example of Output When “all” is Specified
Troubleshooting
Displaying Transceiver Information

Information Displayed with the Detail Parameter

When the `show interfaces transceiver [port-list] detail` command is executed, the following information displays.

### Table C-1. General Transceiver Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Index</td>
<td>The switch interface number</td>
</tr>
<tr>
<td>Transceiver-type</td>
<td>Pluggable transceiver type</td>
</tr>
<tr>
<td>Transceiver model</td>
<td>Pluggable transceiver model</td>
</tr>
<tr>
<td>Connector-type</td>
<td>Type of connector of the transceiver</td>
</tr>
<tr>
<td>Wavelength</td>
<td>For an optical transceiver: the central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, the values will be separated by a comma. An electrical transceiver value is displayed as N/A.</td>
</tr>
<tr>
<td>Transfer Distance</td>
<td>Link-length supported by the transceiver in meters. The corresponding transfer medium is shown in brackets following the transfer distance value, for example, 50um multimode fiber. If the transceiver supports multiple transfer media, the values are separated by a comma.</td>
</tr>
<tr>
<td>Diagnostic Support</td>
<td>Shows whether the transceiver supports diagnostics: None: supported DOM: supported VCT: supported</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the transceiver</td>
</tr>
</tbody>
</table>

The information in tables C-2, C-3, and C-4 is only displayed when the transceiver supports DOM.

### Table C-2. DOM Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>Transceiver temperature (in degrees Centigrade)</td>
</tr>
<tr>
<td>Voltage</td>
<td>Supply voltage in transceiver (Volts)</td>
</tr>
<tr>
<td>Bias</td>
<td>Laser bias current (mA)</td>
</tr>
<tr>
<td>RX power</td>
<td>Rx power (mW and dBm)</td>
</tr>
<tr>
<td>TX power</td>
<td>Tx power (mW and dBm)</td>
</tr>
</tbody>
</table>
Troubleshooting
Displaying Transceiver Information

The alarm information for GBIC/SFP transceivers is shown in Table C-3.

Table C-3. Alarm and Error Information (GBIC/SFP Transceivers Only)

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX loss of signal</td>
<td>Incoming (RX) signal is lost</td>
</tr>
<tr>
<td>RX power high</td>
<td>Incoming (RX) power level is high</td>
</tr>
<tr>
<td>RX power low</td>
<td>Incoming (RX) power level is low</td>
</tr>
<tr>
<td>TX fault</td>
<td>Transmit (TX) fault</td>
</tr>
<tr>
<td>TX bias high</td>
<td>TX bias current is high</td>
</tr>
<tr>
<td>TX bias low</td>
<td>TX bias current is low</td>
</tr>
<tr>
<td>TX power high</td>
<td>TX power is high</td>
</tr>
<tr>
<td>TX power low</td>
<td>TX power is low</td>
</tr>
<tr>
<td>Temp high</td>
<td>Temperature is high</td>
</tr>
<tr>
<td>Temp low</td>
<td>Temperature is low</td>
</tr>
<tr>
<td>Voltage High</td>
<td>Voltage is high</td>
</tr>
<tr>
<td>Voltage Low</td>
<td>Voltage is low</td>
</tr>
</tbody>
</table>

The alarm information for XENPAK transceivers is shown in Table C-4.

Table C-4. Alarm and Error Information (XENPAK Transceivers)

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WIS local fault</td>
<td>WAN Interface Sublayer local fault</td>
</tr>
<tr>
<td>Receive optical power fault</td>
<td>Receive optical power fault</td>
</tr>
<tr>
<td>PMA/PMD receiver local fault</td>
<td>Physical Medium Attachment/Physical Medium Dependent receiver local fault</td>
</tr>
<tr>
<td>PCS receiver local fault</td>
<td>Physical Coding Sublayer receiver local fault</td>
</tr>
<tr>
<td>PHY XS receive local fault</td>
<td>PHY Extended Sublayer receive local fault</td>
</tr>
<tr>
<td>RX power high</td>
<td>RX power is high</td>
</tr>
<tr>
<td>RX power low</td>
<td>RX power is low</td>
</tr>
<tr>
<td>Laser bias current fault</td>
<td>Laser bias current fault</td>
</tr>
<tr>
<td>Laser temperature fault</td>
<td>Laser temperature fault</td>
</tr>
</tbody>
</table>
### Troubleshooting

#### Displaying Transceiver Information

An example of the output for the `show interfaces transceiver [port-list] detail` for a 1000SX transceiver is shown in Figure C-15.

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laser output power fault</td>
<td>Laser output power fault</td>
</tr>
<tr>
<td>TX fault</td>
<td>TX fault</td>
</tr>
<tr>
<td>PMA/PMD transmitter local fault</td>
<td>PMA/PMD transmitter local fault</td>
</tr>
<tr>
<td>PCS Transmit local fault</td>
<td>PCS transmit local fault</td>
</tr>
<tr>
<td>PHY XS transmit local fault</td>
<td>PHY SX transmit local fault</td>
</tr>
<tr>
<td>TX bias high</td>
<td>TX bias current is high</td>
</tr>
<tr>
<td>TX bias low</td>
<td>TX bias current is low</td>
</tr>
<tr>
<td>TX power high</td>
<td>TX power is high</td>
</tr>
<tr>
<td>TX power low</td>
<td>TX power is low</td>
</tr>
<tr>
<td>Temp high</td>
<td>Temperature is high</td>
</tr>
<tr>
<td>Temp low</td>
<td>Temperature is low</td>
</tr>
</tbody>
</table>

An example of the output for the `show interfaces transceiver [port-list] detail` for a 1000SX transceiver is shown in Figure C-15.

```plaintext
HP Switch(config)# show interfaces transceiver 21 detail

Transceiver in 21
Interface index : 21
Type : 1000SX
Model : J4858B
Connector type : LC
Wavelength : 850nm
Transfer distance : 300m (50um), 150m (62.5um),
Diagnostic support : DOM
Serial number : PAD45CP

Status
Temperature : 50.111°C
Voltage : 3.1234V
TX Bias : 6mA
TX Power : 0.2650mW, -5.768dBm
RX Power : 0.3892mW, -4.098dBm

```

Figure C-15. Example of Detailed Information for a 1000SX Mini-GBIC Transceiver

An example of the output for a 10GbE-LR transceiver is shown in Figure C-16.
### Troubleshooting

**Displaying Transceiver Information**

HP Switch(config)# show interfaces transceiver 23 detail

<table>
<thead>
<tr>
<th>Transceiver in 23</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Index   : 24</td>
</tr>
<tr>
<td>Type              : 10GbE-LR</td>
</tr>
<tr>
<td>Model             : J8437A</td>
</tr>
<tr>
<td>Connector type    : SC</td>
</tr>
<tr>
<td>Wavelength        : Channel #0: 1310nm, #1:0nm, #2:0nm, #3:0nm</td>
</tr>
<tr>
<td>Transfer distance : 10000m (SM)</td>
</tr>
<tr>
<td>Diagnostic support: DOM</td>
</tr>
<tr>
<td>Serial number     : ED456SS987</td>
</tr>
</tbody>
</table>

**Status**

| Temperature      : 32.754C |
| TX Bias          : 42.700mA |
| TX Power         : 0.5192mW, -2.847dBm |
| RX Power         : 0.0040mW, -23.979dBm |

Recent Alarms:

- Rx power low alarm
- Rx power low warning

Recent errors:

- Receive optical power fault
- PMA/PMD receiver local fault
- PMA/PMD transmitter local fault
- PCS receive local fault
- PHY XS transmit local fault

Time stamp : Mon Mar 7 16:26:06 2011

---

**Figure C-16. Example of Detailed Information for a 10GbE-LR Transceiver**

**Displaying Transceiver Information for Copper Transceivers with VCT Support**

This feature provides the ability to view diagnostic monitoring information for copper transceivers with Virtual Cable Test (VCT) support. The cable quality of the copper cables connected between transceivers can be ascertained using the transceiver cable diagnostics. Results of the diagnostics are displayed with the appropriate CLI show commands and with SNMP using the hpicfTransceiver MIB.

The J8177C 1000Base-T Mini-GBIC is supported.
Troubleshooting
Displaying Transceiver Information

Testing the Cable

Enter the test cable-diagnostics command in any context to begin cable diagnostics for the transceiver. The diagnostic attempts to identify cable faults. The tests may take a few seconds to complete for each interface. There is the potential of link loss during the diagnostic.

Syntax: test cable-diagnostics [port-list]

Invokes cable diagnostics and displays the results.

```
HP Switch # test cable-diagnostics a23-a24
The 'test cable-diagnostics' command will cause a loss of link and will take a few seconds per interface to complete.
Continue (Y/N)? y

<table>
<thead>
<tr>
<th>Port</th>
<th>Pair</th>
<th>Status</th>
<th>Distance to Fault</th>
<th>Skew</th>
<th>Polarity</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>A23</td>
<td>1-2</td>
<td>OK</td>
<td>0 m</td>
<td>6 ns</td>
<td>Normal</td>
<td>MDIX</td>
</tr>
<tr>
<td></td>
<td>3-6</td>
<td>OK</td>
<td>0 m</td>
<td>0 ns</td>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4-5</td>
<td>OK</td>
<td>0 m</td>
<td>6 ns</td>
<td>Normal</td>
<td>MDIX</td>
</tr>
<tr>
<td></td>
<td>7-8</td>
<td>OK</td>
<td>0 m</td>
<td>6 ns</td>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td>A24</td>
<td>1-2</td>
<td>Short</td>
<td>2 m</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3-6</td>
<td>Impedance</td>
<td>3 m</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4-5</td>
<td>Impedance</td>
<td>3 m</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7-8</td>
<td>Open</td>
<td>1 m</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Figure C-17. Example of Output from test cable-diagnostics Command

Displaying Transceiver Information

Enter this command to display transceiver information and cable test results for the transceivers in the switch.

Syntax: show interfaces transceiver [port-list] [detail]

Displays information about the transceivers. If a port is specified, displays information for the transceiver in that port.

[detail]: Displays detailed transceiver information.
Troubleshooting
Displaying Transceiver Information

```
HP Switch# show interfaces transceiver a23 detail

Transceiver in A23
  Interface Index : 23
  Type : 1000T-sfp
  Model : J8177C
  Connector Type : RJ45
  Wavelength : n/a
  Transfer Distance : 100m (copper),
  Diagnostic Support : VCT
  Serial Number : US051HF099

  Link Status : Up
  Speed : 1000
  Duplex : Full

  MDI   Cable   Distance Pair   Pair   MDI
  Port  Pair  Status     to Fault  Skew  Polarity  Mode
  ----- ----- ---------- --------- ----- --------- -----
  A23   1-2   OK         0 m       6 ns  Normal    MDIX
        3-6   OK         0 m       0 ns  Normal
        4-5   OK         0 m       6 ns  Normal    MDIX
        7-8   OK         0 m       6 ns  Normal

  Test Last Run : Fri Apr 22 20:33:23 2011
```

Figure C-18. Example of Copper Cable Diagnostic Test Results
### Troubleshooting

#### Displaying Transceiver Information

**Table C-5. General Transceiver Information**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Index</td>
<td>The switch interface number</td>
</tr>
<tr>
<td>Transceiver-type</td>
<td>Pluggable transceiver type</td>
</tr>
<tr>
<td>Transceiver model</td>
<td>Pluggable transceiver model</td>
</tr>
<tr>
<td>Connector-type</td>
<td>Type of connector of the transceiver</td>
</tr>
<tr>
<td>Wavelength</td>
<td>For an optical transceiver: the central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, the values will be separated by a comma. An electrical transceiver value is displayed as N/A.</td>
</tr>
<tr>
<td>Transfer Distance</td>
<td>Link-length supported by the transceiver in meters. The corresponding transfer medium is shown in brackets following the transfer distance value, for example, 50um multimode fiber. If the transceiver supports multiple transfer media, the values are separated by a comma.</td>
</tr>
<tr>
<td>Diagnostic Support</td>
<td>Shows whether the transceiver supports diagnostics: None: supported</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the transceiver</td>
</tr>
<tr>
<td>Link Status</td>
<td>Link up or down</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed of transceiver in Mbps</td>
</tr>
<tr>
<td>Duplex</td>
<td>Type of duplexing</td>
</tr>
<tr>
<td>Cable Status</td>
<td>Values are OK, Open, Short, or Impedance</td>
</tr>
<tr>
<td>Distance to Fault</td>
<td>The distance in meters to a cable fault (accuracy is +/- 2 meters); displays 0 (zero) if there is no fault</td>
</tr>
<tr>
<td>Pair Skew</td>
<td>Difference in propagation between the fastest and slowest wire pairs</td>
</tr>
<tr>
<td>Pair Polarity</td>
<td>Signals on a wire pair are polarized, with one wire carrying the positive signal and one carrying the negative signal.</td>
</tr>
<tr>
<td>MDI Mode</td>
<td>The MDI crossover status of the two wire pairs (1&amp;2, 3&amp;6, 4&amp;5, 7&amp;8), will be either MDI or MDIX</td>
</tr>
</tbody>
</table>
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.

The maximum number of entries supported in the Event Log is increased from 1000 to 2000 entries. 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-19, each Event Log entry is composed of five or six fields, depending on whether numbering is turned on or not:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Date</th>
<th>Time</th>
<th>Event number</th>
<th>System Module</th>
<th>Event Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>08/05/06</td>
<td>10:52:32</td>
<td>00063</td>
<td></td>
<td>ports: port 1 enabled</td>
</tr>
</tbody>
</table>

Figure C-19. 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.
Troubleshooting
Using the Event Log for Troubleshooting Switch Problems

D (debug) is reserved for HP internal 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

<table>
<thead>
<tr>
<th>System Module</th>
<th>Description</th>
<th>Documented in HP Hardware/Software guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x</td>
<td>802.1X authentication: Provides access control on a per-client or per-port basis:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Client-level security that allows LAN access to 802.1X clients (up to 32 per port) with valid user credentials</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Port-level security that allows LAN access only on ports on which a single 802.1X-capable client (suppliant) has entered valid RADIUS user credentials</td>
<td></td>
</tr>
<tr>
<td>acl</td>
<td>Access Control Lists (ACLs): Filter layer-3 IP traffic to or from a host to block unwanted IP traffic, and block or limit other protocol traffic such as TCP, UDP, IGMP, and ICMP. Access control entries (ACEs) specify the filter criteria and an action (permit or deny) to take on a packet if it meets the criteria.</td>
<td></td>
</tr>
<tr>
<td>addrmgr</td>
<td>Address Table Manager: Manages MAC addresses that the switch has learned and are stored in the switch’s address table.</td>
<td></td>
</tr>
<tr>
<td>arp-protect</td>
<td>Dynamic ARP Protection: Protects the network from ARP cache poisoning. Only valid ARP requests and responses are relayed or used to update the local ARP cache. ARP packets with invalid IP-to-MAC address bindings advertised in the source protocol address and source physical address fields are discarded.</td>
<td></td>
</tr>
<tr>
<td>auth</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
## Troubleshooting
Using the Event Log for Troubleshooting Switch Problems

<table>
<thead>
<tr>
<th>System Module</th>
<th>Description</th>
<th>Documented in HP Hardware/Software guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdp</td>
<td>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.</td>
<td>Management and Configuration Guide</td>
</tr>
<tr>
<td>connfilt</td>
<td>Connection-Rate filtering: Used on the network edge to protect the network from attack by worm-like malicious code by detecting hosts that are generating IP traffic that exhibits this behavior and (optionally) either throttling or dropping all IP traffic from the offending hosts. Connection-Rate filtering messages include events on virus throttling. Virus throttling uses connection-rate filtering to stop the propagation of malicious agents.</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>console</td>
<td>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.</td>
<td>Installation and Getting Started Guide</td>
</tr>
<tr>
<td>cos</td>
<td>Class of Service (CoS): Provides priority handling of packets traversing the switch, based on the IEEE 802.1p priority carried by each packet. 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.</td>
<td>Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>dca</td>
<td>Dynamic Configuration Arbiter (DCA) determines the client-specific parameters that are assigned in an authentication session.</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>dhcp</td>
<td>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.</td>
<td>Management and Configuration Guide</td>
</tr>
<tr>
<td>dhcp v6c</td>
<td>DHCP for IPv6 prefix assignment</td>
<td>IPv6 Management Guide</td>
</tr>
<tr>
<td>dhcp pr</td>
<td>DHCP relay: Forwards client-originated DHCP packets to a DHCP network server.</td>
<td>Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>download</td>
<td>Download operation for copying a software version or files to the switch.</td>
<td>Management and Configuration Guide</td>
</tr>
<tr>
<td>dhcp-snoop</td>
<td>DHCP snooping: Protects your network from common DHCP attacks, such as address spoofing and repeated address requests.</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>dma</td>
<td>Direct Access Memory (DMA): Transmits and receives packets between the CPU and the switch.</td>
<td>—</td>
</tr>
</tbody>
</table>
## Troubleshooting

Using the Event Log for Troubleshooting Switch Problems

<table>
<thead>
<tr>
<th>System Module</th>
<th>Description</th>
<th>Documented in HP Hardware/Software guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>fault</td>
<td>Fault Detection facility, including response policy and the sensitivity level at which a network problem should generate an alert.</td>
<td>Management and Configuration Guide</td>
</tr>
<tr>
<td>ffi</td>
<td>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.</td>
<td>Installation and Getting Started Guide Management and Configuration Guide</td>
</tr>
<tr>
<td>gvrp</td>
<td>Generic Attribute 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.</td>
<td>Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>hpesp</td>
<td>Management module that maintains communication between switch ports.</td>
<td>Installation and Getting Started Guide</td>
</tr>
<tr>
<td>idm</td>
<td>Identity-driven Management: Optional management application used to monitor and control access to switch.</td>
<td>Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>igmp</td>
<td>Internet Group Management Protocol: Reduces unnecessary bandwidth usage for multicast traffic transmitted from multimedia applications on a per-port basis.</td>
<td>Multicast and Routing Guide</td>
</tr>
<tr>
<td>ip</td>
<td>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; enables IP routing on the switch.</td>
<td>Basic Operation Guide Multicast and Routing Guide</td>
</tr>
<tr>
<td>ipaddrmgr</td>
<td>IP Address Manager: Programs IP routing information in switch hardware.</td>
<td>Multicast and Routing Guide</td>
</tr>
<tr>
<td>iplock</td>
<td>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.</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>ipx</td>
<td>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.</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>licensing</td>
<td>HP premium licensing: Provide access to expanded features on certain HP network devices.</td>
<td>Premium License Installation Guide</td>
</tr>
<tr>
<td>kms</td>
<td>Key Management System: Configures and maintains security information (keys) for all routing protocols, including a timing mechanism for activating and deactivating an individual protocol.</td>
<td>Access Security Guide</td>
</tr>
</tbody>
</table>
**Troubleshooting**

*Using the Event Log for Troubleshooting Switch Problems*

<table>
<thead>
<tr>
<th>System Module</th>
<th>Description</th>
<th>Documented in HP Hardware/Software guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>lacp</td>
<td>LACP trunks: The switch can either automatically establish an 802.3ad-compliant trunk group or provide a manually configured, static LACP trunk.</td>
<td>Management and Configuration Guide</td>
</tr>
<tr>
<td>ldbal</td>
<td>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. Load-balancing messages also include switch meshing events. The Switch Meshing feature provides redundant links, improved bandwidth use, and support for different port types and speeds.</td>
<td>Management and Configuration Guide, Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>lldp</td>
<td>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.</td>
<td>Management and Configuration Guide</td>
</tr>
<tr>
<td>loop_protect</td>
<td>Loop protection: Detects the formation of loops when an unmanaged device on the network drops spanning tree packets, and provides protection by transmitting loop protocol packets out ports on which loop protection has been enabled.</td>
<td>Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>macauth</td>
<td>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: - Web page login to authenticate users for access to the network - RADIUS server that uses a device's MAC address for authentication</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>maclock</td>
<td>MAC lockdown and MAC lockout - MAC lockdown prevents station movement and MAC address &quot;hijacking&quot; 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. - MAC lockout blocks a specific MAC address so that the switch drops all traffic to or from the specified address.</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>mgr</td>
<td>PCM and PCM+: Windows-based network management solutions for managing and monitoring performance of HP devices. PCM messages also include events for configuration operations.</td>
<td>Basic Operation Guide</td>
</tr>
<tr>
<td>mld</td>
<td>Multicast Listener Discovery (MLD): IPv6 protocol used by a router to discover the presence of multicast listeners. MLD can also optimize IPv6 multicast traffic flow with the snooping feature.</td>
<td>Multicast and Routing Guide</td>
</tr>
</tbody>
</table>
### Troubleshooting

Using the Event Log for Troubleshooting Switch Problems

<table>
<thead>
<tr>
<th>System Module</th>
<th>Description</th>
<th>Documented in HP Hardware/Software guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtm</td>
<td>Multicast Traffic Manager (MTM): Controls and coordinates L3 multicast traffic for upper layer protocols.</td>
<td>Multicast and Routing Guide</td>
</tr>
<tr>
<td>netinet</td>
<td>Network Internet: Monitors the creation of a route or an Address Resolution Protocol (ARP) entry and sends a log message in case of failure.</td>
<td>Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>ports</td>
<td>Port status and port configuration features, including mode (speed and duplex), flow control, broadcast limit, jumbo packets, and security settings. Port messages include events on Power Over Ethernet (POE) operation and transceiver connections with other network devices.</td>
<td>Management and Configuration Guide Access Security Guide</td>
</tr>
<tr>
<td>radius</td>
<td>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.</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>ratelim</td>
<td>Rate-limiting: Enables a port to limit the amount of bandwidth a user or device may utilize for inbound traffic on the switch.</td>
<td>Management and Configuration Guide</td>
</tr>
<tr>
<td>sflow</td>
<td>Flow sampling: sFlow is 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.</td>
<td>Management and Configuration Guide</td>
</tr>
<tr>
<td>snmp</td>
<td>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.</td>
<td>Management and Configuration Guide</td>
</tr>
<tr>
<td>ssh</td>
<td>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. 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.</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>ssl</td>
<td>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.</td>
<td>Access Security Guide</td>
</tr>
</tbody>
</table>
## Troubleshooting

### Using the Event Log for Troubleshooting Switch Problems

<table>
<thead>
<tr>
<th>System Module</th>
<th>Description</th>
<th>Documented in HP Hardware/Software guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack</td>
<td>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.</td>
<td>Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>stp</td>
<td>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.</td>
<td>Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>system</td>
<td>Switch management, including system configuration, switch bootup, activation of boot ROM image, memory buffers, traffic and security filters. System messages also include events from Management interfaces (menu, CLI, web browser, PCM used to reconfigure the switch and monitor switch status and performance.</td>
<td>Management and Configuration Guide Basic Operation Guide Access Security Guide</td>
</tr>
<tr>
<td>tacacs</td>
<td>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).</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>tcp</td>
<td>Transmission Control Protocol: A transport protocol that runs on IP and is used to set up connections.</td>
<td>Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>telnet</td>
<td>Session established on the switch from a remote device through the Telnet virtual terminal protocol.</td>
<td>Basic Operation Guide</td>
</tr>
<tr>
<td>tftp</td>
<td>Trivial File Transfer Protocol: Supports the download of files to the switch from a TFTP network server.</td>
<td>Management and Configuration Guide</td>
</tr>
<tr>
<td>udld</td>
<td>Uni-directional Link Detection: Monitors a link between two switches and blocks the ports on both ends of the link if the link fails at any point between the two devices.</td>
<td>Access Security Guide</td>
</tr>
<tr>
<td>udpf</td>
<td>UDP broadcast forwarding: Supports the forwarding of client requests sent as limited IP broadcasts addressed to a UDP application port on a network server.</td>
<td>Multicast and Routing Guide</td>
</tr>
<tr>
<td>update</td>
<td>Updates (TFTP or serial) to HP software and updates to running-config and start-up config files</td>
<td>Management and Configuration Guide Basic Operation Guide</td>
</tr>
</tbody>
</table>
Troubleshooting

Using the Event Log for Troubleshooting Switch Problems

Menu: Displaying and Navigating in the Event Log

To display the Event Log from the Main Menu, select Event Log. Figure C-20 shows a sample event log display.

<table>
<thead>
<tr>
<th>System Module</th>
<th>Description</th>
<th>Documented in HP Hardware/Software guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Static 802.1Q VLAN operations, including port-and protocol-based configurations that group users by logical function instead of physical location. A port-based VLAN creates a layer-2 broadcast domain comprised of member ports that bridge IPv4 traffic among themselves. A protocol-based VLAN creates a layer-3 broadcast domain for traffic of a particular routing protocol, and is comprised of member ports that bridge traffic of the specified protocol type among themselves. VLAN messages include events from Management interfaces (menu, CLI, web browser, PCM) used to reconfigure the switch and monitor switch status and performance.</td>
<td>Advanced Traffic Management Guide</td>
</tr>
<tr>
<td>xmodem</td>
<td>Xmodem: Binary transfer feature that supports the download of software files from a PC or Unix workstation.</td>
<td>Management and Configuration Guide</td>
</tr>
</tbody>
</table>

Figure C-20. Example of an Event Log Display
Troubleshooting
Using the Event Log for Troubleshooting Switch Problems

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 Table Table C-6.

Table C-6. Event Log Control Keys

<table>
<thead>
<tr>
<th>Key</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Advances the display by one page (next page).</td>
</tr>
<tr>
<td>P</td>
<td>Rolls back the display by one page (previous page).</td>
</tr>
<tr>
<td>[v]</td>
<td>Advances display by one event (down one line).</td>
</tr>
<tr>
<td>[^]</td>
<td>Rolls back display by one event (up one line).</td>
</tr>
<tr>
<td>E</td>
<td>Advances to the end of the log.</td>
</tr>
<tr>
<td>H</td>
<td>Displays Help for the Event Log.</td>
</tr>
</tbody>
</table>
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, -m, -p, -w, -i, -d] [<Option-str>]`

*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.
- `-m` displays only major log events.
- `-p` displays only performance log events.
- `-w` displays only warning log events.
- `-i` displays only informational log events.
- `-d` displays only debug log events.

*Option-Str filters the events*

**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.
Troubleshooting
Using the Event Log for Troubleshooting Switch Problems

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:

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Log Throttle Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>I (Information)</td>
<td>6000 Seconds</td>
</tr>
<tr>
<td>W (Warning)</td>
<td>600 Seconds</td>
</tr>
<tr>
<td>D (Debug)</td>
<td>60 Seconds</td>
</tr>
<tr>
<td>M (Major)</td>
<td>6 Seconds</td>
</tr>
</tbody>
</table>

Example of Log Throttling

For example, suppose that you configure VLAN 100 on the switch to support PIM operation, but do not configure an IP address. If PIM attempted to use VLAN 100, the switch would generate the first instance of the following Event Log message and counter.

```
W 10/01/06 09:00:33 PIM: No IP address configured on VID 100. (1)
```

The counter indicates that this is the first instance of this event since the switch last rebooted.

If PIM operation caused the same event to occur six more times during the initial log throttle period, there would be no further entries in the Event Log. However, if the event occurred again after the log throttle period expired, the switch would repeat the message (with an updated counter) and start a new log throttle period.

```
W 10/01/06 09:00:33 PIM: No IP address configured on VID 100. (1)
```

This message indicates the original instance of the event (since the last switch reboot).

```
W 10/01/06 09:28:42 PIM: No IP address configured on VID 100. (8)
```

The duplicate of the original message is the first instance of the event since the previous log throttle period expired, and indicates that a new log throttle period has begun for this event.

The counter now indicates that this is the eighth instance of this event since the switch last rebooted.
Note that if the same type of event occurs under different circumstances, the switch handles these as unrelated events for the purpose of Event Log messages. For example, if PIM operation simultaneously detected that VLANs 100 and 205 were configured without IP addresses, you would see log messages similar to the following:

*These two messages report separate events involving separate log throttle periods and separate counters.*

\[
\begin{align*}
W & 10/01/06 09:00:33 PIM: No IP address configured on VID 100 (1) \\
W & 10/01/06 09:00:33 PIM: No IP address configured on VID 205 (1)
\end{align*}
\]

**Figure C-23. Example of Log Messages Generated by Unrelated Events of the Same Type**

**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-7. (The same operation would apply for messages sent to any configured SNMP trap receivers.)

**Table C-7. How the Duplicate Message Counter Increments**

<table>
<thead>
<tr>
<th>Instances During 1st Log Throttle Period</th>
<th>Instances During 2nd Log Throttle Period</th>
<th>Instances During 3rd Log Throttle Period</th>
<th>Duplicate Message Counter*</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>5</td>
<td>4</td>
<td>9</td>
</tr>
</tbody>
</table>

*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.*
Reporting Information About Changes to the Running Configuration

Syslog can be used for sending notifications to a remote syslog server about changes made to the running configuration. The notifications in the syslog messages are sent in ASCII format and contain this information:

- **Notice-Type**: Describes the syslog notification as a “running config change”.
- **Event-ID**: Identifier for the running config change event that occurred on the switch.
- **Config-Method**: The source for the running config change.
- **Device-Name**: The managed device.
- **User-Name**: User who made the running config change.
- **Remote-IP-Address**: IP address of a remote host from which the user is connected.

**Syntax:**

```
[no] logging notify <running-config-change> [transmission-interval <0-4294967295>]
```

Enables sending the running configuration change notifications to the syslog server.

The **no** form of the command disables sending the running configuration changes to the syslog server.

**Default:** Disabled

- **<running-config-change>**: Mandatory option for the **notify** parameter. Specifies the type of notification to send.
- **transmission-interval<0-4294967295>**: Specifies the time interval (in seconds) between the transmission of two consecutive notifications. Running config changes occurring within the specified interval will not generate syslog notifications.

A value of zero means there is no limit; a notification is sent for every running config change.

**Default:** Zero

```
HP Switch(config)# logging notify running-config-change
transmission-interval 10
```

Figure C-24. Example of Sending Running Config Changes to the Syslog Server
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 routing 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-25, you can perform the following operations:

- Use the `debug` command to configure messaging reports for the following event types:
  - ACL “deny” matches
  - Dynamic ARP protection events
  - DHCP snooping events
  - Events recorded in the switch’s Event Log
  - IP routing events (IPv4 and IPv6)
  - LLDP events
  - SSH events
  - Wireless Services 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-58 and “Configuring a Syslog Server” on page C-60.
Troubleshooting
Debug/Syslog Operation

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. |
| Event Notification Logging | <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-description | Text string associated with the values of facility, severity, and system-module. Provides a user-friendly description for the combined filter values of 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. 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 ACL, Event Log, and IP-RIP options. |
| debug Command | cdp | Displays cdp information. |
| destination logging | 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-58. session: | Assigns or re-assings destination status to the terminal device that was most recently used to request debug output. “Debug Destinations” on page C-58. 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-58. |
| dhcp-snooping agent | Displays DHCP snooping agent messages. event | Displays DHCP snooping event messages. packet | Displays DHCP snooping packet messages. |
Troubleshooting

Debug/Syslog Operation

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.
- 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 of 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 <acl|all|arp-protect|cdp|destination |dhcp-snooping|dynamic-ip-lockdown|event|ip [fib|forwarding|packet |rip]|ipv6|lldp|security|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-35.

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 >
   ```
Troubleshooting
Debug/Syslog Operation

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
    Enabled debug types:
      event

Figure C-26. 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-27. Syslog Configuration to Receive Event Log Messages From Specified System Module and Severity Levels](image)

As shown at the top of Figure C-27, 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.)
Example. The next example shows how to configure:

- Debug logging of ACL packet messages on a Syslog server at 18.38.64.164 (with user as the default logging facility).
- Display of these messages in the CLI session of your terminal device’s management access to the switch.
- Blocking Event Log messages from being sent from the switch to the Syslog server and a CLI session.

To configure Syslog operation in these ways with the Debug/Syslog feature disabled on the switch, you would enter the commands shown in Figure C-28.

![Figure C-28. Debug/Syslog Configuration for Multiple Debug Types and Multiple Destinations](image-url)
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-60.

Debug Messages

Use the **debug** command to configure the types of debug messages that the switch can send to configured debug destinations.

**Syntax:**  
```plaintext
[no] debug < debug-type >
```

- acl
  
  When a match occurs on an ACL “deny” Access Control Entry (with log configured), the switch sends an ACL message to configured debug destinations. For information on ACLs, refer to the “Access Control Lists (ACLs)” chapter in the latest version of the following guides:
  
  - IPv4 ACLs: Access Security Guide
  - IPv6 ACLs: IPv6 Configuration Guide

**Note:** Beginning with software release A.14.01, ACE matches (hits) for permit and deny entries can be tracked using the **show statistics < aclv4 | aclv6 >** command.

  (Default: Disabled - ACL messages for traffic that matches “deny” entries are not sent.)

- 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.
Troubleshooting
Debug/Syslog Operation

**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-58.
- **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-58.
- **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-58.

**dynamic-ip-lockdown**

Sends dynamic IP lockdown debug messages to the debug destination.

**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 | forwarding | packet | rip]**

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.
Troubleshooting
Debug/Syslog Operation

```
ip [ rip [ database | event | trigger ] ]

rip < database | event | trigger >> — Enables the specified RIP message type for the configured destination(s).
  database — Displays database changes.
  event — Displays RIP events.
  trigger — Displays trigger messages.

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.
```
Debug/Syslog Operation

security [arp-protect | dhcp-snooping | dynamic-ip-lockdown | port-access | port-security | radius-server | ssh | tacacs-server | user-profile-mib]

- **arp-protect**: Sends dynamic ARP protection debug messages to configured debug destinations.
- **dhcp-snooping**: Sends DHCP snooping debug messages to configured debug destinations.
  - **agent**: Displays DHCP snooping agent messages.
  - **event**: Displays DHCP snooping event messages.
  - **packet**: Displays DHCP snooping packet messages.
- **dynamic-ip-lockdown**: Sends dynamic IP lockdown debug messages to the debug destination.
- **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:**

```plaintext
[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-55) are sent. (Default: Logging disabled)

To configure a Syslog server IP address, refer to “Configuring a Syslog Server” on page C-60.
Troubleshooting
Debug/Syslog Operation

**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-65.

**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-55.)

**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.
Troubleshooting
Debug/Syslog Operation

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-55).
- 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-63 and “Configuring the System Module Used to Select the Event Log Messages Sent to a Syslog Server” on page C-64).
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-52).

**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. The ACL and/or IP-RIP message types will also be sent to the Syslog server(s) if they are currently enabled as debug types. (Refer to “Debug Messages” on page C-55.)

- `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-55.)
Troubleshooting
Debug/Syslog Operation

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.) HP recommends 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.

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:
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 HP internal 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-60.

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-29. Example of the Logging Command with a Priority Description

---

Troubleshooting
Debug/Syslog Operation
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-60.

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:**

```plaintext
[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.**

<table>
<thead>
<tr>
<th>Debug Option</th>
<th>Effect of a Reboot or Reset</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging (debug destination)</td>
<td>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.</td>
</tr>
<tr>
<td>session (debug destination)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>ACL (debug type)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>All (debug type)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>event (debug type)</td>
<td>If a Syslog server IP address is configured in the startup-config file, the sending of Event Log messages is reset to <strong>enabled</strong>, regardless of the last active setting. If no Syslog server is configured, the sending of Event Log messages is <strong>disabled</strong>.</td>
</tr>
<tr>
<td>IP (debug type)</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

- **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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Auto negotiation</td>
<td>n/a</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Ping test</td>
<td>n/a</td>
<td>—</td>
<td>page C-67</td>
</tr>
<tr>
<td>Link test</td>
<td>n/a</td>
<td>—</td>
<td>page C-67</td>
</tr>
<tr>
<td>Traceroute operation</td>
<td>n/a</td>
<td>—</td>
<td>page C-69</td>
</tr>
<tr>
<td>View switch configuration files</td>
<td>n/a</td>
<td>—</td>
<td>page C-73</td>
</tr>
<tr>
<td>View switch (show tech) operation</td>
<td>n/a</td>
<td>—</td>
<td>page C-73</td>
</tr>
<tr>
<td>View crash information and command history</td>
<td>n/a</td>
<td>—</td>
<td>page C-79</td>
</tr>
<tr>
<td>View system information and software version</td>
<td>n/a</td>
<td>—</td>
<td>page C-79</td>
</tr>
<tr>
<td>Useful commands in a troubleshooting session</td>
<td>n/a</td>
<td>—</td>
<td>page C-83</td>
</tr>
<tr>
<td>Resetting factory-default configuration</td>
<td>page C-84 (Buttons)</td>
<td>—</td>
<td>page C-84</td>
</tr>
<tr>
<td>Restoring a flash image</td>
<td>n/a</td>
<td>—</td>
<td>page C-85</td>
</tr>
<tr>
<td>Port Status</td>
<td>n/a</td>
<td>page B-7</td>
<td>page B-7</td>
</tr>
</tbody>
</table>

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”.

C-66
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.

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-87.

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.

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:**

```plaintext
ping <ip-address | hostname> [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.

```plaintext
<ip-address | hostname>
```

*Target IP address or hostname of the destination node being pinged.*
Troubleshooting
Diagnostic Tools

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

| Basic Ping Operation | Switch> ping 10.28.227.103
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.28.227.103 is alive, time = 15 ms</td>
</tr>
</tbody>
</table>

| Ping with Repetitions | Switch> ping 10.28.227.103 repetitions 3
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.28.227.103 is alive, iteration 1, time = 15 ms</td>
</tr>
<tr>
<td></td>
<td>10.28.227.103 is alive, iteration 2, time = 15 ms</td>
</tr>
<tr>
<td></td>
<td>10.28.227.103 is alive, iteration 3, time = 15 ms</td>
</tr>
</tbody>
</table>

| Ping with Repetitions and Timeout | Switch> ping 10.28.227.103 repetitions 3 timeout 2
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.28.227.103 is alive, iteration 1, time = 15 ms</td>
</tr>
<tr>
<td></td>
<td>10.28.227.103 is alive, iteration 2, time = 10 ms</td>
</tr>
<tr>
<td></td>
<td>10.28.227.103 is alive, iteration 3, time = 15 ms</td>
</tr>
</tbody>
</table>

| Ping Failure | Switch> ping 10.28.227.105
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>--------------</td>
<td>Target did not respond.</td>
</tr>
</tbody>
</table>

Figure C-30. 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-87.
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-31. Example of Link Tests**

<table>
<thead>
<tr>
<th>Basic Link Test</th>
<th>HP Switch# link 0030c1-7fcc40</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Link-test passed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Link Test with Repetitions</th>
<th>HP Switch# link 0030c1-7fcc40 repetitions 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>802.2 TEST packets sent: 3, responses received: 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Link Test with Repetitions and Timeout</th>
<th>HP Switch# link 0030c1-7fcc40 repetitions 3 timeout 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>802.2 TEST packets sent: 3, responses received: 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Link Test Over a Specific VLAN</th>
<th>HP Switch# link 0030c1-7fcc40 repetitions 3 timeout 1 vlan 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>802.2 TEST packets sent: 3, responses received: 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Link Test Over a Specific VLAN; Test Fail</th>
<th>HP Switch# link 0030c1-7fcc40 repetitions 3 timeout 1 vlan 222</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>802.2 TEST packets sent: 3, responses received: 0</td>
</tr>
</tbody>
</table>

---

**Traceroute Command**

The *traceroute* command enables you to trace the route from the switch to a host address.
Troubleshooting
Diagnostic Tools

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)
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:

```
HP Switch# traceroute 125.25.24.35
traceroute to 125.25.24.35 , 1 hop min, 30 hops max, 5 sec. timeout, 3 probes
    1 10.255.120.2           0 ms       0 ms       0 ms
    2 10.71.217.2            7 ms       3 ms       0 ms
    3 10.243.170.1           0 ms       1 ms       0 ms
    4 125.25.24.35           3 ms       3 ms       0 ms
```

```
Intermediate router hops with the time taken for the switch to receive acknowledgement of each probe reaching each router.
```

![Figure C-32. Example of a Completed Traceroute Enquiry](image)

```
Traceroute does not reach destination IP address because of low maxttl setting.
```

Continuing from the previous example (Figure C-32, above), executing `traceroute` with an insufficient `maxttl` for the actual hop count produces an output similar to this:

```
HP Switch# traceroute 125.25.24.35 maxttl 3
traceroute to 125.25.24.35 , 1 hop min, 30 hops max, 5 sec. timeout, 3 probes
    1 10.255.120.2           0 ms       0 ms       0 ms
    2 10.71.217.2            0 ms       0 ms       0 ms
    3 10.243.170.1           0 ms *        0 ms
```

```
The asterisk indicates there was a timeout on the second probe to the third hop.
```

![Figure C-33. Example of Incomplete Traceroute Due to Low Maxttl Setting](image)
Troubleshooting
Diagnostic Tools

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-33, 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:

```
HP Switch# traceroute 125.25.24.35 maxttl 7
trace route to 107.64.197.100 ,
1 hop min, 7 hops max, 5 sec. timeout, 3 probes
1 10.255.120.2           0 ms       0 ms       0 ms
2 10.71.217.2            0 ms       0 ms       0 ms
3 * 10.243.170.1           0 ms *
4 *  *  *  *
5 *  *  *  *
6 *  *  *  *
7 *  *  *  *
```

Figure C-34. Example of Traceroute Failing to Reach the Destination Address
Troubleshooting
Viewing Switch Configuration and Operation

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 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.

**Syntax:** write terminal

*Displays the running configuration.*

```
show config
```

*Displays the startup configuration.*

```
show running-config
```

*Displays the running-config file.*

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
Troubleshooting
Viewing Switch Configuration and Operation

- Load balancing (trunk and LACP)

Figure C-35 shows sample output from the `show tech` command.

```
HP Switch# show tech
show system
Status and Counters - General System Information
System Name        : 400_1
System Contact     :
System Location    :
MAC Age Time (sec) : 300
Time Zone          : 0
Daylight Time Rule : None
Software revision  : A.15.XX
ROM Version        : A.15.01
Up Time            : 23 hours
CPU Util (%)       : 10
IP Mgmt - Pkts Rx : 759
Pkts Tx : 2
Base MAC Addr      : 001871-c42f00
Serial Number      : SG641SU00L
Memory - Total     :
Free               :
Packet - Total     : 6750
Buffers Free       : 5086
Lowest Missed      : 4961
Missed             : 0
```

**Figure C-35. Example of Show Tech Command**

To specify the data displayed by the `show tech` command, use the `copy show tech` command as described in “Customizing show tech Command Output” on page C-76.

**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-36. Capture Text window of the Hyperterminal Application](image)

2. In the `File` field, enter the path and file name in which you want to store the `show tech` output.

![Figure C-37. Entering a Path and Filename for Saving show tech Output](image)

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.
Troubleshooting
Viewing Switch Configuration and Operation

6. To access the file, open it in Microsoft Word, Notepad, or a similar text editor.

Customizing show tech Command Output

Use the `copy show tech` command to customize the detailed switch information displayed with the `show tech` command to suit your troubleshooting needs.

To customize the information displayed with the `show tech` command:

1. Determine the information that you want to gather to troubleshoot a problem in switch operation.
2. Enter the `copy show tech` command to specify the data files that contain the information you want to view.

**Syntax:** `copy <source> show-tech`

Specifies the operational and configuration data from one or more source files to be displayed by the `show tech` command. Enter the command once for each data file that you want to include in the display.

Default: Displays data from all source files, where `<source>` can be any one of the following values:

- `command-output "<command>"`
  
  Includes the output of a specified command in `show-tech` command output. Enter the command name between double-quotation marks; for example, `copy "show system" show-tech`.

- `crash-data`:
  
  Includes the crash data from all management and interface modules in `show tech` command output.

**Syntax:** `copy <source> show-tech`

- `crash-log`
  
  Includes the crash logs in `show tech` command output.

- `event-log`
  
  Copies the contents of the Event Log to `show tech` command output.
Troubleshooting
Viewing Switch Configuration and Operation

Syntax: copy <source> show tech

running-config

Includes the contents of the running configuration file in show tech command output.

startup-config

Includes the contents of the startup configuration file in show tech command output.

tftp config < startup-config | running-config > < ip-addr > < remote-file > < pc | unix >

Downloads the contents of a configuration file from a remote host to show tech command output, where:

ip-addr: Specifies the IP address of the remote host device.

remote-file: Specifies the pathname on the remote host for the configuration file whose contents you want to include in the command output.

pc | unix: Specifies whether the remote host is a DOS-based PC or UNIX workstation.

For more information on using copy tftp commands, refer to the “File Transfers” appendix.

Syntax: copy <source> show tech

usb config < startup-config < filename > | command-file < acl-filename.txt >

Copies the contents of a configuration file or ACL command file from a USB flash drive to show tech command output, where:

startup-config < filename >: Specifies the name of a startup configuration file on the USB drive.

command-file < acl-filename.txt >: Specifies the name of an ACL command file on the USB drive.

For more information on using copy usb commands, refer to the “File Transfers” appendix.

xmodem config < startup-config | config < filename > | command-file < acl-filename.txt > < pc | unix >
Troubleshooting
Viewing Switch Configuration and Operation

Syntax: copy <source> show tech

Copies the contents of a configuration file or ACL command file from a serially connected PC or UNIX workstation to show tech command output, where:

startup-config: Specifies the name of the startup configuration file on the connected device.
config <filename>: Specifies the pathname of a configuration file on the connected device.
command-file <acl-filename.txt>: Specifies the pathname of an ACL command file on the connected device.

pc | unix: Specifies whether the connected device is a DOS-based PC or UNIX workstation.

For more information on using copy xmodem commands, refer to the “File Transfers” appendix.
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 crash information saved on the switch (see “Displaying Saved Crash Information” in the “Redundancy (Switch 8212zl)” chapter).*

**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).*

**show interfaces-display**

*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.
Troubleshooting
Viewing Switch Configuration and Operation

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"  Displays only lines that contain "ipv6".
HP Switch(config)#
```

Figure C-38. Example of Pattern Matching with Include Option
Figure C-39. Example of Pattern Matching with Exclude Option

```plaintext
HP Switch(config)# show run | exclude ipv6

Running configuration:

; J9562A Configuration Editor; Created on release #A.15.XX

hostname "HP Switch"
snmp-server community "notpublic" Unrestricted
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-24
    ip address dhcp-bootp
    no untagged 21-24
    exit
vlan 20
    name "VLAN20"
    untagged 21-24
    no ip address
    exit
policy qos "michael"
    exit
    exit
no autorun
password manager

Displays all lines that don't contain "ipv6".
```
Troubleshooting
Viewing Switch Configuration and Operation

```yaml
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"
   exit
no autorun
password manager
```

Displays the running config beginning at the first line that contains “ipv6”.

**Figure C-40. Example of Pattern Matching with Begin Option**

Figure C-41 is an example of the `show arp` command output, and then the output displayed when the `include` option has the IP address of **15.255.128.1** as the regular expression.

```plaintext
HP Switch(config)# show arp
IP ARP table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.255.128.1</td>
<td>00000c-07ac00</td>
<td>dynamic</td>
<td>1</td>
</tr>
<tr>
<td>15.255.131.19</td>
<td>00a0c9-b1503d</td>
<td>dynamic</td>
<td></td>
</tr>
<tr>
<td>15.255.133.150</td>
<td>000bcd-3cbec</td>
<td>dynamic</td>
<td>1</td>
</tr>
</tbody>
</table>

HP Switch(config)# show arp | include 15.255.128.1

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.255.128.1</td>
<td>00000c-07ac00</td>
<td>dynamic</td>
<td>1</td>
</tr>
</tbody>
</table>
```

**Figure C-41. 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.

**Syntax:** 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.
Troubleshooting
Restoring the Factory-Default Configuration

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**

HP recommends 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 Hyper-
Terminal 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
   - 1 stop bit
   - No parity
   - No flow control
   - 8 Bits
3. Use the Reset button to reset the switch. The following prompt should
   then appear in the terminal emulator:

   Enter h or ? for help.

=>

---

Troubleshooting
Restoring a Flash Image
Troubleshooting  
Restoring a Flash Image

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:
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:
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.
Troubleshooting
DNS Resolver

Configuring and Using DNS Resolution with DNS-Compatible Commands

(DNS-compatible commands include ping and traceroute.)

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-87.) 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-43 on page C-89.) 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-45, 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-45. 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:

<table>
<thead>
<tr>
<th>Entity</th>
<th>Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Server IP Address</td>
<td>10.28.229.10</td>
</tr>
<tr>
<td>Domain Name (and Domain Suffix for Hosts in the Domain)</td>
<td>pubs.outdoors.com</td>
</tr>
<tr>
<td>Host Name Assigned to 10.28.229.219 by the DNS Server</td>
<td>docservr</td>
</tr>
<tr>
<td>Fully Qualified Domain Name for the IP address Used By the Document Server (10.28.229.219)</td>
<td>docservr.pubs.outdoors.com</td>
</tr>
<tr>
<td>Switch IP Address</td>
<td>10.28.192.1</td>
</tr>
<tr>
<td>Document Server IP Address</td>
<td>10.28.229.219</td>
</tr>
</tbody>
</table>
With the above already configured, the following commands enable a DNS-compliant command with the host name `docserver` to reach the document server at 10.28.229.219.

```plaintext
HP Switch(config)# ip dns server-address 10.28.229.10
HP Switch(config)# ip dns domain-name pubs.outdoors.com
```

**Figure C-46. Configuring Switch “A” in FigureC-45 To Support DNS Resolution**

As mentioned under “Basic Operation” on page C-88, 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-45 as a target:

```plaintext
HP Switch# ping docservr
10.28.229.219 is alive, time = 1 ms

HP Switch# traceroute docservr
traceroute to 10.28.229.219
  1 hop min, 30 hops max, 5 sec. timeout, 3 probes
  1 10.28.192.2        1 ms       0 ms       0 ms
  2 10.28.229.219      0 ms       0 ms       0 ms
```

**Figure C-47. Example of Ping and Traceroute Execution for the Network in Figure C-45 on Page C-92**

```plaintext
HP Switch# ping docservr.pubs.outdoors.com
10.28.229.219 is alive, time = 1 ms

HP Switch# traceroute docservr.pubs.outdoors.com
traceroute to 10.28.229.219
  1 hop min, 30 hops max, 5 sec. timeout, 3 probes
  1 10.28.192.2        1 ms       0 ms       0 ms
  2 10.28.229.219      0 ms       0 ms       0 ms
```

**Figure C-48. Example of Ping and Traceroute Execution When Only the DNS Server IP Address Is Configured**
Troubleshooting

DNS Resolver

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

IP Routing : Disabled

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 | Subnet Mask
------ + ---------- + ----------- +-----------------
DEFAULT_VLAN | Manual    | 10.28.192.1 | 255.255.255.0
```

Figure C-49. 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-43 on page C-80.

- 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

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS server address not configured</td>
<td>The switch does not have an IP address configured for the DNS server.</td>
</tr>
<tr>
<td>DNS server not responding</td>
<td>The DNS server failed to respond or is unreachable. An incorrect server IP address can produce this result.</td>
</tr>
<tr>
<td>Unknown host &lt; host-name &gt;</td>
<td>The host name did not resolve to an IP address. Some reasons for this occurring include:</td>
</tr>
<tr>
<td></td>
<td>• The host name was not found.</td>
</tr>
<tr>
<td></td>
<td>• The named domain was not found.</td>
</tr>
<tr>
<td></td>
<td>• 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.)</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view switch’s base (default vlan) MAC address and the addressing for any added VLANs</td>
<td>n/a</td>
<td>D-2</td>
<td>D-3</td>
<td>—</td>
</tr>
<tr>
<td>view port MAC addresses (hexadecimal format)</td>
<td>n/a</td>
<td>—</td>
<td>D-3</td>
<td>—</td>
</tr>
</tbody>
</table>

- 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.
MAC Address Management
Determining MAC Addresses

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.)
```

<table>
<thead>
<tr>
<th>Switch Series</th>
<th>MAC Address Allocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Models</td>
<td>The switch's base MAC address is assigned to VLAN (VID) 1 and appears in the <code>walkmib</code> listing after the MAC addresses for the ports. (All VLANs in the switch have the same MAC address.)</td>
</tr>
</tbody>
</table>

Figure D-2. Example of Port MAC Address Assignments on a Switch
Viewing the MAC Addresses of Connected Devices

**Syntax**  
show mac-address [ port-list | mac-addr | vlan <vid>]

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.
Monitoring Resources

Viewing Information on Resource Usage

The switch allows you to view information about the current usage and availability of resources in the Policy Enforcement engine, including the following software features:

- Access control lists (ACL)
- Quality-of-service (QoS), including device and application port priority, and QoS policies
- Dynamic assignment of per-port ACLs and QoS through RADIUS authentication designated as “IDM”, with or without the optional identity-driven management (IDM) application
- Other features, including:
  - Management VLAN
  - DHCP snooping
  - Dynamic ARP protection
  - Jumbo IP-MTU

Policy Enforcement Engine

The Policy Enforcement engine is the hardware element in the switch that manages quality-of-service and ACL policies, as well as other software features, using the rules that you configure. Resource usage in the Policy Enforcement engine is based on how these features are configured on the switch.

Dynamic port ACLs configured by a RADIUS server (with or without the optional IDM application) for an authenticated client determine the current resource consumption for this feature on a specified port. When a client session ends, the resources in use for that client become available for other uses.

Resource usage by the following features (when configured globally or per VLAN), applies across all port groups:

- ACLs
- QoS configurations that use the following commands:
Monitoring Resources
Viewing Information on Resource Usage

- QoS device priority (IP Address) through the CLI using the `qos device-priority` command
- QoS application port through the CLI using `qos tcp-port` or `qos udp-port`
- Management VLAN configuration
- DHCP snooping
- Dynamic ARP protection
- Jumbo IP-MTU

Resource usage on ACLs or QoS are configured per-port through RADIUS authentication.

Displaying Current Resource Usage

To display current resource usage in the switch, enter the `show qos resources` or `show access-list resources` command.

**Syntax:** `show <qos | access-list> resources`

*Displays the resource usage of the Policy Enforcement Engine on the switch by software feature. For each type of resource, the amount still available and the amount used by each software feature is shown. The qos and access-list parameters display the same command output.*

The `show <qos | access-list> resources` command output allows you to view current resource usage and, if necessary, help prioritize and reconfigure software features to free resources reserved for less important features.

Resources are used dynamically, that is, resources are reallocated depending on usage. If IDM ACLs are not configured, then the resources are available for other ACLs, or QoS.

An IDM ACL group uses 4 resources for every ACE (2 address matches times 2 entries per address). When the initial IDM ACE is configured, 256 entries are reserved for IDM ACLs, leaving 128 entries free for allocation. When nothing is configured, all 384 entries display as “free”.

Figure E-1 shows the resource usage on a switch configured for ACLs and QoS.
Monitoring Resources

Viewing Information on Resource Usage

Notes on show resources command output:

- A 1:1 mapping of internal rules to configured policies in the switch does not necessarily exist. As a result, displaying current resource usage is the most reliable method for keeping track of available resources. Also, because some internal resources are used by multiple features, deleting a feature configuration may not increase the amount of available resources.

- Resource usage includes resources actually in use, or reserved for future use by the listed features.

- "Internal dedicated-purpose resources" include the following features:
  - Per-port ingress rate limiting through the CLI using rate-limit in
  - Per-port or per-vlan priority or DSCP through the CLI using qos priority or qos dscp
  - Per protocol priority through the CLI using qos protocol

HP Switch(config)# show access-list resources

<table>
<thead>
<tr>
<th>Group</th>
<th>Rules Allocated</th>
<th>Rules Used</th>
<th>Group Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>CLI-ACL</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>IDM-ACL</td>
<td>256</td>
<td>126</td>
<td>3</td>
</tr>
<tr>
<td>Free</td>
<td>128</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure E-1. Example of Displaying Current Resource Usage with 31 ACE in 1 ACL
Monitoring Resources
When Insufficient Resources Are Available

When Insufficient Resources Are Available

The switch has ample resources for configuring features and supporting RADIUS-authenticated clients (with or without the optional IDM application).

If the resources supporting these features become fully subscribed:

- The current feature configuration continues to operate normally.
- The switch generates an event log notice to say that current resources are fully subscribed.
- Currently engaged resources must be released before any of the following actions are supported:
  - Configuration of new entries for ACL, QoS, IDM, and other features (Management VLAN, DHCP snooping, dynamic ARP protection).
  - Acceptance of new RADIUS-based client authentication requests (displayed as a new resource entry for IDM).

Note

Failure to authenticate a client that presents valid credentials may indicate that insufficient resources are available for the features configured for the client in the RADIUS server. To troubleshoot, check the event log.
Daylight Savings Time on HP Switches

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.
Daylight Savings Time on HP Switches

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 F-1. Menu Interface with “User-Defined” Daylight Time Rule Option](image)

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

Configuring the Savepower led Option

The `savepower led` command provides the ability to turn off port LEDs even when a link exists. If power-saving is enabled, it can be temporarily overridden by the LED Mode button on the front panel. If the LED Mode button is pressed, the LEDs will behave normally (turn on) for a period of 10 minutes, and then turn off again.

*Syntax:* `[no] savepower led

*Turns power-saving option on or off for the LEDs.*

```
HP Switch(config)# savepower led
```

*Figure G-1. Example of 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 G-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 G-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 G-4. Example of Output for show savepower port-low-pwr Command**
Index

Symbols
=> prompt … C-85

Numerics
802.1X
   effect, LLDP … 6-75
   LLDP blocked … 6-42
802.1X access control
   authentication failure, SNMP
   notification … 6-24
   SNMP notification of authentication
   failure … 6-24

A
access
   manager … 6-11
   operator … 6-11
access control list
   See ACL.
ACL
   debug messages … C-49
   dynamic port ACL … E-1
   gateway fails … C-8
   resource usage … E-1
   resources … E-2
   transferring command files … A-26
   troubleshooting … C-5
ACLs
   See ACL.
address
   network manager … 6-2
address table, port ... B-11
address, network manager ... 6-3
advertise location … E-55
AES encryption … 6-7
allocation, class … 3-8
allocation, value … 3-8
ARP protection
   SNMP notification … 6-15, 6-24
asterisk
   meaning in traceroute … C-71
authentication
   notification messages … 6-15, 6-24
authentication trap
   See also SNMP.
authorized IP managers
   SNMP, blocking … 6-1
auto MDI/MDI-X
   configuration, display … 2-16
   operation … 2-14, 2-16
   port mode, display … 2-16
Auto-10 … 4-3, 4-5, 4-15
autonegotiate … 6-55

B
bandwidth
   displaying port utilization … 2-9
boot ROM console … A-2
boot ROM mode … C-85
Bootp
   effect of no reply … C-4
Bootp/DHCP, LLDP … 6-51
broadcast limit … 5-6
broadcast storm … 4-2, C-15
broadcast traffic
   IPX … 5-6
   RIP … 5-6

C
CDP … 6-76, 6-77, 6-78, 6-79, 6-81
Clear button
   restoring factory default configuration … C-84
clear logging … C-44
CLI
   context level … 2-11
command line interface
   See CLI.
communities, SNMP … 6-12
   viewing and configuring with the CLI … 6-13
   viewing and configuring with the menu … 6-11
configuration
   copying … A-22
   impacts of software download on … A-2
   network monitoring … B-18
port ... 2-1
port trunk group ... 4-1
port, duplex ... 2-11
port, speed ... 2-11
restoring factory defaults ... C-84
SNMP ... 6-2, 6-3, 6-9
SNMP communities ... 6-11, 6-13
transferring ... A-22
trap receivers ... 6-17
configuration file
browsing for troubleshooting ... C-73
configuration file, multiple
  copy via tftp ... A-23
  copy via Xmodem ... A-24
console
  measuring network activity ... C-4
  troubleshooting access problems ... C-2
copy
  command output ... A-29
  crash data ... A-31
  crash log ... A-31
  event log output ... A-30
  software images ... A-21
  tftp show-tech ... A-23
copy show tech ... C-76
copy tftp
  show-tech ... A-23
CPU utilization ... B-4
cpu utilization data ... B-5
custom, show tech ... A-23

date format, events ... C-35
default trunk type ... 4-8
DES encryption ... 6-7
DHCP
  address problems ... C-4
  effect of no reply ... C-4
DHCP snooping
  resource usage ... E-1
  SNMP notification ... 6-15, 6-24
DHCP/Bootp, LLDP ... 6-51
dhcp-snooping
  debug messages ... C-49
DHCPv6
  debug messages ... C-50
dhcpv6-client ... C-50
diagnostics tools ... C-66
date format, events ... C-35
default trunk type ... 4-8
DES encryption ... 6-7
DHCP
  address problems ... C-4
  effect of no reply ... C-4
DHCP snooping
  resource usage ... E-1
  SNMP notification ... 6-15, 6-24
DHCP/Bootp, LLDP ... 6-51
dhcp-snooping
  debug messages ... C-49
DHCPv6
  debug messages ... C-50
dhcpv6-client ... C-50
diagnostics tools ... C-66

date format, events ... C-35
default trunk type ... 4-8
DES encryption ... 6-7
DHCP
  address problems ... C-4
  effect of no reply ... C-4
DHCP snooping
  resource usage ... E-1
  SNMP notification ... 6-15, 6-24
DHCP/Bootp, LLDP ... 6-51
dhcp-snooping
  debug messages ... C-49
DHCPv6
  debug messages ... C-50
dhcpv6-client ... C-50
diagnostics tools ... C-66
configuration ... C-90, C-93
configuration error ... C-95
configuration, viewing ... C-94
DNS-compatible commands ... C-90
domain name, fully qualified ... C-87, C-89, C-93
domain suffix ... C-87
domain-name configuration ... C-91
event log messages ... C-95
example ... C-92
host name ... C-88
IPv6 DNS resolution ... C-87
operating notes ... C-94
ping ... C-90, C-93
resolver ... C-87
resolver operation ... C-88
secure management VLAN ... C-95
server address, DHCP not used ... C-95
server IP address ... C-89, C-95
server-address configuration ... C-91
three entries supported ... C-90
three server entries supported ... C-91
traceroute ... C-90, C-93
VLAN, best route selection ... C-95
download
software ... A-18
software using TFTP ... A-2
switch-to-switch ... A-17
TFTP ... A-3
troubleshooting ... A-4
Xmodem ... A-15
See also switch software.
duplex advertisements ... 6-53
duplex information, displaying ... 6-70
duplicate MAC address
   See MAC address.
Dyn1
   See LACP.
dynamic ARP protection
   resource usage ... E-1

E
duplex advertisements ... 6-53
duplex information, displaying ... 6-70
duplicate MAC address
   See MAC address.
Dyn1
   See LACP.
dynamic ARP protection
   resource usage ... E-1

event log
   clearing entries ... C-43
   compared to debug/Syslog operation ... C-48
   debugging by severity level ... C-49, C-59
   debugging by system module ... C-49, C-59
   format, date ... C-35
   generated by system module ... C-35
   how to read entries ... C-34
   listing entries ... C-43
   losing messages ... C-34
   navigation ... C-41
   not affected by debug configuration ... C-65
   security levels ... 6-18
   sending event log messages as traps ... 6-18
   sending messages to Syslog server ... C-49
   severity level ... C-34, C-63
   system module ... C-64
   time format ... C-35
   UDLD warning messages ... 2-29
   used for debugging ... C-49
   used for troubleshooting ... C-34
   excessive frames ... 5-14
   
F
facility
logging ... C-49
factory default configuration
   restoring ... C-84
failure, switch software download ... A-5
fault-tolerance ... 4-3
fiber optics, monitoring links ... 2-22
filter, source-port
   jumbo VLANs ... 5-13
firmware version ... B-4
flow control
   constraints ... 2-12
   effect on rate-limiting ... 5-4
   global ... 2-12
   jumbo frames ... 5-13
   per-port ... 2-12
flow control, status ... B-8
flow sampling ... 6-2
friendly port names
   See port names, friendly.

G
gateway
   routing fails ... C-8
giant frames ... 5-14

H
HP
   Auto-MDIx feature ... 2-14
HP, URL ... 6-2
I
ICMP
resources ... E-2
IDM
resource usage ... E-1
resources ... E-2, E-4
IEEE 802.1d ... C-15
IEEE P802.1AB/D9 ... 6-41
IGMP
host not receiving ... C-10
not working ... C-10
statistics ... B-16
Inbound Telnet Enabled parameter ... C-3
informs
sending to trap receiver ... 6-18
SNMP ... 6-19
IP
duplicate address ... C-4
duplicate address, DHCP network ... C-4
time server address ... 1-8, 1-18
IP address
for SNMP management ... 6-1
IP routing
debug messages ... C-49
IPv6
debug dhcpv6 messages ... C-50
IPX
broadcast traffic ... 5-6
network number ... B-6
J
jumbo frames
configuration ... 5-8
excessive inbound ... 5-13
flow control ... 5-13
GVRP operation ... 5-8
management VLAN ... 5-12
maximum size ... 5-7, 5-11
meshing ... 5-8
MTU ... 5-7
port adds and moves ... 5-8
port speed ... 5-8
security concerns ... 5-13
standard MTU ... 5-7
switch mesh domain ... 5-14
through non-jumbo ports ... 5-14
traffic sources ... 5-8
troubleshooting ... 5-14
VLAN tag ... 5-7
voice VLAN ... 5-12
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, 4-14
Dyn1 ... 4-5
dynamic ... 4-16
enabling dynamic trunk ... 4-13
full-duplex required ... 4-3, 4-14
IGMP ... 4-19
monitoring static trunk ... B-19
no half-duplex ... 4-21
operation not allowed ... C-10
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 ... 5-6
link failures
detecting ... 2-22
link speed, port trunk ... 4-2
link test ... C-67
link-change traps ... 6-15, 6-26
Link-Layer Discovery Protocol
See LLDP.
LLDP
802.1D-compliant switch ... 6-75
802.1X blocking ... 6-42
802.1X effect ... 6-75
active port ... 6-36
adjacent device ... 6-36
advertisement ... 6-36
advertisement content ... 6-51
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>advertisement data</td>
<td>6-67</td>
</tr>
<tr>
<td>advertisement, mandatory data</td>
<td>6-51</td>
</tr>
<tr>
<td>advertisement, optional data</td>
<td>6-52</td>
</tr>
<tr>
<td>advertisements, delay interval</td>
<td>6-47</td>
</tr>
<tr>
<td>CDP neighbor data</td>
<td>6-76</td>
</tr>
<tr>
<td>chassis ID</td>
<td>6-51</td>
</tr>
<tr>
<td>chassis type</td>
<td>6-51</td>
</tr>
<tr>
<td>clear statistics counters</td>
<td>6-72</td>
</tr>
<tr>
<td>comparison with CDP data fields</td>
<td>6-76</td>
</tr>
<tr>
<td>configuration options</td>
<td>6-38</td>
</tr>
<tr>
<td>configuring optional data</td>
<td>6-52</td>
</tr>
<tr>
<td>data options</td>
<td>6-39</td>
</tr>
<tr>
<td>data read options</td>
<td>6-41</td>
</tr>
<tr>
<td>data unit</td>
<td>6-36</td>
</tr>
<tr>
<td>debug logging</td>
<td>6-40</td>
</tr>
<tr>
<td>debug messages</td>
<td>C-49, C-50</td>
</tr>
<tr>
<td>default configuration</td>
<td>6-42</td>
</tr>
<tr>
<td>DHCP/Bootp operation</td>
<td>6-42</td>
</tr>
<tr>
<td>disable, per-port</td>
<td>6-50</td>
</tr>
<tr>
<td>display neighbor data</td>
<td>6-70</td>
</tr>
<tr>
<td>ELIN</td>
<td>6-36</td>
</tr>
<tr>
<td>enable/disable, global</td>
<td>6-46</td>
</tr>
<tr>
<td>features</td>
<td>6-34</td>
</tr>
<tr>
<td>general operation</td>
<td>6-37</td>
</tr>
<tr>
<td>global counters</td>
<td>6-72</td>
</tr>
<tr>
<td>holdtime multiplier</td>
<td>6-47</td>
</tr>
<tr>
<td>hub, packet-forwarding</td>
<td>6-38</td>
</tr>
<tr>
<td>IEEE 802.1AB/D9</td>
<td>6-41</td>
</tr>
<tr>
<td>inconsistent value</td>
<td>6-48</td>
</tr>
<tr>
<td>information options</td>
<td>6-39</td>
</tr>
<tr>
<td>invalid frames</td>
<td>6-73</td>
</tr>
<tr>
<td>IP address advertisement</td>
<td>6-41, 6-75</td>
</tr>
<tr>
<td>IP address subelement</td>
<td>6-51</td>
</tr>
<tr>
<td>IP address, DHCP/Bootp</td>
<td>6-51</td>
</tr>
<tr>
<td>IP address, options</td>
<td>6-51</td>
</tr>
<tr>
<td>IP address, version advertised</td>
<td>6-51</td>
</tr>
<tr>
<td>LLDP-aware</td>
<td>6-36</td>
</tr>
<tr>
<td>LLDPDU</td>
<td>6-36</td>
</tr>
<tr>
<td>mandatory TLVs</td>
<td>6-75</td>
</tr>
<tr>
<td>MIB</td>
<td>6-37, 6-41</td>
</tr>
<tr>
<td>neighbor</td>
<td>6-36</td>
</tr>
<tr>
<td>neighbor data remaining</td>
<td>6-75</td>
</tr>
<tr>
<td>neighbor data, displaying</td>
<td>6-70</td>
</tr>
<tr>
<td>neighbor statistics</td>
<td>6-72</td>
</tr>
<tr>
<td>neighbor, maximum</td>
<td>6-74</td>
</tr>
<tr>
<td>operating rules</td>
<td>6-41</td>
</tr>
<tr>
<td>operation</td>
<td>6-37</td>
</tr>
<tr>
<td>optional data, configuring</td>
<td>6-52</td>
</tr>
<tr>
<td>outbound packet options</td>
<td>6-39</td>
</tr>
<tr>
<td>packet boundaries</td>
<td>6-38</td>
</tr>
<tr>
<td>packet dropped</td>
<td>6-38</td>
</tr>
<tr>
<td>packet time-to-live</td>
<td>6-40</td>
</tr>
<tr>
<td>packet-forwarding</td>
<td>6-38, 6-75</td>
</tr>
<tr>
<td>packets not forwarded</td>
<td>6-36</td>
</tr>
<tr>
<td>per-port counters</td>
<td>6-73</td>
</tr>
<tr>
<td>port description</td>
<td>6-52</td>
</tr>
<tr>
<td>port ID</td>
<td>6-51</td>
</tr>
<tr>
<td>port speed</td>
<td>6-53</td>
</tr>
<tr>
<td>port trunks</td>
<td>6-41</td>
</tr>
<tr>
<td>port type</td>
<td>6-51</td>
</tr>
<tr>
<td>refresh interval</td>
<td>6-46</td>
</tr>
<tr>
<td>reinitialization delay</td>
<td>6-48</td>
</tr>
<tr>
<td>remote management address</td>
<td>6-40</td>
</tr>
<tr>
<td>remote manager address</td>
<td>6-51</td>
</tr>
<tr>
<td>reset counters</td>
<td>6-72</td>
</tr>
<tr>
<td>rxonly</td>
<td>6-50</td>
</tr>
<tr>
<td>setmib, delay interval</td>
<td>6-47</td>
</tr>
<tr>
<td>setmib, reinit delay</td>
<td>6-49</td>
</tr>
<tr>
<td>show advertisement data</td>
<td>6-67</td>
</tr>
<tr>
<td>show commands</td>
<td>6-43, 6-45</td>
</tr>
<tr>
<td>show outbound advertisement</td>
<td>6-68</td>
</tr>
<tr>
<td>SNMP notification</td>
<td>6-39</td>
</tr>
<tr>
<td>SNMP traps</td>
<td>6-39</td>
</tr>
<tr>
<td>spanning-tree blocking</td>
<td>6-42</td>
</tr>
<tr>
<td>standards compatibility</td>
<td>6-41</td>
</tr>
<tr>
<td>statistics</td>
<td>6-72</td>
</tr>
<tr>
<td>statistics, displaying</td>
<td>6-72</td>
</tr>
<tr>
<td>system capabilities</td>
<td>6-52</td>
</tr>
<tr>
<td>system description</td>
<td>6-52</td>
</tr>
<tr>
<td>system name</td>
<td>6-52</td>
</tr>
<tr>
<td>terminology</td>
<td>6-36</td>
</tr>
<tr>
<td>time-to-live</td>
<td>6-38, 6-47</td>
</tr>
<tr>
<td>TLV</td>
<td>6-37</td>
</tr>
<tr>
<td>transmission frequency</td>
<td>6-38</td>
</tr>
<tr>
<td>transmission interval, change</td>
<td>6-46</td>
</tr>
<tr>
<td>transmit and receive</td>
<td>6-39</td>
</tr>
<tr>
<td>transmit/receive modes</td>
<td>6-39</td>
</tr>
<tr>
<td>transmit/receive modes, per-port</td>
<td>6-50</td>
</tr>
<tr>
<td>trap notice interval</td>
<td>6-50</td>
</tr>
<tr>
<td>trap notification</td>
<td>6-49</td>
</tr>
<tr>
<td>trap receiver, data change notice</td>
<td>6-49</td>
</tr>
<tr>
<td>TTL</td>
<td>6-38, 6-40</td>
</tr>
<tr>
<td>txonly</td>
<td>6-50</td>
</tr>
<tr>
<td>VLAN, untagged</td>
<td>6-75</td>
</tr>
<tr>
<td>walkmib</td>
<td>6-41</td>
</tr>
</tbody>
</table>

**LLDP-MED**
displaying speed ... 6-70
ELIN ... 6-63
enable or disable ... 6-38
endpoint support ... 6-55
fast start control ... 6-58
location data ... 6-62
medTlvenable ... 6-60
Neighbors MIB ... 6-70
topology change notification ... 6-56
Voice over IP ... 6-54
load balancing
See port trunk.
logging
facility ... C-49
logging command ... C-55
syntax ... C-49, C-59
logical port ... 4-6
loop, network ... 4-2
mesh
jumbo frames ... 5-14
MIB
HP proprietary ... 6-2
listing ... 6-2
standard ... 6-2
mirroring
See port monitoring.
MLTS ... 6-37
monitoring
links between ports ... 2-22
See port monitoring.
monitoring traffic ... B-18
monitoring, port ... B-19
MPS, defined ... 3-2
Multiline Telephone system ... 6-37
multiple forwarding database ... B-7, B-14
multiple VLAN ... 6-1

M
MAC address ... B-4, D-1
displaying detected devices ... D-4
duplicate ... C-15, C-21
learned ... B-11
port ... D-1, D-2
switch ... D-1
VLAN ... D-1, D-3
walkmib ... D-3
MAC authentication
SNMP notification ... 6-24
mac-count-notify ... 6-82
Maintenance Power Signature ... 3-2
Management Information Base
See MIB.
management VLAN
See VLAN.
management VLAN, DNS ... C-95
manager access ... 6-11
manager password
SNMP notification ... 6-15, 6-24
max frame size, jumbo ... 5-11
MD5 authentication ... 6-7
MDI/MDI-X
configuration, display ... 2-16
operation ... 2-14
port mode, display ... 2-16
media type, port trunk ... 4-2

N
NANP ... 6-37
navigation, event log ... C-42
network management functions ... 6-3, 6-11
network manager address ... 6-2, 6-3
network monitoring
traffic overload ... B-19
Network Monitoring Port screen ... B-18
network slow ... C-4
North American Numbering Plan ... 6-37
notifications
authentication messages ... 6-15, 6-24
configuring trap receivers ... 6-17
enabling for network security ... 6-24
link-change traps ... 6-15
network security ... 6-24

O
operating system
See switch software.
operation not allowed, LACP ... C-10
operator access ... 6-11
OS
version ... A-18
See also switch software.
Overlapping ... C-21
Index – 7

P
password
  SNMP notification … 6-24
  SNMP notification for invalid login … 6-15
pattern matching, show command output … C-79
PCM
  security concerns when deleting public community … 6-3
  SNMP and network management … 6-1
  updating switch software … A-20
PD … 6-37
ping … C-90, C-93
  See also DNS, resolver.
  See also troubleshooting.
ping test … C-67
PoE
  active ports, defined … 3-2
  advertisements … 6-62
  allocation, usage … 3-8
  benefit of LLDP-MED … 6-54
  changing priority level … 3-5
  changing the threshold … 3-5, 3-11
  configuration planning … 3-22
  configuring operation … 3-5
  enable or disable operation … 3-3, 3-6
  EPS, defined … 3-2
  event log messages … 3-23
  LLDP detection, enabling or disabling … 3-12
  manually configuring power levels … 3-9
  messages … 3-23
  MPS, defined … 3-2
  other fault … 3-19
  oversubscribed … 3-2
  overview of status … 3-18
  PD, defined … 3-2
  port-number priority … 3-5
  port-number priority, defined … 3-2
  power, provisioning … 3-3
  priority class … 3-2, 3-5, 3-6
  priority class, defined … 3-2
  priority policies … 3-23
  priority, port … 3-4, 3-5
  PSE, defined … 3-2
  QoS classifiers … 3-23
  related publications … 3-1
  RPS, defined … 3-2
  security … 3-22
  status on specific ports … 3-19
  supporting pre-standard devices … 3-8
  terminology … 3-2
  threshold, global power … 3-4
  threshold, power … 3-10
  viewing status … 3-17
  VLAN assignments … 3-22
policy enforcement engine
  described … E-1
  displaying resource usage … E-1
poll interval
  See TimeP.
port
  address table … B-11
  blocked by UDLD … 2-24
  broadcast limit … 5-6
  CLI access … 2-6
  configuration … 2-1
  configuring UDLD … 2-24
  context level … 2-11
  counters … B-8
  counters, reset … B-9
  duplex, view … 2-7
  enabling UDLD … 2-25
  MAC address … D-2, D-3
  menu access … 2-2
  monitoring … B-18
  monitoring, static LACP trunk … B-19
  speed, view … 2-7
  traffic patterns … B-8
  transceiver status … 2-10
  trunk
    See port trunk.
    utilization … 2-9
    CLI … 2-9
port configuration … 4-1
port names, friendly
  configuring … 2-18
  displaying … 2-19
  summary … 2-17
port security
  port trunk restriction … 4-2
  trunk restriction … 4-6
port trunk … 4-1
  bandwidth capacity … 4-2
  caution … 4-2, 4-7, 4-14
  CLI access … 4-9
  default trunk type … 4-8

Index – 7
enabling dynamic LACP ... 4-13
enabling UDLD ... 2-25
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-18
nonconsecutive ports ... 4-1
port security restriction ... 4-6
removing port from static trunk ... 4-12
requirements ... 4-5
SA/DA ... 4-23
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 ... 4-22
types ... 4-4
UDLD configuration ... 2-24
VLAN ... 4-6
VLAN operation ... 4-5
See also LACP.

port trunk group
interface access ... 4-1
port, active ... 6-36
port-access authentication
SNMP notification ... 6-24
port-based access control
event log ... C-11
LACP not allowed ... 4-18
troubleshooting ... C-11
port-utilization and status displays ... 2-9
power levels, configuring ... 3-9
power-over-ethernet
See PoE.
Power-Sourcing Equipment ... 3-2, 6-37
priority class, defined ... 3-2
priority of operation ... 3-3
prompt, => ... C-85
PSAP ... 6-37
PSE ... 6-37
PSE, defined ... 3-2
Public Safety Answering Point ... 6-37
public SNMP community ... 6-3, 6-11

Q
QoS
See Quality of Service.
Quality of Service
resource usage ... E-1
resources ... E-2

R
RADIUS-assigned ACLs
resources ... E-1
rate display for ports ... 2-9
rate-limiting
cautions ... 5-2
configuration ... 5-2
displaying configuration ... 5-3
displaying configuration ... 5-3
edge ports ... 5-2
effect of flow control ... 5-4
effect on port trunks ... 5-4
how measured ... 5-4
ICMP
See ICMP rate-limiting.
intended use ... 5-2
note on testing ... 5-5
operating notes ... 5-4
optimum packet size ... 5-5
per-port only ... 5-1
purpose ... 5-1
traffic filters ... 5-5
Reset button
restoring factory default configuration ... C-84
reset port counters ... B-9
resetting the switch
factory default reset ... C-84
resource monitor
event log ... E-4
resource usage
displaying ... E-2
insufficient resources ... E-4
restricted write access ... 6-11
RFCs
RFC 1493 ... 6-2
RFC 1515 ... 6-2
RFC 2737 ... 6-41
RFC 2863 ... 6-41
RFC 2922 ... 6-41
RFC 3176 ... 6-31
See also MIB.

RIP
broadcast traffic ... 5-6
debug command ... C-57

RMON ... 6-2
RMON groups supported ... 6-31
routing
gateway fails ... C-8
OSPF debug messages ... C-57
RIP debug messages ... C-57
traceroute ... C-69

S
savepower
command ... G-1
port-low-pwr ... G-2
show led ... G-1

SCP/SFTP
enabling ... A-8
session limit ... A-12, A-15
troubleshooting ... A-14

secure copy
See SCP/SFTP.

secure FTP
See SCP/SFTP.

secure management VLAN
See VLAN.

secure management VLAN, DNS ... C-95

security
enabling network security notifications ... 6-24
Self Test LED
behavior during factory default reset ... C-85
serial number ... B-4
setmib, delay interval ... 6-47
setmib, reinit delay ... 6-49
severity level
event log ... C-34
selecting Event Log messages for debugging ... C-63

sFlow ... 6-2
agent ... 6-31
CLI-owned versus SNMP-owned configurations ... 6-32
configuring via the CLI ... 6-32
destination ... 6-31
sampling-polling information ... 6-34
show commands ... 6-32
SHA authentication ... 6-7
show
displaying specific output ... C-79
exclude option
show
begin option ... C-79
include option ... C-79
interfaces brief ... 2-7
interfaces config ... 2-7
pattern matching with ... C-79
tech, custom ... A-23
show cpu ... B-5
show debug ... C-52
show interfaces
dynamic display ... 2-8
show interfaces display ... C-79
show management ... 1-8, 1-18
show tech ... C-73
custom ... A-23
show-tech ... A-23
slow network ... C-4

SNMP ... 6-1
ARP protection events ... 6-15
authentication notification ... 6-15, 6-24
CLI commands ... 6-11
communities ... 6-2, 6-3, 6-11, 6-12
configuring with the CLI ... 6-13
configuring with the menu ... 6-11
mapping ... 6-9
configure ... 6-2, 6-3
configuring MAC address count ... 6-82
configuring security groups ... 6-21
configuring SNMPv3 notification ... 6-21
configuring SNMPv3 users ... 6-21
configuring trap receivers ... 6-17
configuring trap receivers ... 6-17
DHCP snooping events ... 6-15
different versions ... 6-15
enabling informs ... 6-19
enabling network security traps ... 6-25
enabling SNMPv3 ... 6-20
fixed traps … 6-17
invalid password in login … 6-15
IP … 6-1
link-change traps … 6-15, 6-26
manager password change … 6-15
network security notification … 6-24
notification, LLDP
SNMP notification … 6-39
public community … 6-3, 6-11
supported notifications … 6-15
system thresholds … 6-17
traps … 2-24, 6-2, 6-15
walkmib … D-3
well-known traps … 6-17
SNMP trap, LLDP … 6-49
SNMPv3
"public" community access caution … 6-4
access … 6-3
assigning users to groups … 6-5
authentication, configuring … 6-7
communities … 6-9
enable command … 6-5
enabling … 6-4
encryption, configuring … 6-7
group access levels … 6-9
groups … 6-8
network management levels with snmpv3
only … 6-4
restricted-access option … 6-4
set up … 6-3
users … 6-3
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 … 1-25
menu interface operation … 1-24
operating modes … 1-1
poll interval
See TimeP.
selecting … 1-2
show management … 1-8
unicast mode … 1-2, 1-11
unicast time polling … 1-23
unicast, deleting addresses … 1-24
unicast, replacing servers … 1-24
viewing … 1-3, 1-7
software
See switch software.
software image
See switch software.
software version … B-4
source port filters
jumbo VLANs … 5-13
spanning tree
fast-uplink, troubleshooting … C-16
problems related to … C-15
show tech, copy output … C-74
using with port trunking … 4-6
SSH
enabling or disabling … A-11
TACACS exclusion … A-12
troubleshooting … A-14, C-16
standard MIB … 6-2
statistics … B-2
status and counters menu … B-3
subnets
overlapping … C-21
switch software
download using TFTP … A-2
download, failure indication … A-5
download, switch-to-switch … A-18
download, troubleshooting … A-4
download, using TFTP … A-2
software image … A-1
version … A-4, A-16
Syslog
"debug" severity level as default … C-64, C-65
adding priority description … C-62
compared to event log … C-48
configuring for debugging … C-50
configuring server address … C-49
configuring server IP address … C-55
configuring Syslog servers and debug
destinations … C-49
displaying Syslog configuration … C-52
event log messages sent by default … C-61
logging command … C-55, C-58
operating notes … C-65
overview … C-48
priority-descr … C-63
See also debug command.
sending event log messages … C-48
server configuration … C-60
severity, "debug" ... C-59
specifying severity level events for
debugging ... C-63
specifying system module events for
debugging ... C-64
user facility as default ... C-62, C-65
using event log for debugging ... C-49, C-59

system module
selecting event log messages for
debugging ... C-64

T

TACACS
SSH exclusion ... A-12
task monitor ... B-5
taskusage -d ... B-5
taskUsageShow ... B-5

Telnet
troubleshooting access ... C-3

TFTP
copy command output ... A-29
copy crash data ... A-31
copy crash log ... A-31
copy event log output ... A-30
copying a configuration file ... A-23
copying software image ... A-21
download software using CLI ... A-5
downloading software using console ... A-3
switch-to-switch transfer ... A-17
troubleshooting download failures ... A-4
uploading an ACL command file ... A-26
using to download switch software ... A-2

threshold setting ... 6-3, 6-11
thresholds, SNMP ... 6-17
time format, events ... C-35
time protocol
selecting ... 1-2

TimeP
assignment methods ... 1-1
disabling ... 1-22
enabling and disabling ... 1-19
poll interval ... 1-21
selecting ... 1-2
server address listing ... 1-8, 1-18
show management ... 1-18
viewing and configuring, menu ... 1-16
viewing, CLI ... 1-18

timesync, disabling ... 1-22
time-to-live, LLDP ... 6-38
TLV ... 6-37
TLVs, mandatory ... 6-75
traceroute ... C-90, C-93
asterisk ... C-71
blocked route ... C-72
fails ... C-71

traffic monitoring ... 6-3, 6-11
See also sFlow and RMON.
traffic, monitoring ... B-18
traffic, port ... B-9
transceiver
alarm information
transceiver
error information ... C-28
detail info ... C-27
display info ... C-25
DOM info ... C-27
DOM support ... C-24
error messages ... 2-10
supported products for DOM ... C-24
view status ... 2-9
XENPAK alarm info ... C-28
XENPAK error information ... C-28

trap
CLI access ... 6-17
configuring trap receivers ... 6-17
security levels ... 6-18

trap notification ... 6-49
trap receiver ... 6-2, 6-3
configuring ... 6-17

traps
arp-protect ... 6-25
authentication trap ... 6-25
auth-server-fail ... 6-25
dhcp-snooping ... 6-25
enabling network security notifications ... 6-24
fixed ... 6-17
link-change ... 6-25, 6-26
login-failure-mgr ... 6-25
password-change-mgr ... 6-25
port-security ... 6-25
See also notification.
snmp-authentication ... 6-25
threshold ... 6-17
troubleshooting
ACL ... C-5
approaches ... C-1
browsing the configuration file ... C-73
configuring debug destinations ... C-49
console access problems ... C-2
diagnosing unusual network activity ... C-4
diagnostics tools ... C-66
displaying switch operation ... C-73, C-76
DNS
See DNS.
fast-uplink ... C-15
ping and link tests ... C-67
resource usage ... E-1
restoring factory default configuration ... C-84
spanning tree ... C-15
SSH ... C-16
SSH, SFTP, and SCP Operations ... A-14
switch software download ... A-4
switch won't reboot, shows => prompt ... C-85
traceroute ... C-90
unusual network activity ... C-4
using CLI session ... C-49
using debug and Syslog messaging
using the event log ... C-34
viewing switch operation ... C-73
web browser access problems ... C-2
trunk
See port trunk.
TTL
LLDP ... 6-38
Type-Length-Value ... 6-37
U
UDLD
changing the keepalive interval ... 2-25
changing the keepalive retries ... 2-26
configuring for tagged ports ... 2-26
enabling on a port ... 2-25
event log messages ... 2-29
operation ... 2-23
overview ... 2-22
viewing configuration ... 2-27
viewing statistics ... 2-27
warning messages ... 2-29
unauthorized access ... 6-25
undersize frames ... 5-14
Uni-directional Link Detection
See UDLD.
unrestricted write access ... 6-11
unusual network activity ... C-4
up time ... B-4
USB
copy command output ... A-29
copy crash data ... A-31
copy crash log ... A-31
copy event log output ... A-30
users, SNMPv3
See SNMPv3.
utilization, port ... 2-9
V
version, OS ... A-18
version, switch software ... A-4, A-16
view
duplex ... 2-7
port speed ... 2-7
transceiver status ... 2-9
VLAN
address ... 6-1
configuring UDLD for tagged ports ... 2-26
device not seen ... C-20
event log entries ... C-35
jumbo max frame size ... 5-11
link blocked ... C-15
MAC address ... D-1, D-3
management and jumbo frames ... 5-12
management VLAN, resource usage ... E-1
management VLAN, SNMP block ... 6-1
monitoring ... B-1, B-18
multiple ... 6-1
port configuration ... C-20
secure management VLAN, with DNS ... C-95
switch software download ... A-2
tagging broadcast, multicast, and unicast
traffic ... C-20
VoIP
LLDP-MED support ... 6-54
W
walkmib ... 6-41, D-3
warranty … -ii
Web authentication
  SNMP notification … 6-24
web browser interface
  troubleshooting access problems … C-2
web site, HP … 6-2
write access … 6-11

X
Xmodem
  copy command output … A-29
  copy crash data … A-31
  copy crash log … A-31
  copy event log output … A-30
  copying a configuration file … A-24
  copying a software image … A-21
  download to primary or secondary flash … A-16
  uploading an ACL command file … A-28
  using to download switch software … A-15