



Release Notes:

Version H.08.98 Software

for the ProCurve Series 2600, 2600-PWR Switches

“H” software versions are supported on these switches:

| ProCurve Switch | H.07.xx | H.08.5x and newer |
|-------------------------------------|---------|-------------------|
| ProCurve Switch 2626 (J4900A) | ✓ | ✓ |
| ProCurve Switch 2626 (J4900B) | | ✓ |
| ProCurve Switch 2650 (J4899A) | ✓ | ✓ |
| ProCurve Switch 2650 (J4899B) | | ✓ |
| ProCurve Switch 2626-PWR (J8164A) | ✓ | ✓ |
| ProCurve Switch 2650-PWR (J8165A) | | |
| ProCurve Switch 2600-8-PWR (J8762A) | | H.08.80 |
| ProCurve Switch 6108 (J4902A) | ✓ | |

These release notes include information on the following:

- Downloading switch software and Documentation from the Web ([page 1](#))
 - Clarification of operating details for certain software features ([page 8](#))
 - Software Enhancements ([page 11](#))
 - A listing of software fixes included in releases H.07.02 through H.08.9x ([page 51](#))
-

FEC, CDP Removal

Starting with Software version H.08.77, FEC trunks (Cisco Systems’ FastEtherChannel for aggregated links) are no longer supported, and generation of CDP (Cisco Discovery Protocol) packets are no longer supported. In their place are IEEE standards based LACP aggregated links (as well as statically configured trunks) and generation of LLDP packets for device discovery. For more information, please see: <ftp://ftp.hp.com/pub/networking/software/LLDP-and-LACP-statement.pdf>.

Caution: Startup-Config File Compatibility, Pre-H-08.5x Software

New features in release H.08.5x (or greater) do not exist in H.07.xx software. As a result, the startup-config file is NOT backward-compatible. Users are advised to save a copy of the pre-H.08.5x startup-config file, should you need to run H.07.xx software. See “Transferring Switch Configurations” in Appendix A of the *Management and Configuration Guide*.

Caution: Startup-Config File Compatibility, Pre-H-07.31 Software

The startup-config file saved under version H.07.31 or greater, is NOT backward-compatible with previous software versions. Save a copy of the pre-H.07.31 startup-config file BEFORE UPGRADING to H.07.31 or greater, in case you need to revert to pre-H.07.31 software. See “Transferring Switch Configurations” in the *Management and Configuration Guide*.

**© Copyright 2001, 2006
Hewlett-Packard Development Company, LP.
The information contained herein is subject to change
without notice.**

Publication Number

5990-6003
June, 2006

Applicable Products

| | |
|---|----------|
| ProCurve Switch 2626 | (J4900A) |
| ProCurve Switch 2626 | (J4900B) |
| ProCurve Switch 2650 | (J4899A) |
| ProCurve Switch 2650 | (J4899B) |
| ProCurve Switch 2626-PWR | (J8164A) |
| ProCurve Switch 2650-PWR | (J8165A) |
| ProCurve Switch 2600-8-PWR with Gigabit Uplink | (J8762A) |

Trademark Credits

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

Software Credits

SSH on HP ProCurve Switches is based on the OpenSSH software toolkit. This product includes software developed by the OpenSSH Project for use in the OpenSSH Toolkit. For more information on OpenSSH, visit

[http:// www.openssh.com](http://www.openssh.com).

SSL on HP ProCurve Switches is based on the OpenSSL software toolkit. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information on OpenSSL, visit

[http:// www.openssl.org](http://www.openssl.org).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com)

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
www.procurve.com

Disclaimer

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.

Warranty

See the Customer Support/Warranty booklet included with the product.

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

| | |
|--|-----------|
| Software Management | 1 |
| Downloading Switch Documentation and Software from the Web | 1 |
| Downloading Software to the Switch | 2 |
| TFTP Download from a Server | 3 |
| Xmodem Download From a PC or Unix Workstation | 3 |
| Saving Configurations While Using the CLI | 5 |
| Software Index for ProCurve Networking Products | 6 |
| Minimum Software Versions for Series 2600 Features | 7 |
| OS/Web Browser/Java Compatibility Table | 7 |
| Clarifications | 8 |
| LLDP and LACP | 8 |
| IGMP | 8 |
| Supported Standards and RFCs | 8 |
| Using Delayed Group Flush | 9 |
| Setting Fast-Leave and Forced Fast-Leave from the CLI | 9 |
| IGMP Operating Notes | 10 |
| sFlow Support Clarification | 10 |
| IP Routing Interfaces | 10 |
| Displaying Spanning Tree Configuration Detail | 10 |
| Enhancements | 11 |
| Release H.08.69 Enhancements | 11 |
| IP Lockdown | 11 |
| Release H.08.70 through Release H.08.76 Enhancements | 12 |
| Release H.08.77 Enhancements | 12 |
| Release H.08.82 through Release H.08.85 Enhancements | 12 |
| Release H.08.86 Enhancements | 13 |
| Release H.08.87 through Release H.08.88 Enhancements | 13 |
| Release H.08.89 Enhancements | 13 |
| LLDP-MED Implementation | 13 |

| | |
|---|------------|
| LLDP-MED Topology Change Notification | 17 |
| LLDP-MED Fast Start Control | 18 |
| Advertising Device Capability, Network Policy, PoE Status and Location Data | 18 |
| Configuring Location Data for LLDP-MED Devices | 22 |
| Displaying Advertisement Data | 27 |
| Displaying LLDP Statistics | 31 |
| Release H.08.90 Enhancements | 35 |
| Release H.08.91 and H.08.92 Enhancements | 35 |
| Release H.08.93 | 35 |
| DHCP Option 82: Using the Management VLAN IP Address for the Remote ID | 36 |
| UDP Broadcast Forwarding | 38 |
| Release H.08.95 | 43 |
| Custom Login Banners for the Console and Web Browser Interfaces | 44 |
| Release H.08.97 | 48 |
| TCP/UDP Ports Closure | 48 |
| Software Fixes in Releases H.07.02 - H.08.9x | .51 |
| Release H.07.03 | 51 |
| Release H.07.31 | 52 |
| Release H.07.32 | 53 |
| Release H.07.41 | 53 |
| Release H.07.45 (Never Released) | 54 |
| Release H.07.46 | 55 |
| Release H.07.50 | 55 |
| Release H.07.53 | 56 |
| Release H.07.54 | 56 |
| Release H.07.55 | 56 |
| Release H.07.56 | 58 |
| Release H.08.53 | 58 |
| Release H.08.55 | 59 |
| Release H.08.56 | 60 |
| Release H.08.57 | 60 |
| Release H.08.58 | 60 |

| | |
|---------------------------------|----|
| Release H.08.59 | 61 |
| Release H.08.60 | 61 |
| Release H.08.61 | 61 |
| Release H.08.62 | 61 |
| Release H.08.64 | 62 |
| Release H.08.65 | 62 |
| Release H.08.67 | 62 |
| Release H.08.69 | 62 |
| Release H.08.70 | 63 |
| Release H.08.71 | 63 |
| Release H.08.72 | 63 |
| Release H.08.73 | 64 |
| Release H.08.74 | 64 |
| Release H.08.75 | 64 |
| Release H.08.76 | 64 |
| Release H.08.77 | 65 |
| Release H.08.78 - H.08.81 | 65 |
| Release H.08.82 | 65 |
| Release H.08.83 | 65 |
| Release H.08.84 | 65 |
| Release H.08.85 | 66 |
| Release H.08.86 | 66 |
| Release H.08.87 | 66 |
| Release H.08.88 | 67 |
| Release H.08.89 | 67 |
| Release H.08.90 | 67 |
| Release H.08.91 | 67 |
| Release H.08.92 | 68 |
| Release H.08.93 | 68 |
| Release H.08.94 | 69 |
| Release H.08.95 | 69 |

| | |
|--|-----------|
| Release H.08.96 | 69 |
| Release H.08.97 | 69 |
| Release H.08.98 | 70 |
| Known Software Issues and Limitations | 71 |
| Limitations | 71 |
| Displaying the Fast-Leave Setting on a Port | 71 |

Software Management


Downloading Switch Documentation and Software from the Web

You can download software updates and the corresponding product documentation from ProCurve Networking Web site as described below.

To Download a Software Version:

1. Go to the ProCurve Networking Web site at:
<http://www.procurve.com>.
2. Click on **Software updates** (in the sidebar).
3. Under **Latest software**, click on **Switches**.

To Download Product Documentation: You will need the Adobe® Acrobat® Reader to view, print, and/or copy the product documentation. (HP recommends version 5.0 or greater.)

1. Go to the ProCurve Networking Web site at <http://www.procurve.com>.
2. Click on **Technical support**, then **Product manuals**.
3. Click on the name of the product for which you want documentation.
4. On the resulting Web page, double-click on a document you want.
5. When the document file opens, click on the disk icon  in the Acrobat® toolbar and save a copy of the file.

Downloading Software to the Switch

Caution

The startup-config file generated by the latest software release may not be backward-compatible with the same file generated in your switch by earlier software releases. Refer to the “[Caution: Startup-Config File Compatibility, Pre-H-07.31 Software](#)” on the front page.

HP periodically provides switch software updates through the ProCurve Networking Web site (<http://www.procurve.com>). After you acquire the new software file, you can use one of the following methods for downloading the software to the switch:

- For a TFTP transfer from a server, do either of the following:
 - Click on **Download OS** in the Main Menu of the switch’s menu interface and use the (default) **TFTP** option.
 - Use the **copy tftp** command in the switch’s CLI (see below).
- For an Xmodem transfer from a PC or Unix workstation, do either of the following:
 - Click on **Download OS** in the Main Menu of the switch’s menu interface and select the **Xmodem** option.
 - Use the **copy xmodem** command in the switch’s CLI ([page 3](#)).
- A switch-to-switch file transfer

Note

Downloading a new software version does not change the current switch configuration. The switch configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another switch of the same model and running the same software version.

This section describes how to use the CLI to download software to the switch. You can also use the menu interface for software downloads. For more information, refer to the *Management and Configuration Guide* for your switch.

TFTP Download from a Server

Syntax: `copy tftp flash <ip-address> <remote-os-file> [< primary | secondary >]`

Note that if you do not specify the flash destination, the TFTP download defaults to the primary flash.

For example, to download a software file named H_08_8x.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
HPswitch # copy tftp flash 10.28.227.103 H_08_8x.swi
The primary OS image will be deleted. continue [y/n]? Y
03125K
```

2. When the switch finishes downloading the software file from the server, it displays the progress message shown in 1. When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:

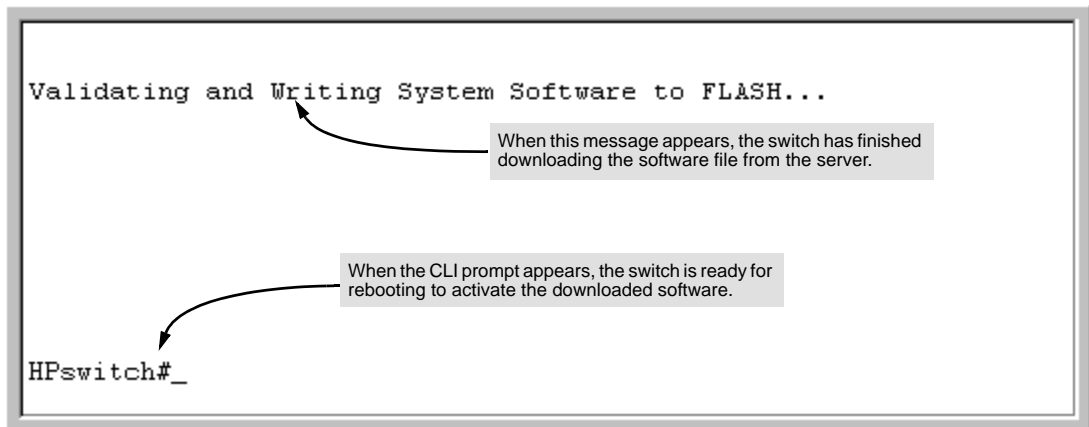


Figure 1. Message Indicating the Switch Is Ready To Activate the Downloaded Software

3. Reboot the switch.

After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

Xmodem Download 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.)

Using Xmodem and a terminal emulator, you can download a switch software file to either primary or secondary flash using the CLI.

Syntax: `copy xmodem flash [< primary | secondary >`

1. To reduce the download time, you may want to increase the baud rate in your terminal emulator and in the switch to a value such as 115200 bits per second. (The baud rate must be the same in both devices.) For example, to change the baud rate in the switch to 115200, execute this command:

```
HPswitch(config)# console baud-rate 115200
```

(If you use this option, be sure to set your terminal emulator to the same baud rate.)

Changing the console baud-rate requires saving to the Startup Config with the "write memory" command. Alternatively, you can logout of the switch and change your terminal emulator speed and allow the switch to AutoDetect your new higher baud rate (i.e. 115200 bps)

2. Execute the following command in the CLI:

```
HPswitch # copy xmodem flash primary
The primary OS image will be deleted. continue [y/n]? Y
Press 'Enter' and start XMODEM on your host...
```

3. 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.

4. If you increased the baud rate on the switch (1), use the same command to return it to its previous setting. (HP recommends a baud rate of 9600 bits per second for most applications.) Remember to return your terminal emulator to the same baud rate as the switch.)
5. Reboot the switch.

After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

Saving Configurations While Using the CLI

The switch operates with two configuration files:

- **Running-Config File:** Exists in volatile memory and controls switch operation. Rebooting the switch erases the current running-config file and replaces it with an exact copy of the current startup-config file. To save a configuration change, you must save the running configuration to the startup-config file.
- **Startup-Config File:** Exists in flash (non-volatile) memory and preserves the most recently-saved configuration as the "permanent" configuration. When the switch reboots for any reason, an exact copy of the current startup-config file becomes the new running-config file in volatile memory.

When using the CLI to make a configuration change, the switch places the change in the running-config file. To preserve the change across reboots, save the change to the startup-config file. Otherwise, the next time the switch reboots, the change will be lost. There are two ways to save configuration changes using the CLI:

- Execute **write memory** from the Manager, Global, or Context configuration level.
- When exiting from the CLI to the Main Menu, press **[Y]** (for Yes) when you see the "Do you want to save current configuration [y/n]?" prompt.

Software Index for ProCurve Networking Products

| Software Letter | ProCurve Networking Products |
|------------------------|---|
| C | 1600M, 2400M, 2424M, 4000M, and 8000M |
| CY | Switch 8100fl Series (8108fl and 8116fl) |
| E | Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl) |
| F | Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324 |
| G | Switch 4100gl Series (4104gl, 4108gl, and 4148gl) |
| H | Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. Switch 6108: H.07.xx and earlier |
| I | Switch 2800 Series (2824 and 2848) |
| J | Secure Router 7000dl Series (7102dl and 7203dl) |
| K | Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, and 5400zl Series (5406zl, 5406zl-48G, 5412zl, and 5412zl-96G) |
| L | Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G) |
| M | Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater. |
| WA | ProCurve Access Point 530 |
| WS | ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module |
| <i>numeric</i> | Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.) |

Minimum Software Versions for Series 2600 Features

For Series 2600 Switches and Hardware.

| ProCurve Device | Minimum Supported Software Version |
|---|------------------------------------|
| Switch 2626 (J4900A) | H.07.31 |
| Switch 2626 (J4900B) | H.08.53 |
| Switch 2650 (J4899A) | H.07.02 |
| Switch 2650 (J4899B) | H.08.53 |
| Switch 2626-PWR (J8164A) | H.07.41 |
| Switch 2650-PWR (J8165A) | H.07.41 |
| Switch 2600-8-PWR (J8762A) with Gigabit Uplink | H.08.80 |

OS/Web Browser/Java Compatibility Table

The switch web agent supports the following combinations of OS browsers and Java Virtual Machines:

| Operating System | Internet Explorer | Java |
|----------------------------|-------------------------------------|---|
| Windows NT 4.0 SP6a | 5.00, 5.01 5.01, SP1 6.0, SP1 | Sun Java 2 Runtime Environment: – Version 1.3.1.12 – Version 1.4.2.05 |
| Windows 2000 Pro SP4 | 5.05, SP2 6.0, SP1 | |
| Windows XP Pro SP2 | 6.0, SP1 | Sun Java 2 Runtime Environment: – Version 1.5.0.02 |
| Windows Server SE 2003 SP1 | 6.0, SP1 | |

Clarifications

LLDP and LACP

Starting with Software version H.08.77, FEC trunks (Cisco Systems' FastEtherChannel for aggregated links) are no longer supported, and generation of CDP (Cisco Discovery Protocol) packets are no longer supported. In their place are IEEE standards-based LACP aggregated links (as well as statically configured trunks) and generation of LLDP packets for device discovery.

For more information, please see: <ftp://ftp.hp.com/pub/networking/software/LLDP-and-LACP-statement.pdf>.

Port Monitoring

The following information updates and clarifies information in Appendix B, "Monitoring and Analyzing Switch Operation" in the *Management and Configuration Guide*—part number 5990-6023, October 2004 edition. Please refer to the section on "Port and Static Trunk Monitoring Features" for detailed information.

All 2600 Series models will support inbound (ingress) and outbound (egress) port monitoring with Version H.08.xx software; however, the 2650 and 2650-PWR require that the "mirror port" be within the same grouping as the monitored ports. On the 2650/2650-PWR switches, ports are grouped as follows: 1-24 + 49, and 25-48 + 50. These groupings represent the connections of ports to NetSwitch ASICs within the models.

IGMP

Note: the following information updates and clarifies information in Chapter 4, "Multimedia Traffic Control with IP Multicast (IGMP)" in the *Advanced Traffic Management Guide*—part number 5990-8853, October 2004. Please review this chapter for a detailed explanation of IGMP operation.

Supported Standards and RFCs

The following are supported:

- RFC2236 (IGMP V.2, with backwards support for IGMP V.1)
- Interoperability with RFC3376 (IGMPv3)
- IETF draft for IGMP and MLD snooping switches (for IGMP V1, V2 V3)

The switch provides full IGMPv2 support as well as full support for IGMPv1 Joins. The switch is interoperable with IGMPv3 Joins as it forwards packets for the joined group from all sources. It does not support IGMPv3 “Exclude Source” or “Include Source” options in the Join Reports. The switch can operate in IGMPv2 Querier mode on VLANs with an IP address.

IGMP is supported in the HP MIB, rather than the standard IGMP MIBs, as the latter reduce Group Membership detail in switched environments.

Using Delayed Group Flush

This feature continues to filter IGMP-Left groups for a specified additional period of time. This is beneficial in switches such as the Series 2600 or 4100gl, where Data-Driven IGMP is not supported. The delay in flushing the group filter prevents stale traffic from being forwarded by the server. Delayed Group Flush is enabled or disabled for the entire switch.

HP recommends that Delayed Group Flush be used whenever Fast Leave or Forced Fast Leave are enabled on the Series 2600 and 2600-PWR Switches. Note that this command must be executed in the configuration context.

Syntax: `igmp delayedflush <time period>`

*Enables the switch to continue to flush IGMP-Left groups for a specified period of time (0 - 255 seconds). The default setting is **Disabled**. To disable, reset the time period to zero.*

Syntax: `Show igmp delayedflush`

Displays the current setting for the switch.

Setting Fast-Leave and Forced Fast-Leave from the CLI

In previous software versions, Fast-Leave and Forced Fast-Leave options for a port were set through the MIB. The following commands now allow a port to be configured for Fast-Leave or Forced Fast-leave operation from the CLI. Note that these command must be executed in a VLAN context

Syntax: `[no] ip igmp fastleave <port-list>`

*Enables IGMP Fast-Leaves on the specified ports in the VLAN (the default setting). In the Config context, use the VLAN specifier, for example, **vlan < vid> ip igmp fastleave <port-list>**. The “no” form disables Fast-Leave on the specified ports.*

`[no] ip igmp forcedfastleave <port-list>`

Forces IGMP Fast-Leaves on the specified ports in the VLAN, even if they are cascaded.

Clarifications

sFlow Support Clarification

To view the IGMP Fast-Leave status of a port use the **show running-config** or **show configuration** commands.

IGMP Operating Notes

- Use Delayed Group Flush on the Series 2600 and 2600-PWR Switches whenever Fast Leave or Forced Fast Leave are set on a port.
- Forced fast leave can be used when there are multiple devices attached to a port.

sFlow Support Clarification

The Series 2600 and 2600-PWR switches do not support sFlow.

IP Routing Interfaces

The Series 2600 and 2600-PWR Switches support a total of 32 routing interfaces (an IP address and a subnet mask). While the switch allows more than 32 IP interfaces to be created, for example, you could create 40 VLANs, each with its own IP address (for a total of 40 routing interfaces), only the first 32 of those interfaces are used for routing. The remaining 8 addresses can only be used to telnet to the switch from their respective VLANs.

Displaying Spanning Tree Configuration Detail

A new CLI command has been added to provide more detailed statistics on spanning tree operation.

Syntax: show spanning-tree <port-list> detail

Lists 802.1D and 802.1w port operating statistics for all ports, or those specified.

Enhancements

Unless otherwise noted, each new release includes the features added in all previous releases.

Enhancements are listed in chronological order, oldest to newest software release. To review the list of enhancements included since the last general release that was published, begin with “[Release H.08.93](#)” on page 35.

Descriptions and instructions for enhancements included in Release H.08.68 or earlier are included in the latest release of manuals for the ProCurve 2600 switches (Oct. 2005), available on the web at http://www.hp.com/rnd/support/manuals/2650_6108.htm

Release H.08.69Enhancements

IP Lockdown

Beginning with release H.08.69 you can use the “IP lockdown” utility to restrict incoming traffic on a port to a specific IP address/subnet, and deny all other traffic on that port for the HP Procurve Switch 2600 and 2800 series.

Operating Rules for IP Lockdown

- Users cannot specify that certain subnets be denied while others are permitted.
- Users cannot filter on protocol or destination IP address.
- The lockdown feature applies to inbound traffic on a port only.
- There is no logging functionality for this feature, i.e. no way to determine if IP address violations occur..
- The same subnet mask must be used for all ports within an 8 port block (1-8, 7-16, etc), for example:
 - If you configure Port 1 with: `ip-lockdown 192.168.0.1/24`
 - Then configure Port 2 with: `ip-lockdown 50.0.0.0/24`
This is an acceptable subnet for port 2
 - Then configure Port 3 with: `ip-lockdown 120.15.32.7/32`
This command would return an error and not be configured due to the differing subnet mask.

Enhancements

Release H.08.70 through Release H.08.76 Enhancements

Using the IP Lockdown Command

The IP lockdown command operates as follows:

Syntax: `ip-lockdown <subnet mask/ips>`

Defines the subnet and related IP addresses allowed for incoming traffic on the port.

The following example will prevent traffic from all IP addresses other than those specified in subnet 192.168.0.1/24 from entering the switch on interface 1.

```
HP Procurve Switch 2626 (config) # interface 1
```

```
HP Procurve Switch 2626 (eth-1) # ip-lockdown 192.168.0.1/24
```

```
HP Procurve Switch 2626 (eth-1) # exit
```

Release H.08.70 through Release H.08.76 Enhancements

Software fixes only; no new enhancements.

Release H.08.77 Enhancements

Implementation of LLDP

For network device discovery solutions, software version H.08.77 implements the industry standard Link Layer Discovery Protocol (LLDP) on your switch, as an alternative to the Cisco Discovery Protocol (CDP).

For more information on LLDP operation and configuration, refer to the latest version of the *Management and Configuration Guide* available on the ProCurve Networking Web site: <http://www.procurve.com>. (Click on Technical support, then Product Manuals, and then select the link for your switch model).

Versions H.08.78 through H.08.81 were never built.

Release H.08.82 through Release H.08.85 Enhancements

Software fixes only; no new enhancements.

Release H.08.86 Enhancements

CLI Port Rate Display

Beginning with release H.08.86 the CLI “**show interface [port list]**” command includes the port rate in the display. The rate displayed is the average for a period of 5 minutes, given in bps for 1G ports, or in Kbps for 10G ports. You can also use the CLI command: **show interface port-utilization** to display port-rate over a period of 5 minutes.

Also added "**show tech transceivers**" to display Serial Number information for installed mGBIC transceivers. Allows removable transceiver serial numbers to be read without removal of the transceivers from the switch.

Release H.08.87 through Release H.08.88 Enhancements

Software fixes only; no new enhancements.

Release H.08.89 Enhancements

LLDP-MED Implementation

Beginning with Release H.08.89, LLDP-MED is supported on ProCurve Series 2600 switches.

LLDP (Link Layer Discovery Protocol) provides a standards-based method for enabling ProCurve switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices.

LLDP-MED (Media-Endpoint-Discovery) extends the LLDP 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 benefits include:

- plug-and-play provisioning for MED-capable, VoIP endpoint devices
- simplified, vendor-independent management enabling different IP telephony systems to interoperate on one network
- automatic deployment of convergence network policies (voice VLANs, Layer 2/CoS priority, and Layer 3/QoS priority)
- configurable endpoint location data to support the Emergency Call Service (ECS) (such as Enhanced 911 service, 999, 112)
- detailed VoIP endpoint data inventory readable via SNMP from the switch
- Power over Ethernet (PoE) status and troubleshooting support via SNMP
- support for IP telephony network troubleshooting of call quality issues via SNMP

This section describes how to configure and use LLDP-MED features in the 2600 switches (running software release H.08.89 or greater) 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

LLDP-MED uses the standard LLDP commands described in the current “Management and Configuration Guide” for the ProCurve 2600 switches, 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.

Note

LLDP-MED is an extension for LLDP, and the switch requires that LLDP be enabled as a prerequisite to LLDP-MED operation.

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).

By using **show** commands to access the switch’s neighbor database (MIB) 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, additional support unique to VoIP applications is also available.

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)

LLDP-MED Endpoint Support

LLDP-MED interoperates with directly connected IP telephony (endpoint) clients having these features and services:

- able to auto-negotiate 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 • serial number • asset ID
 - firmware revision • manufacturer name
 - software revision • model name
- provide information on network connectivity capabilities (for example, a multi-port VoIP phone with Layer 2 switch capability)
- support the fast start capability

Note

LLDP-MED on the ProCurve 2600 switches 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

ProCurve Series 2600 switches running H.08.89 software or newer, support two configurable TLVs for MED-specific capabilities:

- **medTlvEnable:** for per-port enabling or disabling of LLDP-MED operation
- **medPortLocation:** for configuring per-port location or emergency call data

Note

LLDP-MED operation also requires the port speed and duplex TLV (dot3TlvEnable), which is enabled in the default configuration.

Configuring Support for Port Speed and Duplex Advertisements

This feature 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.*

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, or you can use the CLI . For details, see “Displaying the Current Port Speed and Duplex Configuration on a Switch Port” on page 28.

LLDP-MED Topology Change Notification

This optional feature provides information an SNMP application can use to track LLDP-MED connects and disconnects.

Syntax: `lldp top-change-notify < port-list >`

Topology change notification, when enabled on an LLDP port, causes the switch to send an SNMP trap if it detects LLDP-MED endpoint connection or disconnection activity on the port, or an age-out of the LLDP-MED neighbor on the port. The trap includes the following information:

- *the port number (internal) on which the activity was detected (For more in internal port numbers, refer to “LLDP-MED Topology Change Notification” on page 17.)*
- *the LLDP-MED class of the device detected on the port (“LLDP-MED Endpoint Device Classes” on page 15.)*

The **show running** command shows whether the topology change notification feature is enabled or disabled. For example, if ports A1-A10 have topology change notification enabled, the following entry appears in the **show running** output:

```
lldp top-change-notify A1-A10
```

(Default: Disabled)

Note: To send traps, this feature requires access to at least one SNMP server. For information on configuring traps, go to the chapter titled “Configuring for Network Management Applications” in the Management and Configuration Guide for your switch, and refer to one of the following sections:

- SNMPv1 and SNMPv2c Trap Features
- SNMPv3 Notification and Traps

Also, if a detected LLDP-MED neighbor begins sending advertisements without LLDP-MED TLVs, the switch sends a top-change-notify trap.

Note

Topology change notifications provide one method for monitoring system activity. However, because SNMP normally employs UDP, which does not guarantee datagram delivery, topology change notification should not be relied upon as the sole method for monitoring critical endpoint device connectivity.

LLDP-MED Fast Start Control

Syntax: `lldp fast-start-count < 1 - 10 >`

*An LLDP-MED device connecting to a switch port may use the data contained in the MED TLVs from the switch to configure itself. However, the **lldp refresh-interval** setting (default: 30 seconds) for transmitting advertisements can cause an unacceptable delay in MED device configuration. To support rapid LLDP-MED device configuration, the **lldp fast-start-count** command temporarily overrides the **refresh-interval** setting for the **fast-start-count** advertisement interval. This results in the port initially advertising LLDP-MED at a faster rate for a limited time. Thus, when the switch detects a new LLDP-MED device on a port, it transmits one LLDP-MED advertisement per second out the port for the duration of the **fast-start-count** interval. In most cases, the default setting should provide an adequate **fast-start-count** interval.*

(Range: 1 - 10 seconds; Default: 5 seconds)

Note: This global command applies only to ports on which a new LLDP-MED device is detected. It does not override the refresh-interval setting on ports where non-MED devices are detected.

Advertising Device Capability, Network Policy, PoE Status and Location Data

The `medTlvEnable` option on the switch is enabled in the default configuration and supports the following LLDP-MED TLVs:

- LLDP-MED capabilities: This TLV enables the switch to determine:
 - whether a connected endpoint device supports LLDP-MED
 - which specific LLDP-MED TLVs the endpoint supports
 - the device class (1, 2, or 3) for the connected endpoint

This TLV also enables an LLDP-MED endpoint to discover what LLDP-MED TLVs the switch port currently supports.

- network policy operating on the port to which the endpoint is connected (VLAN, Layer 2 QoS, Layer 3 QoS)
- PoE (MED Power-over-Ethernet)
- physical location data — [page 22](#)

Note

LLDP-MED operation requires the `macphy_config` TLV subelement—enabled by default—that is optional for IEEE 802.1AB LLDP operation. Refer to the **`dot3TlvEnable macphy_config`** command on page 16.

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.

Note:

All mandatory TLVs required for LLDP operation are also mandatory for LLDP-MED operation.

Policy Elements

These policy elements may be statically configured on the switch or dynamically imposed during an authenticated session on the switch using a RADIUS server and 802.1X or MAC authentication. (Web authentication does not apply to VoIP telephones and other telecommunications devices that are not capable of accessing the switch through a Web browser.) The QoS and voice VLAN policy elements can be statically configured with the following CLI commands:

```
vlan < vid > voice  
vlan < vid > < tagged | untagged > < port-list >  
int < port-list > qos priority < 0 - 7 >  
vlan < vid > qos dscp < codepoint >
```

Notes

A codepoint must have an 802.1p priority before you can configure it for use in prioritizing packets by VLAN-ID. If a codepoint you want to use shows **No Override** in the **Priority** column of the DSCP policy table (display with **show qos-dscp map**, then use **qos-dscp map < codepoint > priority < 0 - 7 >** to configure a priority before proceeding. For more on this topic, refer to the chapter titled “Quality of Service (QoS): Managing Bandwidth More Effectively” in the *Advanced Traffic Management Guide* for your switch.

Enabling or Disabling medTlvEnable

In the default LLDP-MED configuration, the TLVs controlled by medTlvEnable are enabled.

Syntax: [no] lldp config < port-list > medTlvEnable < medTlv >

- *Enables or disables advertisement of the following TLVs on the specified ports:*
 - *device capability TLV*
 - *configured network policy TLV*
 - *configured location data TLV (Refer to “Configuring Location Data for LLDP-MED Devices” on page 22.)*
 - *current PoE status TLV**(Default: All of the above TLVs are enabled.)*
- *Helps to locate configuration mismatches by allowing use of an SNMP application to compare the LLDP-MED configuration on a port with the LLDP-MED TLVs advertised by a neighbor connected to that port.*

capabilities

This TLV enables the switch to determine:

- *which LLDP-MED TLVs a connected endpoint can discover*
- *the device class (1, 2, or 3) for the connected endpoint*

This TLV also enables an LLDP-MED endpoint to discover what LLDP-MED TLVs the switch port currently supports.

(Default: enabled)

Note: This TLV cannot be disabled unless the network_policy, poe, and location_id TLVs are already disabled.

network-policy

This TLV enables the switch port to advertise its configured network policies (voice VLAN, Layer 2 QoS, Layer 3 QoS), and allows LLDP-MED endpoint devices to auto-configure the voice network policy advertised by the switch. This also enables the use of SNMP applications to troubleshoot statically configured endpoint network policy mismatches.

(Default: Enabled)

Notes: Network policy is only advertised for ports that are configured as members of the voice VLAN. If the port belongs to more than one voice VLAN, then the voice VLAN with the lowest-numbered VID is selected as the VLAN for voice traffic. Also, this TLV cannot be enabled unless the capability TLV is already enabled.

For more information, refer to “Network Policy Advertisements” on page 19

location_id

This TLV enables the switch port to advertise its configured location data (if any). For more on configuring location data, refer to “[Configuring Location Data for LLDP-MED Devices](#)”.

(Default: Enabled)

Note: When disabled, this TLV cannot be enabled unless the capability TLV is already enabled.

poe

This TLV enables the switch port to advertise its current PoE (Power over Ethernet) state and to read the PoE requirements advertised by the LLDP-MED endpoint device connected to the port.

(Default: Enabled)

Note: When disabled, this TLV cannot be enabled unless the capability TLV is already enabled.

For more on this topic, refer to “[PoE Advertisements](#)” , below.

PoE Advertisements

These advertisements inform an LLDP-MED endpoint of the power (PoE) configuration on switch ports. Similar advertisements from an LLDP-MED endpoint inform the switch of the endpoint’s power needs and provide information that can be used to identify power priority mismatches.

Power-over-Ethernet TLVs include the following power data:

- **power type:** indicates whether the device is a power-sourcing entity (PSE) or a powered device (PD). Ports on the J8702A PoE zl module are PSE devices. 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 [29](#).

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 the chapter titled “Power Over Ethernet (PoE) Operation for the Switches” in the *Management and Configuration Guide* for your switch.

Configuring Location Data for LLDP-MED Devices

You can configure a switch port to advertise location data for the switch itself, the physical wall-jack location of the endpoint (recommended), or the location of a DHCP server supporting the switch and/or endpoint. You also have the option of configuring these different address types:

- **civic address:** physical address data such as city, street number, and building information
- **ELIN (Emergency Location Identification Number):** an emergency number typically assigned to MLTS (Multiline Telephone System Operators) in North America
- **coordinate-based location:** attitude, longitude, and altitude information (Requires configuration via an SNMP application.)

Syntax: [no] lldp config < port-list > medPortLocation < Address-Type >

*Configures location or emergency call data the switch advertises per port in the **location_id** TLV. This TLV is for use by LLDP-MED endpoints employing location-based applications.*

Note: *The switch allows one medPortLocation entry per port (without regard to type). Configuring a new medPortLocation entry of any type on a port replaces any previously configured entry on that port.*

civic-addr < COUNTRY-STR > < WHAT > < CA-TYPE > < CA-VALUE > ...
[< CA-TYPE > < CA-VALUE >] ... [< CA-TYPE > < CA-VALUE >]

This command enables configuration of a physical address on a switch port, and allows up to 75 characters of address information.

COUNTRY-STR: *A two-character country code, as defined by ISO 3166. Some examples include **FR** (France), **DE** (Germany), and **IN** (India). This field is required in a **civic-addr** command. (For a complete list of country codes, visit www.iso.org on the world wide web.)*

WHAT: *A single-digit number specifying the type of device to which the location data applies:*

0: *Location of DHCP server*

1: *Location of switch*

2: *Location of LLDP-MED endpoint (recommended application)*

*This field is required in a **civic-addr** command.*

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**.*

—Continued—

— Continued—

*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 0-1 on page -25.*

CA-VALUE: *This is the second entry in a type/value pair, and is an alphanumeric string containing the location information corresponding to the immediately preceding **CA-TYPE** entry. Strings are delimited by either blank spaces, single quotes (‘ ... ’), or double quotes (“ ... “). Each string should represent a specific data type in a set of unique type/value pairs comprising the description of a location, and each string must be preceded by a **CA-TYPE** number identifying the type of data in the string.*

Note: *A switch port allows one instance of any given **CA-TYPE**. For example, if a type/value pair of **6 Atlantic** (to specify “Atlantic” as a street name) is configured on port A5 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 A5.*

—Continued—

— Continued —

elin-addr < emergency-number >

This feature is intended for use in Emergency Call Service (ECS) applications to support class 3 LLDP-MED VoIP telephones connected to a switch covered in this guide in a multiline telephone system (MLTS) infrastructure. An ELIN (Emergency Location Identification Number) is a valid North American Numbering Plan (NANP) format telephone number assigned to MLTS operators in North America by the appropriate authority. The ELIN is used to route emergency (E911) calls to a Public Safety Answering Point (PSAP). (Range: 1-15 numeric characters)

Configuring Coordinate-Based Locations

Latitude, longitude, and altitude data can be configured per switch port using an SNMP management application. For more information, refer to the documentation provided with the application. A further source of information on this topic is *RFC 3825-Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information*.

Note

Endpoint use of data from a medPortLocation TLV sent by the switch is device-dependent. Refer to the documentation provided with the endpoint device.

Table 0-1. Some Location Codes Used in CA-TYPE Fields*

| Location Element | Code | Location Element | Code |
|---|------|--------------------------|------|
| national subdivision | 1 | street number | 19 |
| regional subdivision | 2 | additional location data | 22 |
| city or township | 3 | unit or apartment | 26 |
| city subdivision | 4 | floor | 27 |
| street | 6 | room number | 28 |
| street suffix | 18 | | |
| *The code assignments in this table are examples from a work-in-progress (the internet draft titled “Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information draft-ietf-geopriv-dhcp-civil-06” dated May 30, 2005.) For the actual codes to use, contact the PSAP or other authority responsible for specifying the civic addressing data standard for your network. | | | |

Example of a Location Configuration

Suppose a system operator wanted to configure the following information as the civic address for a telephone connected to her company's network through port A2 of a switch at the following location:

| Description | CA-Type | CA-VALUE |
|----------------------|---------|-------------|
| national subdivision | 1 | CA |
| city | 3 | Widgitville |
| street | 6 | Main |
| street number | 19 | 1433 |
| unit | 26 | Suite 4-N |
| floor | 27 | 4 |
| room number | 28 | N4-3 |

The following figure shows the commands for configuring the above data.

```
ProCurve(config)# lldp config a2 medportlocation civic-addr US 2 1 CA 3 Widgitville 6 Main 19 1433 26 Suite_4-N 27 4 28 N4-3
ProCurve(config)# show lldp config a2

LLDP Port Configuration Detail

Port : A2
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 1. Example of commands for Civic Address Configuration

Displaying Advertisement Data

| Command | Page |
|--|-------|
| show lldp info local-device | below |
| walkmib lldpXdot3LocPortOperMauType | |
| show lldp info remote-device | -29 |
| walkmib lldpXdot3RemPortAutoNegAdvertisedCap | |
| show lldp info stats | -31 |

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 2 on the next page.

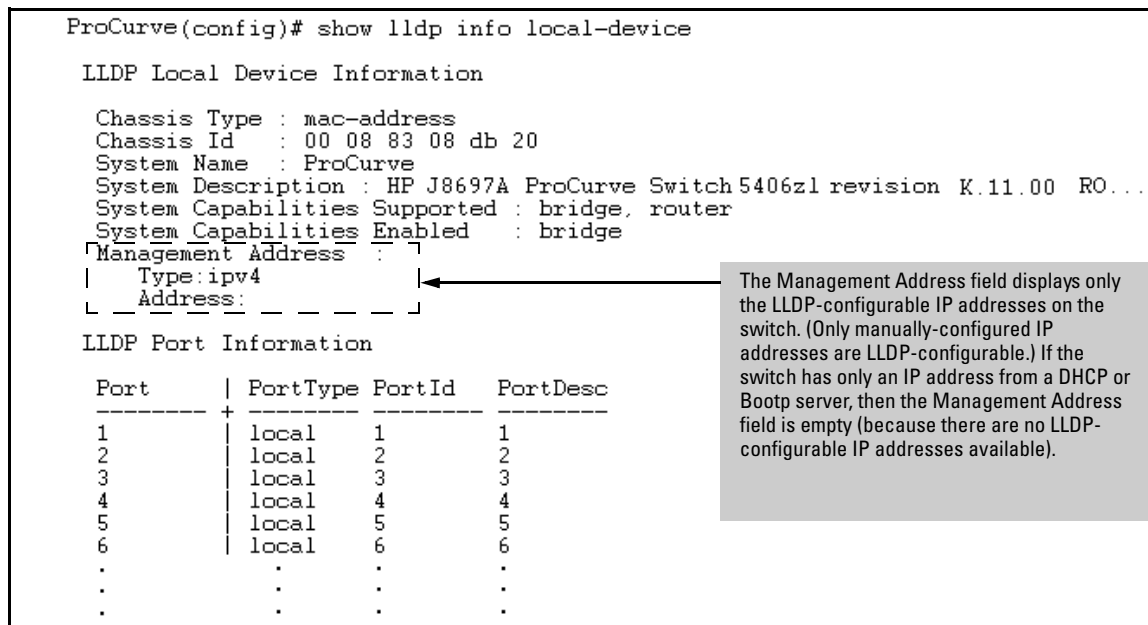


Figure 2. Example of Displaying the Global and Per-Port Information Available for Outbound Advertisements

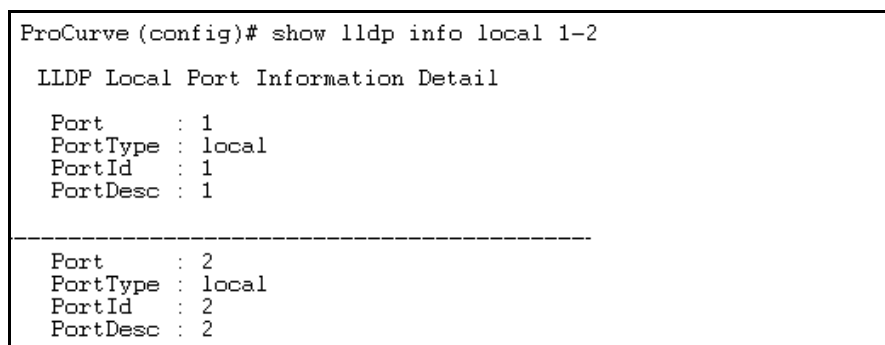


Figure 3. Example of the Default Per-Port Information Content for Ports 1 and 2

Displaying the Current Port Speed and Duplex Configuration on a Switch Port

Port speed and duplex information for a switch port and a connected LLDP-MED endpoint can be compared for configuration mismatches by using an SNMP application. You can also use the switch CLI to display this information, if necessary. The following two commands provide methods for displaying speed and duplex information for switch ports. For information on displaying the currently

configured port speed and duplex on an LLDP-MED endpoint, refer to “Displaying the Current Port Speed and Duplex Configuration on a Switch Port” on page 28.

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 net-work 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.

```
ProCurve# show lldp info remote
```

LLDP Remote Devices Information

| LocalPort | ChassisId | PortId | PortName | SysName |
|-----------|-------------------|--------|----------|------------------------|
| 1 | 00 11 85 c6 54 60 | 17 | 17 | HP ProCurve Switch ... |
| 2 | 00 11 85 cf 66 80 | 33 | 33 | HP ProCurve Switch ... |

Figure 4. Example of a Global Listing of Discovered Devices

```
ProCurve(config)# show lldp info remote-device a2
```

LLDP Remote Device Information Detail

```
Local Port      : A2
ChassisType     : network-address
ChassisId       : 0f ff 7a 5c
PortType        : mac-address
PortId          : 08 00 0f 14 de f2
SysName         : regDN 3004.<IP-Phone-Data>
System Descr    : regDN 3004.<IP-Phone-Data>,h/w rev 0,ASIC rev 0,f/w Boot FW...
PortDescr       : LAN port
```

```
System Capabilities Supported : bridge, telephone
System Capabilities Enabled   : bridge, telephone
```

Remote Management Address

MED Information Detail

```
EndpointClass : Class3
Media Policy Vlan id : 10
Media Policy Priority : 7
Media Policy Dscp : 44
Media Policy Tagged : False
Poe Device Type : PD
Power Requested : 47
Power Source : Unknown
Power Priority : High
```

Indicates the policy configured on the telephone. A configuration mismatch occurs if the supporting port is configured differently.

Figure 5. Example of an LLLDP-MED Listing of an Advertisement Received From an LLDP-MED (VoIP Telephone) Source

Displaying LLDP Statistics

LLDP statistics are available on both a global and a per-port levels. Rebooting the switch resets the LLDP statistics counters to zero. Disabling the transmit and/or receive capability on a port “freezes” the related port counters at their current values.

Syntax `show lldp stats [port-list]`

The global LLDP statistics command displays an overview of neighbor detection activity on the switch, plus data on the number of frames sent, received, and discarded per-port. The per-port LLDP statistics command enhances the list of per-port statistics provided by the global statistics command with some additional per-port LLDP statistics.

Global LLDP Counters:

Neighbor Entries List Last Updated: *Shows the elapsed time since a neighbor was last added or deleted.*

New Neighbor Entries Count: *Shows the total of new LLDP neighbors detected since the last switch reboot. Disconnecting, then reconnecting a neighbor increments this counter.*

Neighbor Entries Deleted Count: *Shows the number of neighbor deletions from the MIB for AgeOut Count and forced drops for all ports. For example, if the admin status for port on a neighbor device changes from **tx_rx** or **txonly** to **disabled** or **rxonly**, then the neighbor device sends a “shutdown” packet out the port and ceases transmitting LLDP frames out that port. The device receiving the shutdown packet deletes all information about the neighbor received on the applicable inbound port and increments the counter.*

Neighbor Entries Dropped Count: *Shows the number of valid LLDP neighbors the switch detected, but could not add. This can occur, for example, when a new neighbor is detected when the switch is already supporting the maximum number of neighbors. Refer to “Neighbor Maximum” on page 32.*

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

— Continued —

— *Continued* —

Per-Port LLDP Counters:

NumFramesRecv: *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](#)” below. 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.*

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.

```
ProCurve(config)# show lldp stats

LLDP Device Statistics

Neighbor Entries List Last Updated : 2 hours
New Neighbor Entries Count : 20
Neighbor Entries Deleted Count : 20
Neighbor Entries Dropped Count : 0
Neighbor Entries AgeOut Count : 20

LLDP Port Statistics
```

| Port | NumFramesRecvd | NumFramesSent | NumFramesDiscarded |
|------|----------------|---------------|--------------------|
| 1 | 628 | 316 | 0 |
| 2 | 21 | 12 | 0 |
| 3 | 0 | 252 | 0 |
| 4 | 446 | 226 | 0 |
| 5 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 |
| . | . | . | . |
| . | . | . | . |

Counters showing frames sent on a port but no frames received on that port indicates an active link with a device that either has LLDP disabled on the link or is not LLDP-aware.

Figure 6. Example of a Global LLDP Statistics Display

```
ProCurve(config)# show lldp stats 1

LLDP Port Statistics Detail

PortName : 1
Frames Discarded : 0
Frames Invalid : 0
Frames Received : 658
Frames Sent : 331
TLVs Unrecognized : 0
TLVs Discarded : 0
Neighbor Ageouts : 0
```

Figure 7. Example of a Per-Port LLDP Statistics Display

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 ProCurve fixed-port or chassis-based switch. Examples of PDs include Voice-over-IP (VoIP) telephones, wireless access points, and remote video cameras.

PSAP (Public Safety Answering Point): PSAPs are typically emergency telephone facilities established as a first point to receive emergency (911) calls and to dispatch emergency response services such as police, fire and emergency medical services.

PSE (Power-Sourcing Equipment): A PSE, such as a PoE module installed in a switch covered in this guide, provides power to IEEE 802.3af-compliant PDs directly connected to the ports on the module.

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.)

Release H.08.90 Enhancements

Software fixes only; no new enhancements.

Release H.08.91 and H.08.92 Enhancements

MSTP Default Path Cost Controls

Summary: 802.1D and 802.1t specify different default path-cost values (based on interface speed). These are used if the user hasn't configured a "custom" path-cost for the interface. The default of this toggle is to use 802.1t values. The reason one might set this control to 802.1D would be for better interoperability with legacy 802.1D STP (Spanning Tree Protocol) bridges.

To support legacy STP bridges, the following commands (options) have been added to CLI:

spanning-tree legacy-path-cost – Use 802.1D values for default path-cost

no spanning-tree legacy-path-cost – Use 802.1t values for default path-cost

The “legacy-path-cost” CLI command does not affect or replace functionality of the “spanning-tree force-version” command. The “spanning-tree force-version” controls whether MSTP will send and process 802.1w RSTP, or 802.1D STP BPDUs. Regardless of what the “legacy-path-cost” parameter is set to, MSTP will interoperate with legacy STP bridges (send/receive Config and TCN BPDUs).

spanning-tree legacy-mode - A “macro” that is the equivalent of executing the “spanning-tree legacy-path-cost” and “spanning-tree force-version stp-compatible” commands.

no spanning-tree legacy-mode - A “macro” that is the equivalent of executing the “no spanning-tree legacy-path-cost” and “spanning-tree force-version mstp-compatible” commands.

When either legacy-mode or legacy-path-cost control is toggled, all default path costs will be recalculated to correspond to the new setting, and spanning tree is recalculated if needed.

Release H.08.93

Release H.08.93 includes the following enhancements

- TheDHCP Option 82 enhancement.
- Support for UDP broadcast forwarding.

DHCP Option 82: Using the Management VLAN IP Address for the Remote ID

This section describes the Management VLAN enhancement to the DHCP option 82 feature. For more information on DHCP option 82 operation, refer to “Configuring DHCP Relay” in the chapter titled “IP Routing Features” in the *Advanced Traffic Management Guide*.

When the routing switch is used as a DHCP relay agent with Option 82 enabled, it inserts a relay agent information option into client-originated DHCP packets being forwarded to a DHCP server. The option automatically includes two suboptions:

- Circuit ID: the identity of the port through which the DHCP request entered the relay agent
- Remote ID: the identity (IP address) of the DHCP relay agent

Using earlier software releases, the remote ID can be either the routing switch’s MAC address (the default option) or the IP address of the VLAN or subnet on which the client DHCP request was received. Beginning with software release H.08.93x, if a Management VLAN is configured on the routing switch, then the Management VLAN IP address can be used as the remote ID.

Syntax: `dhcp-relay option 82 < append | replace | drop > [validate] [ip | mac | mgmt-vlan]`

[ip | mac | mgmt-vlan] : Specifies the remote ID suboption the routing switch will use in Option 82 fields added or appended to DHCP client packets. The choice depends on how you want to define DHCP policy areas in the client requests sent to the DHCP server. If a remote ID suboption is not configured, then the routing switch defaults to the **mac** option.

mgmt-vlan: Specifies the IP address of the (optional) Management VLAN configured on the routing switch. Requires that a Management VLAN is already configured on the switch. If the Management VLAN is multinetted, then the primary IP address configured for the Management VLAN is used for the remote ID.

ip: Specifies the IP address of the VLAN on which the client DHCP packet enters the routing switch. In the case of a multinetted VLAN, the remote ID suboption uses the IP address of the subnet on which the client request packet is received.

mac: Specifies the routing switch’s MAC address. (The MAC address used is the same MAC address that is assigned to all VLANs configured on the routing switch.)
(Default: **mac**)

Example

In the routing switch shown below, option 82 has been configured with **mgmt-vlan** for the Remote ID.

```
ProCurve(config)# dhcp-relay option 82 append mgmt-vlan
```

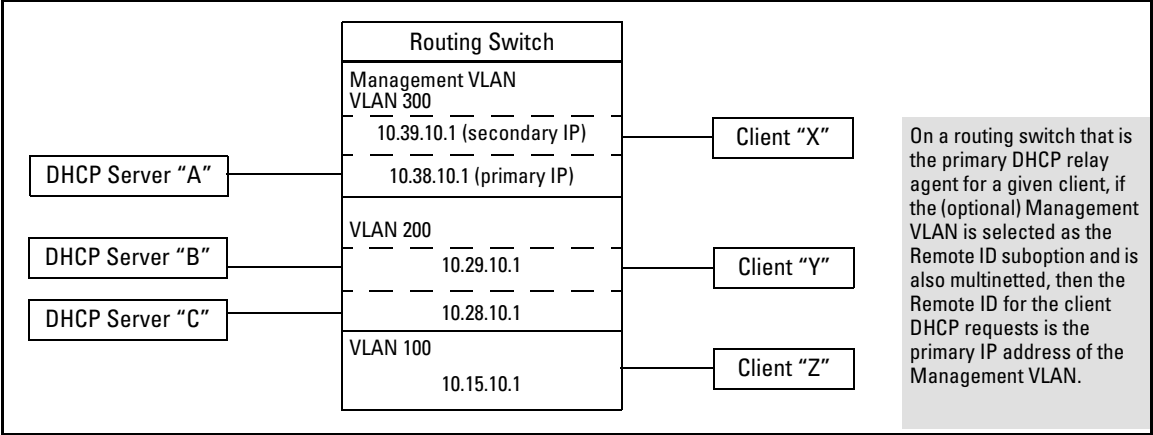


Figure 2. DHCP Option 82 When Using the Management VLAN as the Remote ID Suboption

The resulting effect on DHCP operation for clients X, Y, and Z is shown in [1](#).

Table 1. DHCP Operation for the Topology in Figure 2

| Client | Remote ID | giaddr* | DHCP Server | |
|--------|------------|------------|-------------|---|
| X | 10.38.10.1 | 10.39.10.1 | A only | If a DHCP client is in the Management VLAN, then its DHCP requests can go only to a DHCP server that is also in the Management VLAN. Routing to other VLANs is not allowed. |
| Y | 10.38.10.1 | 10.29.10.1 | B or C | Clients outside of the Management VLAN can send DHCP requests only to DHCP servers outside of the Management VLAN. Routing to the Management VLAN is not allowed. |
| Z | 10.38.10.1 | 10.15.10.1 | B or C | |

*The IP address of the primary DHCP relay agent receiving a client request packet is automatically added to the packet, and is identified as the giaddr (*gateway interface address*). This is the IP address of the VLAN on which the request packet was received from the client. For more information, refer to RFC 2131 and RFC 3046.

Operating Notes

- Routing is not allowed between the Management VLAN and other VLANs. Thus, a DHCP server must be available in the Management VLAN if there are clients in the Management VLAN that require a DHCP server.
- If the Management VLAN IP address configuration changes after **mgmt-vlan** has been configured as the remote ID suboption, the routing switch dynamically adjusts to the new IP addressing for all future DHCP requests.
- The Management VLAN and all other VLANs on the routing switch use the same MAC address.

UDP Broadcast Forwarding

Some applications rely on client requests sent as limited IP broadcasts addressed to a UDP application port. If a server for the application receives such a broadcast, the server can reply to the client. Since typical router behavior, by default, does not allow broadcast forwarding, a client's UDP broadcast requests cannot reach a target server on a different subnet unless the router is configured to forward client UDP broadcasts to that server.

Series 2600 switches with software release H.08.93 and later, that have routing enabled, include optional per-VLAN UDP broadcast forwarding that allows up to 256 server and/or subnet entries on the switch (16 entries per-VLAN). If an entry for a particular UDP port number is configured on a VLAN and an inbound UDP broadcast packet with that port number is received on the VLAN, then the switch routes the packet to the appropriate subnet. (Each entry can designate either a single device or a single subnet. The switch ignores any entry that designates multiple subnets.)

Note

The number of UDP broadcast forwarding entries supported is affected by the number of IP helper addresses configured to support DHCP Relay. Refer to "Operating Notes for UDP Broadcast Forwarding" on page 42.

A UDP forwarding entry includes the desired UDP port number, and can be either an IP unicast address or an IP subnet broadcast address for the subnet the server is in. Thus, an incoming UDP packet carrying the configured port number will be:

- Forwarded to a specific host if a unicast server address is configured for that port number.
- Broadcast on the appropriate destination subnet if a subnet address is configured for that port number.

Note that a UDP forwarding entry for a particular UDP port number is always configured in a specific VLAN and applies only to client UDP broadcast requests received inbound on that VLAN. If the VLAN includes multiple subnets, then the entry applies to client broadcasts with that port number from any subnet in the VLAN.

For example, VLAN 1 (15.75.10.1) is configured to forward inbound UDP packets as shown in table 0-3:

Table 0-3. Example of a UDP Packet-Forwarding Environment

| Interface | IP Address | Subnet Mask | Forwarding Address | UDP Port | Notes |
|-----------|------------|---------------|--------------------|----------|--|
| VLAN 1 | 15.75.10.1 | 255.255.255.0 | 15.75.11.43 | 1188 | Unicast address for forwarding inbound UDP packets with UDP port 1188 to a specific device on VLAN 2. |
| | | | 15.75.11.255 | 1812 | Broadcast address for forwarding inbound UDP packets with UDP port 1812 to any device in the 15.75.11.0 network. |
| | | | 15.75.12.255 | 1813 | Broadcast address for forwarding inbound UDP packets with UDP port 1813 to any device in the 15.75.12.0 network. |

| Interface | IP Address | Subnet Mask | Forwarding Address | UDP Port | Notes |
|-----------|------------|---------------|--------------------|------------|---|
| VLAN 2 | 15.75.11.1 | 255.255.255.0 | <i>None</i> | <i>N/A</i> | Destination VLAN for UDP 1188 broadcasts from clients on VLAN 1. The device identified in the unicast forwarding address configured in VLAN 1 must be on this VLAN. Also the destination VLAN for UDP 1812 from clients on VLAN 1. |
| VLAN 3 | 15.75.12.1 | 255.255.255.0 | <i>None</i> | <i>N/A</i> | Destination VLAN for UDP 1813 broadcasts from clients on VLAN 1. |

Note

If an IP server or subnet entry is invalid, a switch will not try to forward UDP packets to the configured device or subnet address.

Subnet Masking for UDP Forwarding Addresses

The subnet mask for a UDP forwarding address is the same as the mask applied to the subnet on which the inbound UDP broadcast packet is received. To forward inbound UDP broadcast packets as limited broadcasts to other subnets, use the broadcast address that covers the subnet you want to reach. For example, if VLAN 1 has an IP address of 15.75.10.1/24 (15.75.10.1 255.255.255.0), then you can configure the following unicast and limited broadcast addresses for UDP packet forwarding to subnet 15.75.11.0:

| Forwarding Destination Type | IP Address |
|---|--------------|
| UDP Unicast to a Single Device in the 15.75.11.0 Subnet | 15.75.11.X |
| UDP Broadcast to Subnet 15.75.11.0 | 15.75.11.255 |

Configuring and Enabling UDP Broadcast Forwarding

To configure and enable UDP broadcast forwarding on the switch:

1. Enable routing.
2. Globally enable UDP broadcast forwarding.
3. On a per-VLAN basis, configure a forwarding address and UDP port type for each type of incoming UDP broadcast you want routed to other VLANs.

Globally Enabling UDP Broadcast Forwarding

Syntax [no] ip udp-bcast-forward

*Enables or disables UDP broadcast forwarding on the router. Routing must be enabled before executing this command. Using the **no** form of this command disables any **ip forward protocol udp** commands configured in VLANs on the switch. (Default: Disabled)*

Configuring UDP Broadcast Forwarding on Individual VLANs

This command routes an inbound UDP broadcast packet received from a client on the VLAN to the unicast or broadcast address configured for the UDP port type.

Syntax [no] ip forward-protocol udp < ip-address > < port-number | port-name >

*Used in a VLAN context to configure or remove a server or broadcast address and its associated UDP port number. You can configure a maximum of 16 **forward-protocol udp** assignments in a given VLAN. The switch allows a total of 256 **forward-protocol udp** assignments across all VLANs. You can configure UDP broadcast forwarding addresses regardless of whether UDP broadcast forwarding is globally enabled on the switch. However, the feature does not operate unless globally enabled.*

< ip-address >: *This can be either of the following:*

- *The unicast address of a destination server on another subnet. For example: 15.75.10.43.*
- *The broadcast address of the subnet on which a destination server operates. For example, the following address directs broadcasts to All hosts in the 15.75.11.0 subnet: 15.75.11.255.*

Note: *The subnet mask for a forwarded UDP packet is the same as the subnet mask for the VLAN (or subnet on a multinetted VLAN) on which the UDP broadcast packet was received from a client.*

< udp-port-# >: *Any UDP port number corresponding to a UDP application supported on a device at the specified unicast address or in the subnet at the specified broadcast address. For more information on UDP port numbers, refer to “TCP/UDP Port Number Ranges” on page 42.*

< **port-name** >: Allows use of common names for certain well-known UDP port numbers. You can type in the specific name instead of having to recall the corresponding number:

dns: Domain Name Service (53)
nntp: Network Time Protocol (123)
netbios-ns: NetBIOS Name Service (137)
netbios-dgm: NetBIOS Datagram Service (138)
radius: Remote Authentication Dial-In User Service (1812)
radius-old: Remote Authentication Dial-In User Service (1645)
snmp: Simple Network Management Protocol (161)
snmp-trap: Simple Network Management Protocol (162)
tftp: Trivial File Transfer Protocol (69)
timep: Time Protocol (37)

For example, the following command configures the router to forward UDP broadcasts from a client on VLAN 1 for a time protocol server:

```
ProCurve(config)# ip forward-protocol udp 15.75.11.155 timep
```

Displaying the Current IP Forward-Protocol Configuration

Syntax show ip forward-protocol [vlan < vid >]

Displays the current status of UDP broadcast forwarding and lists the UDP forwarding address(es) configured on all static VLANs in the switch or on a specific VLAN.

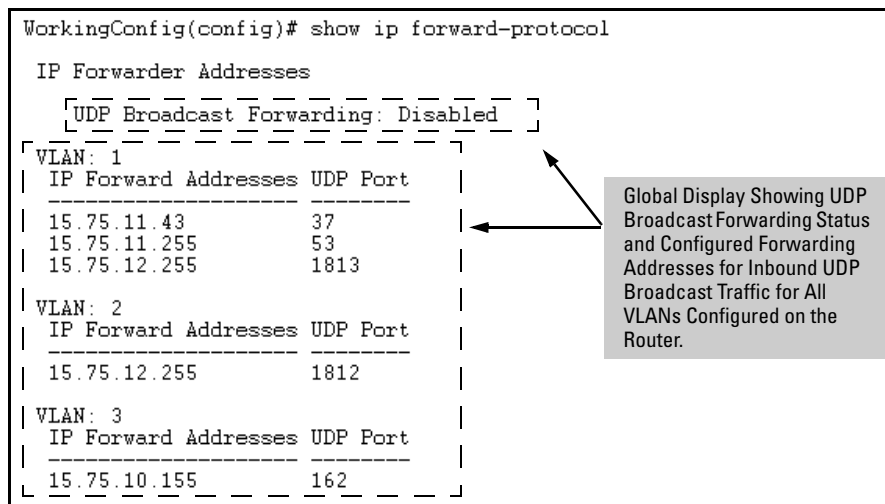


Figure 0-1. Displaying Global IP Forward-Protocol Status and Configuration

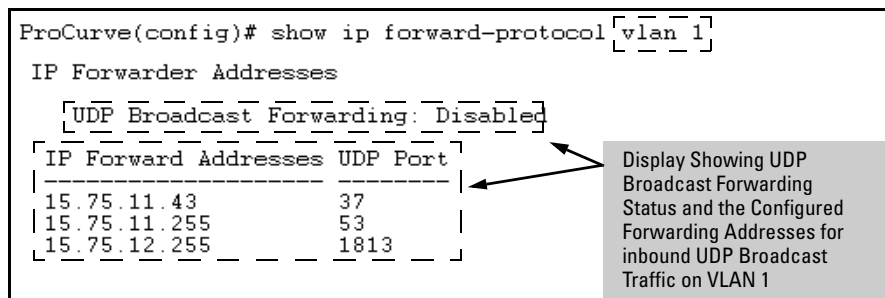


Figure 0-2. Displaying IP Forward-Protocol Status and Per-VLAN Configuration

Operating Notes for UDP Broadcast Forwarding

Maximum Number of Entries. The number of UDP broadcast entries and IP helper addresses combined can be up to 16 per VLAN, with an overall maximum of 256 on the switch. (IP helper addresses are used with the switch's DHCP Relay operation. For example, if VLAN 1 has 2 IP helper addresses configured, you can add up to 14 UDP forwarding entries in the same VLAN.

TCP/UDP Port Number Ranges. There are three ranges:

- Well-Known Ports: 0 - 1023
- Registered Ports: 1024 - 49151
- Dynamic and/or Private Ports: 49152 - 65535

For more information, including a listing of UDP/TCP port numbers, go to the *Internet Assigned Numbers Authority* (IANA) web site at:

<http://www.iana.org>

Then click on:

Protocol Number Assignment Services

P (Under “Directory of General Assigned Numbers” heading)

Port Numbers

Messages Related to UDP Broadcast Forwarding

| Message | Meaning |
|--|---|
| udp-bcast-forward: IP Routing support must be enabled first. | Appears in the CLI if an attempt to enable UDP broadcast forwarding has been made without IP routing being enabled first. Enable IP routing, then enable UDP broadcast forwarding. |
| UDP broadcast forwarder feature enabled | UDP broadcast forwarding has been globally enabled on the router. Appears in the Event Log and, if configured, in SNMP traps. |
| UDP broadcast forwarder feature disabled | UDP broadcast forwarding has been globally disabled on the router. This action does not prevent you from configuring UDP broadcast forwarding addresses, but does prevent UDP broadcast forwarding operation. Appears in the Event Log and, if configured, in SNMP traps. |
| UDP broadcast forwarder must be disabled first. | Appears in the CLI if you attempt to disable routing while UDP forwarding is enabled on the switch. |

Release H.08.95

Release H.08.95 includes the following enhancements:

- Enhancement to display Port Name along with Port number on the Web User Interface Status and Configuration screens.
- Enabled custom login banners with "Message of the Day" (MOTD) feature.

Custom Login Banners for the Console and Web Browser Interfaces

You can now configure the switch to display a login banner of up to 320 characters when an operator initiates a management session with the switch through any of the following methods:

- Telnet
- serial connection
- SSHv2 (SSHv1 does not include support for banners.)
- Web browser

In the factory default configuration, the switch displays the following default banner:

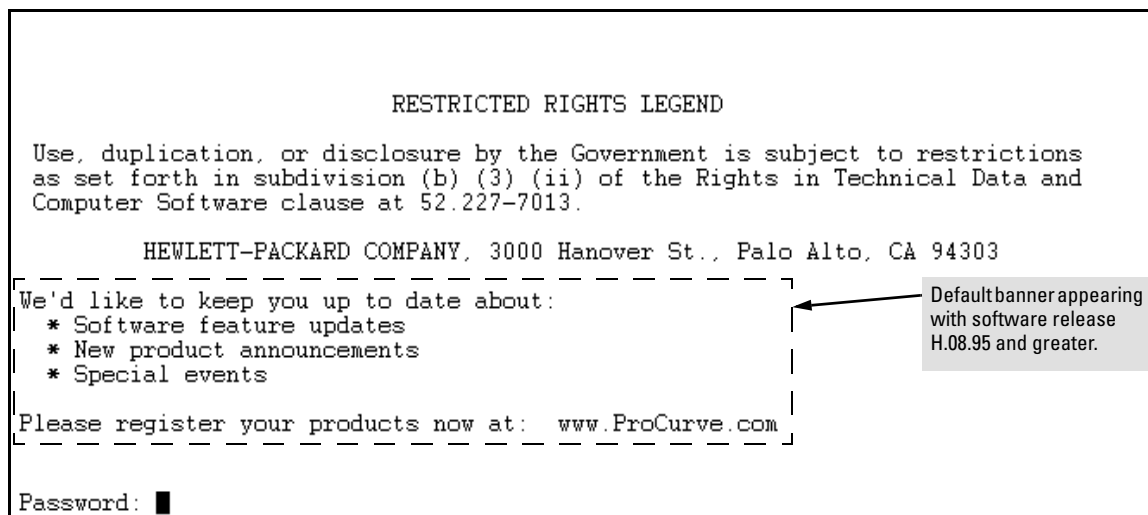


Figure 1. The Default Login Banner

Note

The switch's Web browser interface does not display the default banner.

Banner Operation with Telnet, Serial, or SSHv2 Access

When a system operator begins a login session, the switch displays the banner above the local password prompt or, if no password is configured, above the **Press any key to continue prompt**. Entering a correct password or, if no password is configured, pressing any key clears the banner from the CLI and displays the CLI prompt. (Refer to figure1 on page 44.)

Banner Operation with Web Browser Access

When a system operator uses a Web browser to access the switch, the text of a non-default banner configured on the switch appears in a dedicated banner window with a link to the Web agent home page. Clicking on **To Home Page** clears the banner window and prompts the user for a password (if configured). Following entry of the correct username/password information (or if no username/password is required), the switch then displays either the Registration page or the switch's home page. Note that if the banner feature is disabled or if the switch is using the factory-default banner shown in figure 1, then the banner page does not appear in the Web browser when an operator initiates a login session with the switch.

Configuring and Displaying a Non-Default Banner

You can enable or disable banner operation using either the switch's CLI or an SNMP application. The steps include:

1. Enable non-default banner operation and define the endpoint delimiter for the banner.
2. Enter the desired banner text, including any specific line breaks you want.
3. Enter the endpoint delimiter.
4. Use **show banner motd** to display the current banner status.

Syntax: banner motd < delimiter >
no banner motd

This command defines the single character used to terminate the banner text and enables banner text input. You can use any character except a blank space as a delimiter. The **no** form of the command disables the login banner feature.

< banner-text-string >

*The switch allows up to 320 banner characters, including blank spaces and CR-LF ([Enter]). (The tilde “~” and the delimiter defined by **banner motd <delimiter>** are not allowed as part of the banner text.) While entering banner text, you can backspace to edit the current line (that is, a line that has not been terminated by a CR-LF.) However, terminating a line in a banner by entering a CR-LF prevents any further editing of that line. To edit a line in a banner entry after terminating the line with a CR-LF requires entering the delimiter described above and then re-configuring new banner text.*

The banner text string must terminate with the character defined by banner motd < delimiter >.

Example of Configuring and Displaying a Banner

Suppose a system operator wanted to configure the following banner message on her company's 5300xl switches:

```
This is a private system maintained by the
      Allied Widget Corporation.
Unauthorized use of this system can result in
      civil and criminal penalties!
```

In this case, the operator will use the [Enter] key to create line breaks, blank spaces for line centering, and the % symbol to terminate the banner message.

```
ProCurve(config)# banner motd %
Enter TEXT message. End with the character '%'
      This is a private system maintained by the
      Allied Widget Corporation.
      Unauthorized use of this system can result in
      civil and criminal penalties!%
ProCurve(config)# write memory
```

Figure 2. Example of Configuring a Login Banner

To view the current banner configuration, use either the **show banner motd** or **show running** command.

```
ProCurve(config)# show banner motd

Banner Information

Banner status: Enabled
Configured Banner:

      This is a private system maintained by the
      Allied Widget Corporation.
      Unauthorized use of this system can result in
      civil and criminal penalties!
```

Figure 3. Example of show banner motd Output

```
ProCurve(config)# show running
Running configuration:
; J4850A Configuration Editor; Created on release #E.10.02

hostname "ProCurve"
module 1 type J8161A
module 2 type J8161A
snmp-server community "notpublic" Unrestricted
vlan 1
    name "DEFAULT_VLAN"
    untagged A1-A24,B1-B24
    ip address dhcp-bootp
    exit
banner motd "
    _ _ _ _ _ This is a private system maintained by the _ _ _ _ _
    _ _ _ _ _ Allied Widget Corporation. _ _ _ _ _
    _ _ _ _ _ Unauthorized use of this system can result in _ _ _ _ _
    _ _ _ _ _ civil and criminal penalties! _ _ _ _ _
password manager
password operator
```

Shows the current banner configuration.

Figure 4. The Current Banner Appears in the Switch's Running-Config File

The next time someone logs onto the switch's management CLI, the following appears:

```
Copyright (C) 1991-2005 Hewlett-Packard Co. All Rights Reserved.

RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure by the Government is subject to restrictions
as set forth in subdivision (b) (3) (ii) of the Rights in Technical Data and
Computer Software clause at 52.227-7013.

HEWLETT-PACKARD COMPANY, 3000 Hanover St., Palo Alto, CA 94303

_ _ _ _ _ This is a private system maintained by the _ _ _ _ _
_ _ _ _ _ Allied Widget Corporation. _ _ _ _ _
_ _ _ _ _ Unauthorized use of this system can result in _ _ _ _ _
_ _ _ _ _ civil and criminal penalties! _ _ _ _ _
_ _ _ _ _

Password: █
```

The login screen displays the configured banner.
Entering a correct password clears the banner and displays the CLI prompt.

Figure 5. Example of CLI Result of the Login Banner Configuration

If someone uses a Web browser to log in to the switch interface, the following message appears:

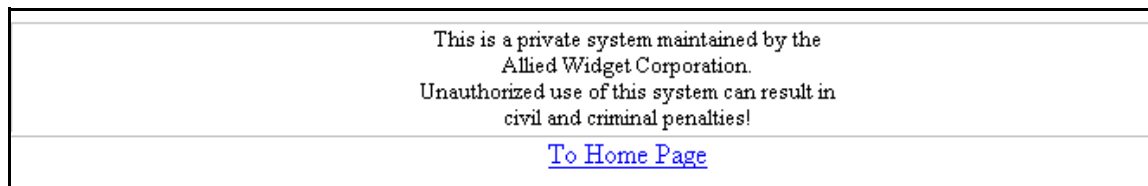


Figure 6. Example of Web Browser Interface Result of the Login Banner Configuration

Operating Notes

- The default banner appears only when the switch is in the factory default configuration. Using **no banner motd** deletes the currently configured banner text and blocks display of the default banner. The default banner is restored only if the switch is reset to its factory-default configuration.
- The switch supports one banner at any time. Configuring a new banner replaces any former banner configured on the switch.
- If the switch is configured with **ssh version 1** or **ssh version 1-or-2**, configuring the banner sets the SSH configuration to ssh version 2 and displays the following message in the CLI:

```
Warning: SSH version has been set to v2.
```
- If a banner is configured, the switch does not allow configuration with **ssh version 1** or **ssh version 1-or-2**. Attempting to do so produces the following error message in the CLI:

```
Banner has to be disabled first.
```
- If a banner is enabled on the switch, the Web browser interface displays the following link to the banner page:

Notice to all users

Release H.08.97

Release H.08.97 includes the following enhancement.

TCP/UDP Ports Closure

In earlier software releases, certain UDP ports were always open. Beginning with software release H.08.97, all TCP/UDP ports on the ProCurve Series 2600 switches will remain closed until the associated services are enabled on the switch.

The following ports and services are affected by this change:

| Port | Service |
|------|-----------------|
| 69 | TFTP |
| 161 | SNMP |
| 1507 | Stacking (SNMP) |

To open any of these ports, the respective services must first be enabled on the switch. For information on how to enable/disable these services, refer to the following command listings . For details on each service, refer to the latest version of the switch's software documentation available on the ProCurve Networking Web site.

Enabling/Disabling TFTP

The TFTP server and client can be enabled and/or disabled independently.

Syntax: [no] tftp < client | server >

Enables or disables the TFTP client.

client: *Enables or disables the TFTP client.*

(Default: disabled)

server: *Enables or disables the TFTP server.*

(Default: disabled)

Note: Both the **tftp** command (with no arguments) and the **tftp client** command can be used to enable or disable the tftp client.

Enabling/Disabling SNMP

To enable/disable SNMP, use the following commands.

Syntax: [no] snmp-server enable

Enables or disables SNMP v1/v2.

(Default: disabled)

Syntax: [no] snmpv3 enable

Enables or disables SNMP v3.

(Default: disabled)

Notes

- The SNMP port (161) will be opened if either SNMP v1/2 or SNMP v3 are enabled, or remain closed if both are disabled.

- The **snmp-server enable** command takes precedence over the **snmp-server enable traps** command that is used to enable or disable authentication traps to be sent when a management station attempts an unauthorized access.
 - If SNMP is disabled, both the SNMP port (161) and the stacking port (1507) will remain closed.
-

Enabling/Disabling Stacking

To enable/disable stacking, use the following command.

Syntax: [no] stack

Enables stacking (SNMP) on the switch. (Default: disabled)

Note

The **stack** command exists in previous software versions. In this implementation, however, both stacking and SNMP must be enabled to open the port on the switch. If either feature is disabled, the port will remain closed.

Software Fixes in Releases H.07.02 - H.08.9x

Software fixes are listed in chronological order, oldest to newest software release. To review the list of fixes included since the last general release that was published, begin with [“Release H.08.93” on page 68](#).

Unless otherwise noted, each new release includes the fixes added in all previous releases.

Release H.07.02 was the original software released to support the HP ProCurve Switch 2650 and the Switch 6108.

Release H.07.03

Problems Resolved in Release H.07.03

- **Agent Unresponsive (PR_5903)** — The switch may get into a state where end nodes and other network devices cannot contact (ping, telnet, SNMP, etc) switch's agent.
- **Crash (PR_5877)** — When setting the host name to a very long (~20 characters) string, the switch may crash with a bus error similar to:

```
-> Bus error: HW Addr=0x29283030 IP=0x002086ac Task='mSnmpCtrl' Task ID=0x165ae00.
```
- **Crash (PR_5345)** — Switch may crash with a message similar to:

```
->Assertion failed:0, file drvmem.c, line 167
```
- **IGMP (PR_5991)** — If switch receives an IGMPv3 Join with a reserved Multicast address, or an invalid IP Multicast address, the switch may crash with a message similar to:

```
-> Software exception at alloc_free.c:479 -- in 'tDevPollTx' Task ID = 0x1900f18 buf_free: corrupted buffer
```
- **IGMP (PR_6001)** — When an IGMP v3 Join contains an invalid IP Multicast address or a reserved IP Multicast address in the IGMP Group Address field, the switch will attempt to stop processing the Join, and mistakenly double-free, or double-forward the Join packet. One possible symptom is a switch crash similar to:

```
->Software exception at alloc_free.c ... buf_free: corrupted buffer
```
- **SNMP (PR_6006)** — The ifAlias OID is defaulted to "not assigned", which may cause network management applications such as Network Node Manager to log error messages. [The fix is to default ifAlias to a zero-length string, as stated in the MIB.]

Release H.07.31

Release numbers H.07.04 through H.07.30 were never created. Release H.07.31 is the first software release for the HP ProCurve Switch 2626.

Problems Resolved in Release H.07.31

- **CLI (PR_81948)** — A duplicate "enable" command is present in the Interface Configuration text within the CLI.
- **CLI (PR_82475)** — Within the CLI, the "ip" auto-extend help text for "source-route" is incorrect.
- **Config / Switch Management (PR_89846)** — When the "no web-management" command is executed, "no telnet-server" is also added to the running config. A loss of Telnet connectivity is only seen when the config file is saved to a TFTP server, then copied back.
- **IGMP (PR_90376)** — In some cases, the switch would display "0.0.0.0" for the output of the CLI command "show ip igmp."
- **IP Stack Mgmt/Web (PR_89753)** — A bus error occurs when accessing the close-up view of a 15-member stack (IP Stack Management) through the Web interface.
- **IP Routing (PR_90711)** — Switch incorrectly identifying packets routed from a trunk port across the stack link as port security violations. This resulted in overrunning the CPU queues and causing management problems.
- **QOS (PR_90937)** — Switch only utilizing three of the four available priority queues.
- **Spanning Tree (PR_90412)** — Enhancements to 802.1w operation to address version 3 BPDU communication issues.
- **Self Test (PR_90777)** — A self test error may occur when a Gigabit-SX, or LX mini-GBIC module is inserted into the switch while powered on.
- **UI / CLI (PR_90302)** — Addressed grammatical errors for the "interfaces" command when "show <tab>" is executed.
- **UI (PR_81885)** — In the absence of a time server, the switch may report that it is the year "26".
- **Web/Stack Mgmt (PR_88743)** — Inverted IP address displayed in the Identity tab when the IP Stack Member switch is accessed through the IP Stack Commander switch.
- **Web-Browser Interface (PR_82530)** — A client using Sun java 1.3.X or 1.4.X to access the Web-Browser Interface of the switch, may cause the switch's CPU utilization to increase causing agent processes (such as console, telnet, STP, ping, etc.) to stop functioning.

- **Web-Browser Interface (PR_82652)** — The Web agent is showing disabled ports as "Port Not Connected", rather than "Port Disabled."
- **Web-Browser Interface / Port Security (PR_88612)** — When static MAC addresses are configured under port security to allow PCs to communicate through the switch, and one of those MAC addresses is removed via the Web interface of the 2650 and then re-entered, the owner of that MAC address cannot communicate again until the link of that port is toggled.

Release H.07.32

Problems Resolved in Release H.07.32

- **Agent Hang (PR_92802)** — The switch may become unresponsive or hang due to UDP port 1024 broadcast packets never being freed, after the TIMEP and SNTP clients are disabled on the switch.
- **VLAN (PR_92466)** — The switch may experience a Bus error related to 802.1X/unauthorized VLAN. The Bus error is similar to:


```
Bus error: HW Addr=0x3861000c IP=0x002df470 Task='mAdMgrCtrl '  
Task ID=0x16e616 0 fp: 0x006a090c sp:0x016e5df0 lr:0x0021d6d8
```
- **Web Browser (PR_90068)** — There is a Netscape 4.7, 7.0, and 7.1 problem when changing any attribute in the stacking menu. After clicking 'OK', Netscape returns error "The document contains no data. Try again later."

Release H.07.41

Release numbers H.07.33 through H.07.40 were never created.

Problems Resolved in Release H.07.41

- **Bridge Management (PR_82358)** — Switch was not forwarding multicast packets with address of 01-80-C2-00-00-10 reserved for Bridge Management functions.
- **Crash (PR_95850)** — software exception in ISR at hardware.c:3871
- **Link (PR_96223/95598)** — Mini-GBIC ports that were configured to a forced speed/duplex (vs. 'auto' mode) were incorrectly reporting Link state when there were no fiber links connected.
- **Management (PR_92720)** — Switch 'show CPU' reports 136 percent busy. The calculation for CPU busy was being performed incorrectly.

- **Port Security (PR_88612)** — Port security enabled via the MIB hpSecPtLearnMode was improperly filtering a host MAC entry, when the entry was removed via the CLI, SNMP or Web interface.
- **Web (PR_82652)** — Web agent showing disabled ports as "Port Not Connected."

Release H.07.45 (Never Released)

Release numbers H.07.42 through H.07.44 were never created.

Problems Resolved in Release H.07.45

- **CLI (PR_97671)** — Uncertain error message when trying to add more than the maximum VLANs
- **Crash (PR_95525)** — Switch is crashing with a bus error from the instrumentation data structure.

`Crash msg: Bus error: HW Addr=0xe1f08796 IP=0x003a51b4 Task='mInstCtrl'
Task I D=0x1767af8 fp: 0x00000006 sp:0x01767988 lr:0x003979a4`
- **IP Stacking (PR_97323)** — back-of-box stacking support for all current stackable products
- **Port Security (PR_98193)** — "port-security learn-mode configured" not working properly.
- **RSTP (PR_1000001612)** — Port takes ~30 seconds to go into the Forwarding state
- **Web (PR_81848)** — Clear changes button does not work for the Default Gateway or VLAN selections
- **Web (PR_82039)** — When using the Web agent and you select GVRP mode, a user can select a port and then select nothing as an option for the port mode and all ports below the selected port disappear.
- **Web (PR_82199)** — VLAN port modification shows misleading mode
- **Web (PR_92078)** — After making changes under the Device Features tab, Web page never fully loads.
- **Web Mgmt Crash (PR_92826)** — Commander switch for IP-stack / Web Mgmt Crash of commander. With an eight switch IP stack, using the Web interface can cause the commander switch to crash. If the user-administrator using the WEB interface selects options too quickly or moves from one option to another, the Web agent can freeze and become unresponsive. The commander can also crash with a Bus Error. Telnet and console interfaces both can also become unresponsive.
- **Web (PR_97407)** — Port security error message is unclear with mac lockdown feature
- **Web (PR_98500)** — Browser window spontaneously closes
- **Web (PR_1000000452)** — when you reset a device using the Web Browser, the refreshed page returns to a incorrect URL.

Release H.07.46

Problems Resolved in Release H.07.46

- **(PR_1000004025)** — System Uptime counter wrapped in approx. 49 days.

Release H.07.50

Release numbers H.07.47 through H.07.49 were never released.

Problems Resolved in Release H.07.50

- **CLI (PR_82086)** — Command **show mac <mac-address>** does not work.
- **CLI (PR_1000005082)** — If GVRP is enabled, an incorrect error message of Commit Failed is generated when trying to add more than the configured “max vlans” in the CLI. The proper error message should be Maximum number of VLANs (max-vlans) has already been reached. Dynamically created VLANs were not being included in the count.
- **Crash(PR_1000012823)** — OpenSSL vulnerability addressed.
- **Flow Control (PR_98957)** — Flow Control mechanism was not generating Pause frames.

Limitations for this fix:

Due to interactions with setting QoS priorities on inbound packets, some packets will be dropped in order to preserve the Queue Priorities when a 4:1 or higher oversubscription of 100- or 1000-Mbps ports have streams flowing to another 100- or 1000-Mbps port.

100-Mbps ports to 10-Mbps ports works correctly.

Workaround: Do not use Flow Control and QoS priorities simultaneously.

2650 (J4899A) and 2650-PWR (J8165A) switches only:

If an ingress port in the range of ports 1-24 and 49 are overflowing an egress port in the range of 25-48 and 50, a Pause Frame will NOT be generated out the ingress port.

- **Link (PR_1000020645)** — 2626 port 25 with a fiber link does not work after reset; also applies to the 6108 port 7.
- **PoE (PR_1000004040)** — Event log message system: PoE controller selftest failure occurs when a system is rebooting while powered by an external power supply (HP 600, J8168A).
- **RMON (PR_1000011690)** — When RMON thresholds in the switch are exceeded, no trap is generated.

- **Web (PR_1000003580)** — In the Diagnostics/LinkTest page, the Web interface allows broadcast/multicast MAC destination addresses. The CLI does not allow them. For consistency and because they should not be used, the Web interface should be changed to not allow them either.
- **Web (PR_1000004111)** — Stack Management view, scrolling problem.
- **Web (PR_1000007144)** — VLAN Configuration help link is not available.

Release H.07.53

Release numbers H.07.51 and H.07.52 were never released.

Problems Resolved in Release H.07.53

- **Switching (PR_1000022819)** — Bringing up a trunk port flushes the addresses in the MAC address table that are located on the next higher-numbered port, which results in unexpected flooding.
- **TELNET (PR_1000019573)** — Switch reboots when TELNET is disabled and port 1506 is accessed. When the switch reboots there is no error listed in the log or in the boot history of the switch.

Release H.07.54

Problems Resolved in Release H.07.54

- **Auto TFTP (PR_1000187649)** — Auto-TFTP will not allow a forced download of software after Auto-TFTP is Disabled.
- **Auto TFTP/Rebooting (PR_1000020802)** — Auto-TFTP causes constant rebooting, with no resulting crash files.
- **Switching (PR_1000022819)** — Bringing up a trunk port flushes the addresses in the MAC address table that are located on the next higher-numbered port, which results in unexpected flooding.

Release H.07.55

Problems Resolved in Release H.07.55

- **802.1X (PR_1000208530)** — Effects are unknown, but could include crashes such as bus errors.
- **CDP (PR_1000195343)** — Entering the command "**show cdp neighbor detail x**" displays incorrect information.

- **Config (PR_1000197097)** — When copying a configuration that doesn't have SNMP community names defined, the 6108 switch adds the 'public' community name with manager unrestricted rights.
- **Crash (PR_1000205768)** — "null" System Name in the Web user interface may crash with:

```
Software exception at lldpSysNameTlv.c:251 -- in 'mlldpCtrl', >task ID = 0x12dc88 -> ASSERT: failed.
```
- **Crash (PR_1000201614)** — When the switch is set with a 16 character manager password, hitting the down arrow keys twice within the start of the setup menu, a 'Bus error' crash may occur. The bus errors vary.
- **Crash (PR_1000092011)** — The switch may crash while using the web user interface with a message similar to:

```
Software exception at exception.c:356 -- in 'mHttpCtrl', task ID = 0x139ba40.
```
- **DHCP Relay (PR_1000188635)** — DHCP Relay sometimes preserves the incoming MAC SA in relayed packets.
- **IGMP (PR_1000191237)** — IGMP will not process any incoming or outgoing IGMP protocol packets if user adds a port to VLAN with 257 groups.
- **RMON (PR_1000196477)** — When RMON thresholds in the switch are exceeded no trap is generated.
- **SNMP (PR_1000212170)** — The Switch transmits Warm and Cold Start traps with an agent address of 0.0.0.0.
- **SNMP (PR_1000190654)** — Some of the fault finder events in the SNMP traps list a 0.0.0.0 IP address in the URL. This happens when the switch has the IP address configured on a VLAN other than the default.
- **SNTP (PR_1000199632)** — NTP (SNTP) Some ProCurve switches on certain code levels will not accept a good NTP version 4 broadcast. Same switches can learn time from version 3 broadcast or version 4 unicast.
- **SNMP (PR_1000086062)** - SNMP Sets allowed in Operator mode and IP Authorized-Manager is set.
- **Web UI (PR_1000191635)** - The Port column may not be sorted correctly in all Web user interface screens.
- **Web UI (PR_93721)** - Scroll bar does not work in Web Status screen.
In the web user interface, the Status screen does not display all ports.

Release H.07.56

Problems Resolved in Release H.07.56

- **Config (PR_1000216051)** — Returning a previously saved startup-configuration with **stack join (mac address)** to a member switch of the IP stack breaks the membership of that same stack. Commander hangs with member mismatched.
- **Open VLAN (PR_1000210932)** — open VLAN mode (Unauth VLAN) does not work with any Port-Security Learn-Mode
- **Web (PR_80857)** — A problem with IE4 and WebAgent. Recompiled the Web Agent with a new Java Development Kit (1.2 - was 1.1)

Release H.08.53

Release numbers H.08.01 through H.08.52 were never released.

Problems Resolved in Release H.08.53

- **802.1p (PR_1*20469)** — Port priority is not adopted as the traffic is forwarded on the appropriate outbound port.
- **CLI (PR_82258)** — **sh ip igmp** command shows blank lines mixed within the displayed table.
- **CLI (PR_1*18700)** — **Show ip route** "IP Route Entries" not centered in output.
- **CLI (PR_1*18755)** — Executing a **show power bri** command results in garbled output.
- **Config (PR_92346)** — Unable to delete empty VLAN.
- **Crash (PR_1*2177)** — 2600, switch may crash with a message similar to:
`Software exception at gamHwLearn.c:412 -- in 'tARL', task ID = 0x1893f08`
- **Crash (PR_1*3433)** — Switch may crash with a message similar to:
`Assertion failed: SOC_MEM_BLOCK_VALID(unit, mem, copyno), file mem.c, line 326`
- **Crash (PR_1*5469)** — 2600 crash during boot on top of tree.
- **Help (PR_98206)** — Help file is not consistent with the actual usage.
- **Help (PR_1*21395)** — Help text incorrect for some **ip icmp** commands.
- **Hot Swap (PR_1*18578)** — Dual personality ports hotswap out problem.
- **LACP (PR_1*6404)** — Dynamic LACP: Standby mode problem.
- **Routing (PR_91549)** — Addr manager using 0 based call to the soc_mem_xx layer.

- **Routing (PR_93481)** — 2650 software routes a packet when the DA MAC belongs to another VLAN.
- **SNMP (PR_88716)** — SNMP walk times out with large configuration.
- **SNMP (PR_1*3361)** — 'snmpv3' configtest failure.
- **Syslog (PR_97016)** — syslog word-complete options are not consistent with 6108 and 2800.
- **Web (PR_89899)** — Web UI port statistic counters are overwriting one another.
- **Web (PR_97621)** — 2650/H.07.32 | Sun Java 1.4.X: Unable to use Web browser.
- **Web (PR_1*12103)** — Garbage in the Web UI Status | Overview screen
- **Web (PR_1*1216)** — Web UI, log error.
- **Web (PR_1*21294)** — Stack Management Screen is blank.
- **Web (PR_1*3133)** — Web UI: Stack Access is not available.

Release H.08.55

Release number H.08.54 was never released.

Problems Resolved in Release H.08.55

- **ACL (PR_1000207620)** — The switch sometimes incorrectly permits TCP and UDP traffic in spite of an ACL configuration.
- **CDP (PR_1000195343)** — Entering the command **show cdp neighbor detail x** (where x is the port number) displays details for all active ports with CDP neighbors whose numbers begin with x. Only occurs when the **detail** parameter is included.
- **Config (PR_1000211397)** — A J4900B does not accept a configuration file saved from a J4900A.
- **IP Helper/DHCP Relay (PR_1000197046)** — DHCP clients successfully acquire their IP address via DHCP. However, when attempting to access additional data from the DHCP server via DHCP Inform messages from the client, the transaction fails.
- **RMON (PR_1000196477)** — When RMON thresholds in the switch are exceeded, no trap is generated.
- **SNMP (PR_1000190654)** — Some of the fault finder events in the SNMP traps list a 0.0.0.0 IP address in the URL. This happens when the switch has the IP address configured on a VLAN other than the default.
- **SNMP (PR_1000196170)** — Switch does not send out SNMP traps for events that occur before the switch IP stack has completed initialization.

- **Web UI/Port Security (PR_1000195894)** — The Web user interface does not allow the user to select multiple ports when configuring port-security.

Release H.08.56

Problems Resolved in Release H.08.56

- **CLI (PR_1000202435)** — When IGMP fast-leave is configured via the CLI, the configuration is not displayed in **show config**.
- **Config (PR_1000212686)** — A J4899B does not accept a configuration file created on a J4899A.

Release H.08.57

Problems Resolved in Release H.08.57

- **Crash (PR_1000213744)** — Creating any source port filter to drop on port 26 on a switch 2626 may result in a crash with error message similar to:

```
Assertion failed: BCM_PBMP_MEMBER(npbm, (B56_STACKING_PORT(unit))),  
file hp_standalone.c, line 7108.
```
- **MSTP (PR_1000207608)** — After the root bridge is agreed, the non-root switch continues to send out BPDUs claiming to be Root, resulting in possible instability in the STP topology.
- **SNMP (PR_1000212170)** — The switch will initially send out reboot traps with an agent address of 0.0.0.0 when the agent address is statically set.

Release H.08.58

Problems Resolved in Release H.08.58

- **Crash (PR_1000205768)** — In some cases, if the user does not configure a System Name within the Web user interface, the switch may crash with the following message:

```
Software exception at lldpSysNameTlv.c:251 - in 'mlldpCtrl', >task ID  
= 0x12dc88 -> ASSERT: failed
```
- **Open VLAN (PR_1000210932)** — A port configured for Open VLAN mode (Unauthorized VLAN) does not work with any Port-Security Learn-Mode setting.
- **Web UI (PR_1000191635)** — Within the Web UI "Port Counters" and "Port Status" pages, the "Port" column may be sorted incorrectly.
- **Web UI (PR_93721)** — The scroll bar within the "Web Status" page does not work.

Release H.08.59

Problems Resolved in Release H.08.59

- **Config (PR_1000216051)** — Copying a previously saved startup-configuration with **stack join (mac address)** to a member switch of the IP stack will break the membership of that stack.
- **Crash (PR_1000201614)** — The switch may crash within the CLI **setup menu** if a 16-character manager password set.
- **Spanning Tree (PR_1000214598)** — The switch will not accept the **spanning-tree 1 mode fast** command within the CLI.

Release H.08.60

Problems Resolved in Release H.08.60

- **Crash (PR_1000207542)** — The switch may crash with a bus error or a task hang.
- **Port Security (PR_1000203984)** — When the limit is reached the warning message is displayed: Number of configured addresses on port xx exceeds address-limit. The address will be saved and displayed in the address list of Show Port-security xx. Data from the added address is passed by the switch.

Release H.08.61

Problems Resolved in Release H.08.61

- **Crash/Static Route (PR_1000217354)** — The switch may crash with a `Bus error in mSnmpCtrl` when adding a less-specific static route.
- **STP/Mirroring (PR_1000211360)** — A loop is created with STP enabled and monitoring port 50 while port 50 is Blocking.

Release H.08.62

Problems Resolved in Release H.08.62

- **RSTP (PR_99049)** — Switch does not detect and block network topology loops on a single port. For example, the port connects to a hub that has a loop or the port connects to an inactive node via IBM 'Type 1' cable.

Release H.08.64

Problems Resolved in Release H.08.64 (never released.)

- **Config (PR_1000207697)** — Loading a startup-configuration file fails when attempting to declare a VLAN in the configuration file as a management VLAN, and the VLAN does not currently exist on the switch. The switch indicates the downloaded file as being corrupted, listing the VID of the specified management VLAN as not being found.

Release H.08.65

- **Config (PR_1000215024)** — The switch may experience a memory leak when loading a configuration file several times.

Release H.08.67

Release number H.08.66 was never released.

Problems Resolved in Release H.08.67

- **Trunk ports (PR_1000231897)** — The switch may duplicate broadcast packets across all ports on a trunk link.

Release H.08.69

Release number H.08.68 was never released.

Problems Resolved in Release H.08.69

- **CLI (PR_1000198460)** — In the CLI help menu for VLANs, the maximum number of VLANs displays incorrect information.
- **Console/TELNET (PR_1000195647)** — When a console or TELNET session hangs, issuing the **kill** command will also hang.
- **Counters (PR_1000221089)** — When accessing the 64 bit counters, the counters may not always be correct.
- **Crash (PR_1000193582)** — Software Exception when clicking on the Identity Tab of a member Switch in the Web user interface. The switch may crash with a message similar to:

`Software exception at http_state.c:1138 in 'mHttpCtrl' TaskID=0x1722cf8`
- **Crash (PR_1000204782)** — Bus error when copying a configuration to the switch. The switch may crash with a message similar to:

`Bus error: HW Addr=0x594f5531 IP=0x004ff8a8 Task='mftTask'
Task ID=0x126eba0 fp: 0x00000000 sp:0x0126e7d0 lr:0x001e655c.`

- **Port Security (Enhancement)** — Added support for IP Lockdown.
- **QOS (PR_1000200746)** — Switch truncates the DSCP-map name after a reboot.
- **Syslog (PR_1000215699)** — Switch does not send all Event Log entries to the syslog server at switch boot..
- **Web UI (PR_1000214188)** — While working in the Status-Overview screen, the scroll bar does not display or respond correctly after resizing a window.

Release H.08.70

Problems Resolved in Release H.08.70 (never released)

- **802.1s (PR_1000227432)** — Leaning flag is not set when CIST port states are transitioning.
- **802.1s (PR_1000233920)** — 802.1s blocks a port that is connected to an RSTP device.
- **Crash (PR_1000229656)** — Switch cannot reach RADIUS server and crashes with a message similar to:


```
Software exception at exception.c:373-in 'tHttpd', task ID = 0x257dda8  
->Memory system error at 0x24ea750 - memPartFree.
```
- **Web Authentication (PR_1000230444)** — Using port-based web authentication on the Switch will cause some users to never receive the web authentication screen. This occurs if a client receives the same unauthenticated DHCP address that a previous authorized client has used.
- **Web/Stack (PR_1000239924)** — As an IP Stack Management Commander, the Switch does not display the device view (back of box) for a switch which is a member.

Release H.08.71

Problems Resolved in Release H.08.71

- **Crash (PR_1000232283)** — The switch may crash with a message similar to:


```
Software exception at fileTransferTFTP.c:182 -- in 'mftTask', task ID  
= 0x107ee0.
```

Release H.08.72

Problems Resolved in Release H.08.72

- **LLDP (PR_1000241315)** — The CLI command **show LLDP** does not display information correctly.

- **Web (PR_1000211978)** — On a Stack Management Commander, when using "stack access" to view members, the screen does not display correct information.

Release H.08.73

Problems Resolved in Release H.08.73

- **SNMP (PR_1000003378)** — SNMP switch time may drift with event log updates occurring every 1.5 hours

Release H.08.74

Problems Resolved in Release H.08.74

- **RADIUS (PR_1000285456)** — If more than one RADIUS assigned vendor specific attribute (including Port-cos, rate-limiting-ingress, or ACLs) is configured with a non-vendor specific attribute, only the first vendor-specific attribute may be recognized by switch.
- **TCP (PR_1000246186)** — Switch is susceptible to VU#498440.
- **Web UI (PR_1000284653)** — When using the web user interface "IP Stack Management", and there are more than 100 potential Members present on a VLAN, the Switch will learn new potential Members, but delete previously learned Members.

Release H.08.75

Problems Resolved in Release H.08.75

- **RSTP (PR_1000286883)** — Slow RSTP fail-over and fall-back time.
- **VLAN (PR_1000214406)** — When trying to delete a VLAN created as a management VLAN, the switch fails to remove the management VLAN statement from the running configuration file.

Release H.08.76

Problems Resolved in Release H.08.76

- **MSTP (PR_1000286883)** — Slow MSTP fail-over and fall-back time.

Release H.08.77

Problems Resolved in Release H.08.77 (Never released)

- **FEC/CDP (PR_1000281734)** — CDP transmit and FEC Trunk negotiation removed.
- **LLDP (Enhancement)** — Added support for LLDP (Link Layer Discovery Protocol) IEEE 802.1AB.
- **Trunking (PR_1000287225)** — Cannot configure LACP trunk ports across ASIC with Intel/HP NIC teaming.

Release H.08.78 - H.08.81

Versions H.08.78 through H.08.81 were never built.

Release H.08.82

Problems Resolved in Release H.08.82 (Never released)

- **Fault (PR_1000089786)** — Chassis fault LED stops blinking after a new OS image is downloaded to the switch.
- **Show Tech (enhancement)** — Show Tech is enhanced as follows: "The 'show tech stat' output now reports the number of ports that currently have links.

Release H.08.83

Problems Resolved in Release H.08.83 (Never released)

- **RSTP (PR_1000297195)** — The switch repeatedly flushes its MAC address table, resulting in intermittent flooding of all traffic.

Release H.08.84

Problems Resolved in Release H.08.84 (Never released)

- **Crash (PR_1000297510)** — When using Web User Interface and the switch is set as commander for stacking, the switch crashes.
- **Key Management System (PR_1000287934)** — Some Key Management System (KMS) configuration commands have no effect.
- **LLDP (PR_1000285649)** — Added LLDP information in "show tech".

- **RSTP (PR_1000300623)** — Under some circumstances, the Switch may allow packets to loop for an extended period of time.

Release H.08.85

Problems Resolved in Release H.08.85 (Never released)

- **Event Log/ARP (PR_1000293466)** — Generic Link Up message not showing up and unnecessary flushing of ARP cache.
- **IGMP (PR_1000301557)** — Data-driven IGMP does not prevent flooding when no IP address exists on a VLAN.

Release H.08.86

Problems Resolved in Release H.08.86

- **CLI (PR_1000292455)** — Enhancement– Rate display for ports on CLI.
New command: “show interface port-utilization”. Not available on Menu nor Web Interface.
- **Config (PR_1000306769)** — When an OS upgrade causes an FEC trunk to be converted, the following messages are logged:

```
[datestamp] mgr: Config file converted due to OS upgrade  
W [datestamp] mgr: FEC trunks not supported; see release notes
```
- **Enhancement (PR_1000306695)** — Added show tech command, "**show tech transceivers**" to allow removable transceiver serial numbers to be displayed without removal of the transceivers from the switch

Release H.08.87

Problems Resolved in Release H.08.87 (Never released)

- **CLI/DHCP (PR_1000286898)** — Under some conditions the CLI may freeze or lock up.
- **IGMP (PR_1000301557)** — Data-driven IGMP does not prevent flooding when no IP address exists on the VLAN.
- **IP Forwarding (PR_1000305739)** — When a user attempts to configure 'ip forward-protocol netbios-dgm', the switch incorrectly configures 'ip forward-protocol netbios-ns' instead.
- **Port Monitoring (PR_1000296797)** — Traffic not isolated from the monitor port.
- **RSTP (PR_TT1000306227)** — RSTP TCNs cause high CPU utilization and slow software-based routing.

- **SNMP (PR_1000295753)** — Removing 'public' SNMP community generates an empty Event Log message.

Release H.08.88

Problems Resolved in Release H.08.88 (Never released)

- **VLAN Enhancement (PR_1000293132)** — The switch uses the same MAC address for all VLANs.

Release H.08.89

Problems Resolved in Release H.08.89 (Never released)

- **STP (PR_1000307280)** — Inconsistent or incorrect STP data.
- **LLDP (PR_1000310081)** — Enhancement, LLDP-MED.
- **RSTP (PR_1000309683)** — Temporary routing or switching problems after RSTP is disabled.

Release H.08.90

Problems Resolved in Release H.08.90 (Never released)

- **Menu (PR_1000306213)** — When using the Menu to create a trunk, the new trunk ports will become disabled after a switch reboot.
- **Performance Enhancement (PR_1000311412)** — Enhancements to improve queuing on Gigabit port response in MAC multicast oversubscription scenarios.

Release H.08.91

Problems Resolved in Release H.08.91 (Never released)

- **Crash (PR_1000282359)** The switch may crash with a bus error similar to:

```
PPC Bus Error exception vector 0x300: Stack Frame=0x0c8c1a70 HW  
Addr=0x6a73616c IP=0x007d3bc0 Task='mSess1' Task ID=0xc8c2920 fp:  
0x6b61736a sp:0x0c8c1b30 lr:0x007d3b28
```
- **LLDP (PR_1000310666)** — The command "show LLDP" does not display information learned from CDPv2 packets.

- **MSTP Enhancement (PR_1000310463)** — Implementation of spanning-tree legacy-path-cost CLI command for MSTP. See “MSTP Default Path Cost Controls” on page 35 for details.
- **Port-Security (PR_1000304202)** — The port-security MAC address learn mode is not functioning correctly between other 'port security' ports.
- **SNMP (PR_1000285195)** — Switch does not save the option to persistently disable the Link up/down SNMP traps for a given port.
- **SNMP (PR_1000310841)** — User can assign illegal values for CosDSCPPolicy through SNMP.
- **Web/Stacking (PR_1000308933)** — Added Web User Interface stacking support for the new Series 3500yl switches, providing a 3500yl "back-of-box" display when a 2600 Series switch is stack commander and a 3500yl is a stack member.

Release H.08.92

Problems Resolved in Release H.08.92

- **Config (PR_1000298146)** — Enabling QoS-passthrough Mode causes incorrect information to be displayed in the **show configuration** command.
- **Help (PR_1000317711)** — In the VLAN menu Help text, the word 'default' is spelled incorrectly.
- **MSTP Enhancement (PR_1000313986)** — Implemented new CLI command, **spanning-tree legacy-mode**. See
- **RADIUS (PR_1000316158)** — After a switch reboot, the switch does not recognize a response from a RADIUS or TACACS server.
- **RSTP (PR_1000307278)** — Replacing an 802.1D bridge device with an end node (non-STP device) on the same Switch port, can result in the RSTP Switch sending TCNs.
- **SNMP (PR_1000315054)**— SNMP security violations appear in syslog after a valid SNMPv3 “get” operation.

Release H.08.93

Problems Resolved in Release H.08.93 (Not a general release)

- **Enhancement (PR_1000319920)** — Added DHCP Option 82 enhancement, and UDP broadcast forwarding enhancement.
- **Menu (PR_1000318531)** — When using the Menu interface, the Switch hostname may be displayed incorrectly.

- **Web (PR_1000302713)** — When using the web interface and a large amount of stacking interactions occur, portions of the information from the stack commander may no longer appear.

Release H.08.94

Problems Resolved in Release H.08.94 (Never released)

- **STP/RSTP/MSTP (PR_1000300623)** — In some cases STP/RSTP/MSTP may allow a loop, resulting in a broadcast storm.

Release H.08.95

Problems Resolved in Release H.08.95 (Not a general release)

- **Crash (PR_1000323675)** — The Switch may crash with a message similar to:
`ASSERT: Software exception at aaa8021x_proto.c:501 -- in 'm8021xCtrl'.`
- **Web UI Enhancement (PR_1000290489)** — Enhancement to display Port Name along with Port number on the Web User Interface Status and Configuration screens.
- **Enhancement (PR_1000242392)** — Enabled login "Message of the Day" (MOTD) banner. For details on using this feature, refer to “Custom Login Banners for the Console and Web Browser Interfaces”.
- **ICMP (PR_1000235905)** — Switch does not send a 'destination unreachable' response message when trying to access an invalid UDP port.
- **SNMPv3 (PR_1000325021)** — Under some conditions, SNMPv3 lines are not written to the running-configuration file.

Release H.08.96

No software fixes in this release. Code revised to modify Manufacturing test processes.

Release H.08.97

Problems Resolved in Release H.08.97 (Not a general release)

- **Crash/SSHv2 (PR_1000320822)** — The Switch does not generate SSHv2 keys and may crash with a message similar to:

```
TLB Miss: Virtual Addr=0x00000000 IP=0x80593a30 Task='swInitTask' Task
ID=0x821ae330 fp:0x00000000 sp:0x821adfb8 ra:0x800803f0 sr:0x1000fc01.
```

- **Enhancement (PR_1000331027)** — TCP/UDP port closure enhancement.
- **STP/RSTP/MSTP (PR_1000330532)** — Improved the "show" commands display of STP ports detail information to assist in monitoring and troubleshooting spanning tree.

Release H.08.98

- **CLI (PR_1000334412)** — Operator level can save Manager privilege level changes to the configuration.
- **Ethernet Errors (PR_10003331494)** — Packets that are transmitted out dual-personality ports that are manually configured in full or half-duplex mode may have FCS or alignment errors.
- **Log (PR_1000323790)** — The switch detects a counterfeit mini-GBIC as a port self test failure and subsequently disables the link.

Known Software Issues and Limitations

There are no known issues at this time.

Limitations

Displaying the Fast-Leave Setting on a Port

Use the **walkmib** command, below, to display this setting for all switch ports or the ports on a specified VLAN.

Syntax: walkmib hpSwitchIgmpPortFastLeaveState<.vlan number>

```
HPswitch# walkmib hpSwitchIgmpPortFastLeaveState.20
hpSwitchIgmpPortFastLeaveState.20.2 = 1
hpSwitchIgmpPortFastLeaveState.20.3 = 2
HPswitch# walkmib hpSwitchIgmpPortFastLeaveState.35
hpSwitchIgmpPortFastLeaveState.35.5 = 2
hpSwitchIgmpPortFastLeaveState.35.6 = 1
hpSwitchIgmpPortFastLeaveState.35.7 = 1
```

The **2** at the end of a port listing shows that Fast-Leave is **disabled** on the corresponding port.

The **1** at the end of a port listing shows that Fast-Leave is **enabled** on the corresponding port.

VLAN Number (Default VLAN=1)

Sequential Port Numbers (not all ports shown here)



© 2002, 2006 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

June, 2006
Manual Part Number
5990-6003