



Release Notes: Version I.08.105 Software *for the ProCurve 2800 Series*

Release I.08.105 supports these switches:

- ProCurve Switch 2824 (J4903A)
- ProCurve Switch 2848 (J4904A)

These release notes include information on the following:

- Downloading switch documentation and software from the Web ([page 1](#))
 - Clarification of operating details for certain software features ([page 8](#))
 - Software features available in releases I.07.32 through I.08.8x ([page 11](#))
 - A listing of software fixes included in releases I.07.31 through I.08.105 ([page 40](#))
-

FEC, CDP Removal

Starting with Software version I.08.74, 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>.

Boot ROM Update Required

If your 2800 is currently running a pre-I.07.68 software version, you must update the Boot ROM before installing I.08.1xx. Load the I.07.68 software and reboot your switch from the I.07.68 software image. NOTE: a copy of the I.07.68 software is included in the I.08.1xxzip file on the ProCurve Networking Web site. See "[Release I.07.64 Enhancements](#)" on [page 13](#) for more information.

There have been subsequent updates to the Boot ROM since I.07.68 but an initial upgrade (using I.07.68) is still required before installing I.08.xx software. Use the "Show Flash" command to check which version of Boot ROM your switch is running. If the version of your Boot ROM is already at I.08.02 or greater, you can simply install this latest release to upgrade to the latest version.

Caution

The startup-config file saved under version I.08.xx or greater, is NOT backward-compatible with previous software versions. Users are advised to save a copy of the pre-I.08.xx startup-config file BEFORE UPGRADING to I.08.xx or greater, in case there is ever a need to revert to pre-I.08.xx software. Instructions for saving a copy of the startup-config file are found in the "Transferring Switch Configurations" section of Appendix A in the *Management and Configuration Guide* available on the ProCurve Networking Web site.

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

Publication Number

5990-6049
September, 2006 -B

Applicable Product

ProCurve Switch 2824	(J4903A)
ProCurve Switch 2848	(J4904A)

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 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 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>.

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

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

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 2800 Switch	7
OS/Web/Java Compatibility Table	7
Clarifications	8
LLDP and LACP	8
IGMP	8
Supported Standards and RFCs	8
IGMP, Multicast Filters, and Configured VLANs	9
Using Delayed Group Flush	9
Setting Fast-Leave and Forced Fast-Leave from the CLI	10
IGMP Operating Notes	10
Displaying Spanning Tree Configuration Detail	10
Enhancements	11
Release I.07.32 Enhancements	11
Release I.07.50 Enhancements	11
Port Trunking	11
Port Monitoring	12
Release I.07.51 Enhancements	12
Release I.07.52 Enhancements (Beta Only)	12
QOS Pass-Through Mode	12
Release I.07.53 - I.07.57 Enhancements	12
Release I.07.58 Enhancements	12
Boot ROM update	12

Release I.07.59 - I.07.63 Enhancements	13
Release I.07.64 Enhancements	13
Boot ROM update	13
Release I.07.68 Enhancements	13
Boot ROM Update	13
Release I.08.55 Enhancements	14
Release I.08.60 Enhancements	15
Release I.08.63 through I.08.70 Enhancements	15
Release I.08.71 Enhancements	15
Release I.08.72 through I.08.73 Enhancements	15
Release I.08.74 Enhancements	15
Implementation of LLDP	15
Release I.08.80 Enhancements	16
Release I.08.81 Enhancements	16
Release I.08.82 through I.08.84 Enhancements	16
Release I.08.85 Enhancements	16
CLI Port Rate Display	16
Release I.08.86 through I.08.88	16
Release I.08.89 through I.08.90 Enhancements	16
IP Lockdown	17
MSTP Default Path Cost Controls	17
Release I.08.91 Enhancements	18
Release I.08.93 Enhancements	18
DHCP Option 82: Using the Management VLAN IP Address for the Remote ID	18
UDP Broadcast Forwarding	20
Release I.08.94 Enhancements	26
Release I.08.95 Enhancements	26
Custom Login Banners for the Console and Web Browser Interfaces	27
Show sFlow Commands	31
Release I.08.97 Enhancements	33
TCP/UDP Ports Closure	33
Release I.08.98 through Release I.08.99 Enhancements	35
Release I.08.100 Enhancements	35

Release I.08.101 Enhancements	35
Spanning Tree Per-Port BPDU Filtering	35
Release I.08.102 through Release I.08.103 Enhancements	39
Release I.08.104 Enhancements	39
Release I.08.105 Enhancements	39
Software Fixes in Release I.07.32 - I.08.9x	40
Release I.07.32	40
Release I.07.50	40
Release I.07.52 (Beta Only)	42
Release I.07.53 (Beta Only)	43
Release I.07.55 (Beta Only)	43
Release I.07.56	43
Release I.07.57 (Never Released)	44
Release I.07.58 (Beta Only)	44
Release I.07.59 (Beta Only)	45
Release I.07.60	45
Release I.07.61	45
Release I.07.62 (Beta Only)	45
Release I.07.63 (Beta Only)	45
Release I.07.64	45
Release I.07.65 (Not Released)	46
Release I.07.66	46
Release I.07.67	46
Release I.07.68	46
Release I.08.55	47
Release I.08.56	48
Release I.08.57	48
Release I.08.58	49
Release I.08.60	49
Release I.08.61	50
Release I.08.62	51

Release I.08.63	51
Release I.08.64	51
Release I.08.67	52
Release I.08.68	53
Release I.08.69	53
Release I.08.70	53
Release I.08.71	54
Release I.08.72	54
Release I.08.73	54
Release I.08.74	54
Release I.08.81	55
Release I.08.82	55
Release I.08.83	55
Release I.08.84	56
Release I.08.85	56
Release I.08.86 (Limited release)	56
Release I.08.87	56
Release I.08.88	57
Release I.08.89	57
Release I.08.90	57
Release I.08.91	58
Release I.08.92	58
Release I.08.93	58
Release I.08.94	59
Release I.08.95	59
Release I.08.96 (Never released)	60
Release I.08.97	60
Release I.08.98	60
Release I.08.99	60
Release I.08.100	61
Release I.08.101	61

Release I.08.102 (Never released)	61
Release I.08.103	61
Release I.08.104	62
Release I.08.105	62
Known Software Issues and Limitations	63
Issues	63
Limitations	63
Displaying the Fast-Leave Setting on a Port	63

Software Management


Downloading Switch Documentation and Software from the Web

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

To Download a Software Version:

1. Go to the ProCurve Networking Web site at:
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.

1. Go to the ProCurve Networking Web site at 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 by earlier software releases. Refer to the “[Caution](#)” on the front page.

HP periodically provides switch software updates through the ProCurve Networking Web site (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).
- HP’s SNMP Download Manager included in ProCurve Manager

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.

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 I_08_8x.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
ProCurve switch # copy tftp flash 10.28.227.103 I_08_8x.swi
The primary OS image will be deleted. continue [y/n]? Y
03125K
```

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

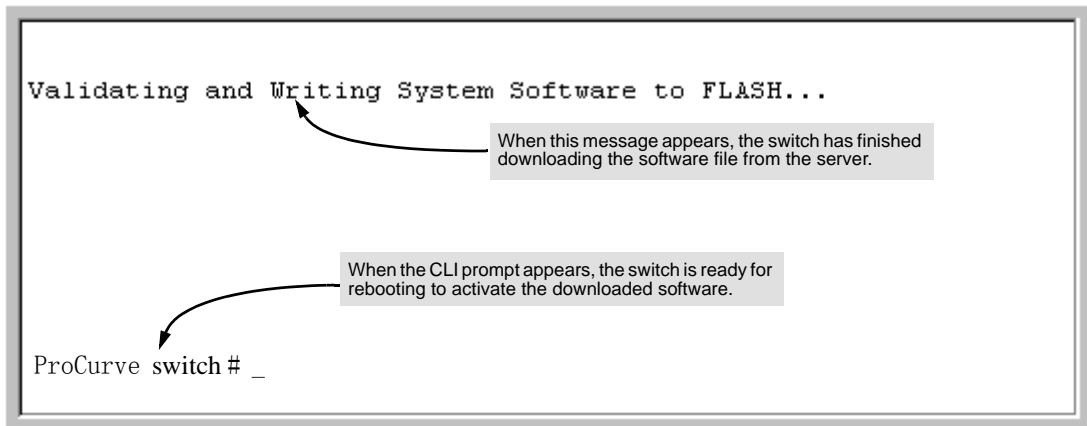


Figure 1. Message Indicating the Switch Is Ready To Activate the Downloaded Software

2. 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:

```
ProCurve switch(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:

```
ProCurve switch # 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 ([step 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 you use the CLI to make a configuration change, the switch places the change in the running-config file. If you want to preserve the change across reboots, you must 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 while using the CLI:

- Execute **write memory** from the Manager, Global, or Context configuration level.
- When exiting from the CLI, press **[Y]** (for Yes) when you see the “save configuration” prompt:

```
Do you want to save current configuration [y/n]?
```

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.
N	Switch 2810 Series (2810-24G and 2810-48G)
P	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
WA	ProCurve Access Point 530
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
numeric	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 2800 Switch

The following table lists minimum software versions required to support ProCurve Series 2800 switch hardware.

ProCurve Device	Minimum Supported Software Version
J4858A Gigabit-SX-LC Mini-GBIC	1.07.31
J4859A Gigabit-LX-LC Mini-GBIC	1.07.31
J4860A Gigabit-LH-LC Mini-GBIC	1.07.31
J8168A ProCurve 600 RPS/EPS	1.07.31

OS/Web/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 I.08.74, 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>

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.

IGMP, Multicast Filters, and Configured VLANs

On the Series 2800 Switches, the number of multicast filters available for use by IGMP is a function of the number of VLANs and the number of IGMP-enabled VLANs configured on the switch. When the number of multicast groups on the network exceeds the number of multicast filters available on the switch, excess multicast group traffic is flooded to all ports on the affected VLAN, to ensure that clients can receive their multicast traffic.

There are 255 multicast filters available in the switch. A filter is used each time a VLAN is configured and each time IGMP is enabled on a VLAN. The table below shows examples of the number of multicast filters available for IGMP use, based on the number of configured VLANs and IGMP-enabled VLANs.

Configured VLANs	IGMP-Enabled VLANs	Multicast Filters Available for IGMP	Average Number of Multicast Filters Available for IGMP per IGMP-Enabled VLAN
256	1	$255 - 256 - 1 = -2$	None. IGMP does not operate.
64	64	$255 - 64 - 64 = 127$	< 2
30	30	$255 - 30 - 30 = 195$	6.5
64	8	$255 - 64 - 8 = 183$	< 23
100	2	$255 - 100 - 2 = 153$	76

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.

As the Series 2800 Switches use Data-Driven IGMP with IGMP Fast-Leave always enabled, HP does **not** recommend that the Delayed Group Flush feature be used on the Series 2800 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-Leave 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-Leave on the specified ports in the VLAN, even if they are cascaded. The “no” form disables Forced Fast-Leave on the specified ports.

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

IGMP Operating Notes

- Review the number of VLANs and the number of IGMP-enabled VLANs you plan to use to determine if you have the sufficient multicast filters available for your expected IGMP groups. If you don't, excess multicast groups are not filtered and are flooded to all ports on the VLAN.
- Do not use Delayed Group Flush for Series 2800 Switches, as this behavior provides no additional benefits when Data-Driven IGMP is supported.
- Forced fast leave can be used when there are multiple devices attached to a port.

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

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 I.08.98 through Release I.08.99 Enhancements” on page 35](#).

Descriptions and instructions for enhancements included in Release I.08.68 or earlier are included in the latest release of manuals for the ProCurve 2800 switches (Oct. 2005), available on the web at <http://www.hp.com/rnd/support/manuals/2800.htm>

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

Release I.07.32 Enhancements

Software fixes only; no new enhancements.

Release I.07.50 Enhancements

Port Trunking

New Maximum for Number of Ports in a Trunk

Trunk groups can now be configured with up to 8 ports per trunk. (Formerly, the switches allowed only 4 ports per trunk.) Also, you can now configure up to 24 trunk groups per switch. (Formerly, the switches allowed only 6 port trunk groups).

Restriction on Grouping of Ports in a Trunk with IP Routing Enabled

Trunk groups can generally be specified as any grouping of ports on the switch. However, if IP routing is enabled on the switch, all of the ports in a given trunk group must be in the same range of ports. These ranges are as follows:

- 1-12
- 13-24
- 25-36 (applies only to the Switch 2848)
- 37-48 (applies only to the Switch 2848)

For more information, refer to the chapter titled “Port Trunking” in the *Management and Configuration Guide* for your switch (October 2004 version, or later). To download the latest version of switch documentation, refer to [“Downloading Switch Documentation and Software from the Web” on page 1](#).

Port Monitoring

In software releases prior to release I.07.50, port monitoring sent only inbound (ingress) traffic to the monitor. Beginning with release I.07.50, the Series 2800 switches will now also send outbound (Egress) traffic to the mirror port when port monitoring is enabled.

Release I.07.51 Enhancements

Software fixes only; no new enhancements.

Release I.07.52 Enhancements (Beta Only)

QOS Pass-Through Mode

Release I.07.52 introduced a new command to enhance the performance of line-rate traffic transfers through the 2800 Series switches. This feature should only be used in environments where Quality of Service (QoS) is not of major importance, but where lossless data transfers are key. This command essentially disables any discrimination of QoS queues for traffic, consolidating packet buffer memory to provide line-rate flows with no loss of data.

For more information, refer to the chapter titled “Port Status and Basic Configuration” in the *Management and Configuration Guide* for your switch (October 2004 version, or later). To download the latest version of switch documentation, refer to [“Downloading Switch Documentation and Software from the Web” on page 1](#)

Release I.07.53 - I.07.57 Enhancements

Software fixes only; no new enhancements.

Release I.07.58 Enhancements

Boot ROM update

This release (and all subsequent releases) include a Boot ROM upgrade facility. If, during boot, it detects a version 7.xx Boot ROM image, it will upgrade the Boot ROM to version I.08.02. This Boot ROM reformats the Flash area to accept code images larger than 3 MB, and is required to be done prior to the next major release of software (expected winter, 2004). No damage is done to the code stored in the secondary flash area.

Once the user initially boots with this release (or later I.07.*xx* releases) the console screen will report that the Boot ROM is being updated:

```
Decompressing...done.

Initializing...

WARNING : This release includes a BootROM upgrade.
          Interrupting this process will cause
          The switch to become unusable.

BootROM upgrade in progress...completed.
```

This process takes approximately 3 minutes to complete, including the normal time to boot up your switch. Note: previous versions of these release notes placed this Boot ROM upgrade facility in Release I.07.56.

Release I.07.59 - I.07.63 Enhancements

Software fixes only; no new enhancements.

Includes the Boot ROM upgrade initially introduced in I.07.58.

Release I.07.64 Enhancements

Boot ROM update

This release (and all subsequent releases) include a Boot ROM upgrade facility. If, during boot, it detects a version 7.*xx* or a version 8.02 Boot ROM image, it will upgrade the Boot ROM to version I.08.04. This Boot ROM reformats the Flash area to accept code images larger than 3 MB, and is required to be done prior to the next major release of software (expected winter, 2004).

No damage is done to the code stored in the secondary flash area. See the process description under [“Release I.07.58 Enhancements”](#) for details.

Release I.07.68 Enhancements

Boot ROM Update

Release I.07.68 is an update to the Boot ROM installer, previously documented in the I.07.64 and I.07.58 software releases. This software installs Boot ROM I.08.05, which aids in preventing some categories of system hang conditions.

Release I.08.55 Enhancements

Enhancement	Overview
Supports 256 VLANs	Previously, the maximum number of VLANs was 60.
DiffServ Codepoint (DSCP) Marking - L3/L4	Provide support for the following DSCP modes: RFC2474 DiffServ Precedence, RFC2597 DiffServ Assured Forwarding (AF), and RFC2598 DiffServ Expedited Forwarding (EF). (Refer to: Chapter 6, "Quality of Service (QoS): Managing Bandwidth More Effectively on the Series 2600/2600-PWR and Series 2800 Switches" in the <i>Advanced Traffic Management Guide</i> , October 2004—on the ProCurve Networking Web site.*)
802.1s Multiple Spanning-Tree	Adds the option for running 802.1s Multiple Spanning-Tree on the switch to enable multiple spanning-tree instances. Interoperates with legacy 802.1D (STP) and 802.1w (RSTP) spanning-tree. (Refer to: Chapter 5, "Spanning-Tree Operation" in the <i>Advanced Traffic Management Guide</i> , October 2004—on the ProCurve Networking Web site.*)
Jumbo Packets	On a VLAN configured for jumbo traffic, all ports belonging to that VLAN and operating at 1 Gbps or 10 Gbps allow inbound jumbo packets of up to 9220 bytes (includes four bytes for a VLAN tag). (Refer to: Chapter 10, "Port Status and Basic Configuration" in the <i>Management and Configuration Guide</i> , October 2004—on the ProCurve Networking Web site.*)
Web Authentication	Web authentication adds a new security option that uses a web page login to authenticate users via a RADIUS server for access to the network. (Refer to: Chapter 3, "Web and MAC Authentication for the Series 2600/2600-PWR and 2800 Switches" in the <i>Access Security Guide</i> , October 2004—on the ProCurve Networking Web site.*)
MAC Authentication	MAC authentication adds a new security option that uses a device's MAC address to authenticate the device via a RADIUS server for access to the network. (Refer to: Chapter 3, "Web and MAC Authentication for the Series 2600/2600-PWR and 2800 Switches" in the <i>Access Security Guide</i> , October 2004—on the ProCurve Networking Web site.*)
MAC Lockdown/Lockout	<ul style="list-style-type: none"> • MAC Lockdown enables the permanent assignment of a MAC address and VLAN to a specific port on the switch. • MAC Lockout causes the switch to drop any traffic to or from the specified MAC address(es). (Refer to: Chapter 9, "Configuring and Monitoring Port Security" in the <i>Access Security Guide</i>, October 2004—on the ProCurve Networking Web site.*)
Secure Copy and Secure FTP	Enables use of a secure, encrypted SSH session for transferring files to or from the switch. (Refer to: Appendix A, "File Transfers" in the <i>Management and Configuration Guide</i> , October 2004—on the ProCurve Networking Web site.*)
Front-Panel Security	Provides the option for enabling or disabling some of the functions of the Reset and Clear buttons on the switch's front panel. This feature also provides the ability to disable password recovery for situations requiring a higher level of security. (Refer to: Chapter 2, "Configuring Username and Password Security" in the <i>Access Security Guide</i> —part number 5990-6024, October 2004—on the ProCurve Networking Web site.*)
Auto-MDI-X manual mode	Provides CLI commands for changing the cable-configuration support on the switch's copper ports. The options include auto-MDIX (the default), MDI, and MDI-X. This also allows the manual configuration of port speed. (Refer to: Chapter 10, "Port Status and Basic Configuration" in the <i>Management and Configuration Guide</i> —part number 5990-6023, October 2004—on the ProCurve Networking Web site.*)
Flow sampling with sFlow	Adds sFlow as a flow-sampling method for use with applicable network management software. (Refer to the documentation provided with your network management software.)

* To download switch documentation for software release I.08.xx, refer to "[To Download Product Documentation:](#)" on page 1.

Release I.08.60 Enhancements

I.08.60 Enhancement	Overview
RADIUS Authentication for Switch 2800 Web Browser Access	The aaa authentication command now allows the optional use of RADIUS as the primary password authentication method for the Web browser interface on Series 2800 switches (as well as for the Series 2600, 2600-PWR, and 5300xl switches). Refer to Chapter 5, "RADIUS Authentication and Accounting" in the <i>Access Security Guide</i> (October 2005 or newer) on the ProCurve Networking Web site.
CLI Local Terminal Mode Command	This new command enables changing from one terminal mode to another without changing the terminal mode configuration or having to reboot the switch. The command is not persistent across reboots, and affects only the current console session. Refer to Chapter 7, "Interface Access and System Information" in the <i>Management and Configuration Guide</i> , (October 2005 or newer) on the ProCurve Networking Web site.
DHCP Option 82	Enables a network administrator using a DHCP server supporting DHCP Option 82 to IP addressing policies based on the network area from which a client DHCP request originates. refer to Chapter 7, "IP Routing Features" in the <i>Advanced Traffic Management Guide</i> (October 2005 or newer) on the ProCurve Networking Web site.

Release I.08.63 through I.08.70 Enhancements

Software fixes only; no new enhancements.

Release I.08.71 Enhancements

Release I.08.71 contains support for the new I.08.07 Boot ROM version.

Release I.08.72 through I.08.73 Enhancements

Software fixes only; no new enhancements.

Release I.08.74 Enhancements

Implementation of LLDP

For network device discovery solutions, software version I.08.74 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>. (See "To Download a Software Version:" on page 1).

Versions I.08.75 through I.08.79 were never built.

Release I.08.80 Enhancements

Software fixes only; no new enhancements.

Release I.08.81 Enhancements

The "Show Tech Statistics" command now reports the number of ports that currently have links.

Release I.08.82 through I.08.84 Enhancements

Software fixes only; no new enhancements.

Release I.08.85 Enhancements

CLI Port Rate Display

Beginning with release I.08.85 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.

Release I.08.86 through I.08.88

Software fixes only; no new enhancements.

Release I.08.89 through I.08.90 Enhancements

- The IP Lockdown command was implemented in release I.08.90
- The MSTP enhancement implementing the CLI command for spanning-tree legacy-path-cost was included in release I.08.89
- The MSTP enhancement implementing the CLI command for spanning-tree legacy-mode was included in release I.08.90

IP Lockdown

Beginning with release I.08.90 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.

The IP lockdown command functions as follows:

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

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

The following operating rules apply 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.

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 I.08.91 Enhancements

Software fixes only; no new enhancements.

Release I.08.93 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*, available on the ProCurve Networking Web site.

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 I.08.93, 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
```

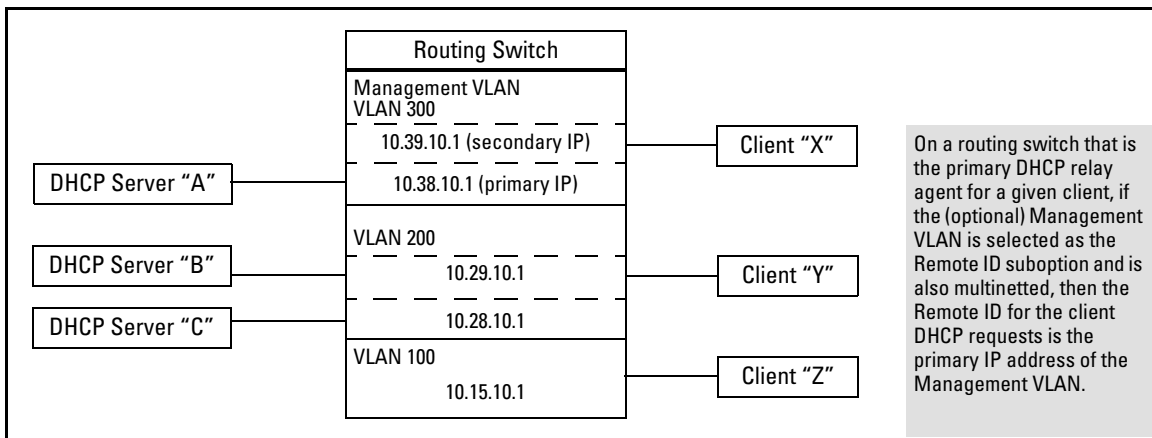


Figure 2. DHCP Option 82 When Using the Management VLAN as the Remote ID Suboption

The resulting effect on DHCP operation for clients X, Y, and Z is shown in [table 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 2800 switches with software release I.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 25.](#)

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 1-3:

Table 1-3. 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.
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 25](#).

< **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)
ntp: 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.

```
WorkingConfig(config)# show ip forward-protocol

IP Forwarder Addresses
  [UDP Broadcast Forwarding: Disabled]
[VLAN: 1]
| IP Forward Addresses  UDP Port |
|-----|
| 15.75.11.43           37      |
| 15.75.11.255         53      |
| 15.75.12.255         1813     |
|-----|
| VLAN: 2              |
| IP Forward Addresses  UDP Port |
|-----|
| 15.75.12.255         1812     |
|-----|
| VLAN: 3              |
| IP Forward Addresses  UDP Port |
|-----|
| 15.75.10.155         162      |
|-----|
```

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

```
ProCurve(config)# show ip forward-protocol [vlan 1]

IP Forwarder Addresses
  [UDP Broadcast Forwarding: Disabled]
[IP Forward Addresses  UDP Port]
|-----|
| 15.75.11.43           37      |
| 15.75.11.255         53      |
| 15.75.12.255         1813     |
|-----|
```

Figure 1-2. 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 I.08.94 Enhancements

Software fixes only; no new enhancements.

Release I.08.95 Enhancements

- Beginning with release I.08.95, the Port Name along with Port number are now displayed on the Web User Interface Status and Configuration screens.
- Enabled custom login banners with "Message of the Day" (MOTD) feature.
- Added new "show sFlow" commands.

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 :

```

                                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

We'd like to keep you up to date about:
 * Software feature updates
 * New product announcements
 * Special events

Please register your products now at:  www.ProCurve.com

Password: █

```

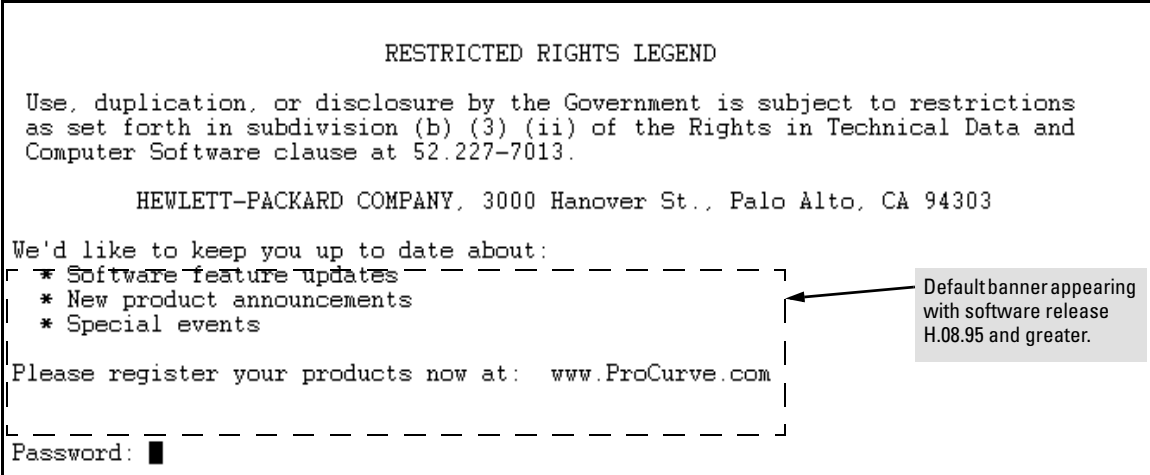


Figure 4. The Default Login Banner

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 figure [Figure 4](#) on page 27.)

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 [Figure 4](#), 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 5. 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 6. 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 7. 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 8. 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:

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

      To Home Page
```

Figure 9. 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

Show sFlow Commands

In earlier software releases, the only method for checking whether sFlow is enabled on the switch was via an snmp request. Beginning with software release I.08.95, the ProCurve Series 2800 switches have added the following 'show sFlow' commands that allow you to see sFlow status via the CLI.

Syntax: show sflow agent

Displays sFlow agent information. The agent address is normally the ip address of the first vlan configured.

Syntax: show sflow destination

Displays information about the management station to which the sFlow sampling-polling data is sent.

Syntax: show sflow sampling-polling <port-list/range>

Displays status information about sFlow sampling and polling.

Syntax: show sflow all

Displays sFlow agent, destination, and sampling-polling status information for all the ports on the switch.

Terminology

sFlow — An industry standard sampling technology, defined by RFC 3176, used to continuously monitor traffic flows on all ports providing network-wide visibility into the use of the network.

sFlow agent — A software process that runs as part of the network management software within a device. The agent packages data into datagrams that are forwarded to a central data collector.

sFlow destination — The central data collector that gathers datagrams from sFlow-enabled switch ports on the network. The data collector decodes the packet headers and other information to present detailed Layer 2 to Layer 7 usage statistics.

Viewing sFlow Configuration

The **show sflow agent** command displays read-only switch agent information. The version information shows the sFlow MIB support and software versions; the agent address is typically the ip address of the first vlan configured on the switch.

```
ProCurve# show sflow agent
Version          1.3;HP;I.08.95
Agent Address    10.0.10.228
```

Figure 10. Viewing sFlow Agent Information

The **show sflow destination** command includes information about the management-station's destination address, receiver port, and owner.

```
ProCurve# show sflow destination
sflow            Enabled
Datagrams Sent   221
Destination Address 10.0.10.41
Receiver Port    6343
Owner            admin
Timeout (seconds) 333
Max Datagram Size 1400
Datagram Version Support 5
```

Figure 11. Example of Viewing sFlow Destination Information

Note the following details:

- **Destination Address** remains blank unless it has been configured on the switch via SNMP.
- **Datagrams Sent** shows the number of datagrams sent by the switch agent to the management station since the switch agent was last enabled.
- **Timeout** displays the number of seconds remaining before the switch agent will automatically disable sFlow (this is set by the management station and decrements with time).
- **Max Datagram Size** shows the currently set value (typically a default value, but this can also be set by the management station).

The **show sflow sampling-polling** command displays information about sFlow sampling and polling on the switch. You can specify a list or range of ports for which to view sampling information.

```

ProCurve# show sflow sampling-polling 1-5

sflow destination Enabled

Port | Sampling           Dropped | Polling
      | Enabled  Rate      Header Samples | Enabled  Interval
-----+-----
1    | Yes      6500000  128   5671234 | Yes      60
2    | No       50        128    0        | Yes     300
3    | Yes     2000       100   24978    | No       30
4    | Yes     200       100  4294967200 | Yes     40
5    | Yes    20000      128    34        | Yes     500

```

Figure 12. Example of Viewing sFlow Sampling and Polling Information

The **show sflow all** command combines the outputs of the preceding three show commands including sFlow status information for all the ports on the switch.

Version I.08.96 was never released

Release I.08.97 Enhancements

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.

Release I.08.98 through Release I.08.99 Enhancements

Software fixes only; no new enhancements.

Release I.08.100 Enhancements

- Added support for Unidirectional Fiber Break Detection.
- Added support for the Advanced Encryption Standard (AES) privacy protocol for SNMPv3.

Release I.08.101 Enhancements

Spanning Tree Per-Port BPDU Filtering

The STP BPDU filter feature allows control of spanning-tree participation on a per-port basis. It can be used to exclude specific ports from becoming part of spanning tree operations. A port with the BPDU filter enabled will ignore incoming BPDU packets and stay locked in the spanning-tree forwarding state. All other ports will maintain their role.

Here are some sample scenarios in which this feature may be used:

- To have STP operations running on selected ports of the switch rather than every port of the switch at a time.
- To prevent the spread of errant BPDU frames.

- To eliminate the need for a topology change when a port's link status changes. For example, ports that connect to servers and workstations can be configured to remain outside of standard spanning-tree operations.
- To protect the network from denial of service attacks with spoofing spanning-tree BPDUs by dropping incoming BPDU frames.

Configuring STP BPDU Filters

The following commands allow you to configure BPDU filters via the CLI.

Syntax: [no] spanning-tree <port-list | all> bpdu-filter

Enables/disables the BPDU filter feature on the specified port(s).

For example, to configure BPDU filtering on port 3, enter:

```
ProCurve(config)# spanning-tree 3 bpdu-filter
```

Caution

Ports configured with the BPDU filter mode remain active (learning and forward frames); however, spanning-tree cannot receive or transmit BPDUs on the port. The port remains in a forwarding state, permitting all broadcast traffic. This can create a network storm if there are any loops (that is, trunks or redundant links) using these ports. If you suddenly have a high load, disconnect the link and remove ("no") the bpdu-filter.

Viewing Status of BPDU Filtering

The **show spanning-tree <port-list> detail** command has been extended to show per-port BPDU filter mode as shown below.

```

ProCurve# show spanning-tree 3 detail

Status and Counters - RSTP Port(s) Detailed Information

Port                : 3
Status              : Down
BPDU Filtering      : Yes
Errant BPUDUs received : 0
Role                : Disabled
State               : Disabled
Priority            : 128
Path Cost           : 200000
Root Path Cost      : 0
Root Bridge ID      : 0:000000-000000
Designated Bridge ID : 0:000000-000000
Designated Port ID  : 0:3
AdminEdgePort       : Yes
OpenEdgePort        : No
AdminPointToPointMAC : Force-True
OpenPointToPointMAC  : No
Aged BPDUs Count    : 0
Loop-back BPDUs Count : 0
TC Detected          : 0
TC Flag Transmitted  : 0 TC ACK Flag Transmitted :0
TC Flag Received    : 0 TC ACK Flag Received :0

RSTP      RSTP      CFG      CFG      TCN      TCN
BPDUs Tx  BPDUs Rx  BPDUs Tx  BPDUs Rx  BPDUs Tx  BPDUs Rx
-----
0         0         0         0         0         0
  
```

Rows indicating BPDU filtering has been enabled and number of errant BPDUs received.

Column indicating BPDU frames accepted for processing when permitted by BPDU filter.

Figure 2. Example of BPDU Filter Fields in Show Spanning Tree Detail Command

The output shown above is an example using the default RSTP (802.1w) protocol. The output will differ if you are using MSTP (802.1s) protocol on the switch.

The **show spanning-tree** command has also been extended to display BPDU filtered ports.

```
ProCurve# show spanning-tree

Multiple Spanning Tree (MST) Information

STP Enabled      : Yes
Force Version    : MSTP-operation
IST Mapped VLANs : 1-7
...

Protected Ports :
Filtered Ports   : 6-7
....
```

Figure 3. Example of BPDU Filtered Ports Field in Show Spanning Tree Command

Viewing Configuration of BPDU Filtering

The BPDU filter mode adds an entry to the spanning tree category within the configuration file.

```
ProCurve(config)# show configuration
. . .
spanning-tree
spanning-tree 7 bpdu-filter
spanning-tree 9 bpdu-filter
spanning-tree Trk2 priority 4
. . .
```

Figure 4. Example of BPDU Filters in the Show Configuration Command

The **spanning-tree show < port> configuration** command displays the BPDU's filter state.

```
ProCurve(config)# show spanning-tree 8 config

...

Port Type      | Cost      Priority Edge Point-to-Point MCheck Filter
-----+-----
8  100/1000T | Auto     128    Yes  Force-True   Yes   No
```

Figure 5. Example of BPDU Filter Status in Show Spanning Tree Configuration Command

Release I.08.102 through Release I.08.103 Enhancements

Software fixes only; no new enhancements.

Release I.08.104 Enhancements

Release I.08.104 includes a DHCP Protection enhancement for switch 2800.

Release I.08.105 Enhancements

Software fixes only; no new enhancements.

Software Fixes in Release I.07.32 - I.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 I.08.99](#)” on [page 60](#).

Release I.07.31 was the first software release for the ProCurve 2800 Series.

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

Release I.07.32

Problems Resolved in Release I.07.32

- **Command Line Interpreter PR_95284** — A too long MAC addresses in a port-security CLI command results in:

```
Software exception at exception.c:345 -- in 'mSess1', task ID = 0x141ae70  
-> Memory system error at 0x131b5a0 - memPartFree
```

Here is an example command that would have crashed Version I_07.31:

```
port-security 1 learn-mode static address-limit 1 mac-address 0800000000010000000
```

- **SSH PR_96648** — CERT Advisory CA-2003-24: OpenSSH vulnerability. Fix implemented. For details, see CERT Advisory CA-2003-24 and associated vulnerability note “VU#333628” at <http://www.cert.org/advisories/CA-2003-24.html>.
- **System Log PR_95689** — Excessive Time Sync entries when using a Timep or SNTP server. The system software needed to be adjusted to properly keep synchronized with a configured SNTP server. In earlier versions of software, this resulted in an excessive number of Time Sync entries in the event log. This only applies to the 2800 Series switches running I_07.31 software.

Release I.07.50

Problems Resolved in Release I.07.50

- **CLI PR_97671** — If the number of max-vlans is greater than 15 and the user tries to add new vlan the Switch reports `Commit failed`. In the Web user interface the Switch reports

An error was encountered while attempting to add the VLAN entry.

The message is changed to:

Maximum number of VLANs (max-vlans) has already been reached.

■ **CLI PR_1*3517** — Counters. Various, related issues:

- ifInDiscards (RX drops in the menu interface) includes outbound drops; fixed to display only true inbound drops.
- ifOutDiscards does not report out-bound drops; fixed to display true outbound drops previously shown on ifInDiscards.
- dot1dtpPortInDiscards includes outbound drops; fixed to display only inbound discards.
- ipInDiscards includes outbound drops; fixed to show only inbound IP based discards.

■ **Crash PR_95525** — Various crashes, including:

```
Bus error: HW Addr=0xe1f08796 IP=0x003a51b4 Task='mInstCtrl' Task  
ID=0x1767af8 fp: 0x00000006 sp:0x01767988 lr:0x003979a4
```

■ **Crash PR_1*2979** — Software exception at rstp_port_role_sm.c:44 -- in mRstpCtrl.

■ **GVRP PR_1*3124** — Uncertain error message when trying to add more than max VLANs.

■ **Port Monitoring PR_1*3540 Enhancement** — Add Egress (output) port monitoring.

■ **RSTP PR_1*1612** — Under some circumstances a port may take approximately 30 seconds to go into Forwarding state.

■ **Services PR_1*3867** — ICMP Redirects never age. Causes any incoming or outgoing agent communications such as ping, TELNET, Web, SNMP, etc. to fail with a message similar to the following:

```
HW Addr=0x000-0000-0 IP=0x0-02a22d8 Task='tNetTask' Task ID=0xe2e740.
```

■ **Trunks PR_1*3530** — Enhancement: Increase the limit on trunks and ports per trunk to:

- Up to 24 trunks, total; and
- Up to 8 ports per trunk

Refer to [“New Maximum for Number of Ports in a Trunk”](#) on page 11.

■ **Web/IP Stack Management PR_92826** — With an eight switch IP Stack Management stack, management of the switches with the Web interface can cause the commander switch to crash or hang. If the user selects options too quickly or moves from one option to another the Web user interface may freeze and become unresponsive. The Commander Switch may also crash with a Bus Error. Also, TELNET and Console interfaces may become unresponsive.

■ **Web/IP Stack Management PR_97323** — In the Web user interface the images displayed for the stack members are not correct.

- **Web PR_98500** — Clicking on tabs in a certain order causes the browser window to close (terminate).
- **Web/SSL PR_98918** — When creating an SSL certificate the Organization name and unit are switched in the web user interface display. **Emphasis: This is only a display issue.**
- **Web PR_81848** — The **[Clear changes]** button does not work for the Default Gateway or VLAN selections
- **Web PR_82199** — VLAN port modification shows misleading mode. In the Configuration - VLANs - Modify page, select a port, then set the “mode” modify pull-down menu to “tagged”. Select another port. The “mode” pulldown field remains set to “tagged”, which is misleading and incorrect, in general.
- **Web PR_97407** — Port security error message is unclear with mac lockdown. The user interface may report “**Unable to add new MAC Address. MAC entry is either a multicast, broadcast or NULL address.**” when, in fact, the MAC address the user is specifying is locked down or locked out.
- **Web PR_1*452** — Resetting the Switch leads to the URL **aol.co.uk**.
- **Web PR_90858** — VLAN Name text field won't clear after 12 characters are entered.
- **Web PR_1*1702** — Sometimes clicking on the **[Apply]** button on the Configuration/Monitor Port screen results in the message **Not enough params specified**.
- **Web PR_92078** — After making changes under the Device Features tab, the page never fully loads.
- **Web PR_82039** — If the user selects GVRP mode, selects a port, and then selects nothing as an option for the port mode, all ports below the selected port disappear. This does not affect the switch configuration.

Release I.07.52 (Beta Only)

Problems Resolved in Release I.07.52

- **GVRP PR_1*5082** — Vague error message (`commit failed`) when trying to add more than the maximum number of allowed VLANs.
- **Performance PR_1*11958** — Enhancement: Added the **qos-passthrough-mode** configuration option to the CLI to configure the number of outbound queues to use. Refer to “[QOS Pass-Through Mode](#)” on page 12.
- **Trunking PR_1*5962** — Unable to form LACP dynamic trunk across ASIC port groups without routing enabled.

- **sysUptime PR_1*4025** — sysUptime wraps in approximately 49 days.
- **Web PR_1*4111** — The Stack Management view has a scroll problem.
- **Web PR_1*3580** — The web interface allows broadcast and multicast destination addresses.
- **Web PR_1*7144** — VLAN Configuration Help link is not available.

Release I.07.53 (Beta Only)

Problems Resolved in Release I.07.53

- **Crash PR_1*3390** — Memory leak causing crash `sw_malloc.c:141` in `snmpevt` task.
- **Crash PR_1*13156** — Master crash in memory system - `memPartFree`. The specific crash symptoms can vary widely.
- **RMON PR_1*11690** — The switch does not send RMON trap PDUs.

Release I.07.55 (Beta Only)

Problems Resolved in Release I.07.55

- **Crash PR_1*20824** — Displays a crash message similar to the following:

```
SubSystem 0 went down: 01/02/90 22:33:36 NMI occurred: IP=0x003164b0
MSR:0x0000b032 LR:0x003164d4 Task='tDPC' Task ID=0x1ad2440 cr:
0x28000080 sp:0x01ad2380 xer:0x00000000.
```
- **Flow Control PR_98957** — The switch honors PAUSE (flow control) frames that it receives, but it does not generate them.
- **Show Mac PR_82086** — The CLI command **show mac** < *mac-address* > does not work.
- **OpenSSL/crash PR_1*12823** — OpenSSL bus error vulnerability.

Release I.07.56

Problems Resolved in Release I.07.56

- **Hang PR_1*87409, PR_1*6985** — Symptoms vary, and can include any of the following:
 - Switch does not respond to pings, WEB access, Telnet, or Console access.
 - Pre-existing links prior to the “hang” still appear to transmit and receive data normally.

- LED behavior on ports that establish link before the “hang” is erratic. For example, the LED remains lit even after dropping physical link.
- New links attempted after the “hang” do not transmit or receive traffic. Also that port's LED on the Switch 2800 remains dark, indicating no link while the neighbor device's LED may light up indicating that link is established.
- Front panel LED Mode, Reset, and Clear buttons, may not function properly.
- CPU-dependent features such as STP may not function properly.

A power cycle of the switch has been the only way to relieve these “hang” symptoms. Since the switch agent does not respond and the front panel buttons may not respond, it may be necessary to unplug and re-plug the power cable in order to reset the switch.

Release I.07.57 (Never Released)

Release I.07.58 (Beta Only)

Problems Resolved in Release I.07.58

- **IGMP PR_1*06552 and 1*20234** — The switch floods multicast packets on a VLAN when IGMP is enabled, due to h/w & s/w MAC tables being out of sync.
- **TELNET PR_1*19573** — Switch reboots when telnet is disabled and port 1506 accessed. The switch produces no crash-log.
- **Web PR_89899** — In the Web UI, port statistic counters are overwriting one another.
- **IGMP/EIGRP PR_1*20234** — With IGMP enabled the switch drops EIGRP packets (when triggered by receiving an SSDP packet).
- **VLAN PR_95593** — The switch will not allow the user to delete a VLAN that contained a mini-GBIC port that was removed.
- **CLI/Config PR_1*01628** — In the CLI, switch reports “Inconsistent value” error when adding ports to a VLAN.
- **Hot-swap/Config PR_1*89150** — Switch configuration is not properly updated on transceiver swap events
- **Boot ROM** — Updated to I.08.02 version to support up to 3 MB size System Image files.

Release I.07.59 (Beta Only)

Release I.07.60

Problems Resolved in Release I.07.60

- **Auto-TFTP/Rebooting PR_1*20802** — Auto-TFTP causes constant rebooting, with no resulting crash files.
- **Auto-TFTP PR_1*187649** — Auto-TFTP will not allow a forced download of software after Auto-TFTP is Disabled.
- **Hang PR_1*190119** — Additional case of system hang found and addressed.

Release I.07.61

Problems Resolved in Release I.07.61

- **DHCP Relay PR_1*188635** — DHCP Relay sometimes preserves the incoming MAC SA in relayed packets.
- **HANG/WEB PR_1*190109** — Fix for cases where the Web interface would stop responding when the user enters the Configuration Screen. Once triggered, no access to the Web agent is possible from any client.

Release I.07.62 (Beta Only)

- **QOS PR_1*194538** — QOS-Pass -Through-Mode (introduced in I.07.52) does not work in software versions I.07.54-I.07.61

Release I.07.63 (Beta Only)

- **Boot ROM PR_1*85713** — Introduced the I.08.03 Boot ROM patcher to address a 'boot hang' issue. This Boot ROM was later updated to I.08.04 (see Release I.07.64).

Release I.07.64

Problems Resolved in Release I.07.64

- **Boot ROM PR_1*202277** — Contains and installs the I.08.04 Boot ROM which fixes the 'port hang' problem when back-revving to software versions older than I.07.58 when running the I.08.03 Boot ROM. Also, improves on the 'reload hang' fix that is in I.08.03 by specifically addressing the 'boot hang' that can occur after the I.08.03 Boot ROM's patcher (the 'patcher' is the part of the software that installs the new Boot ROM) does a reboot.

Release I.07.65 (Not Released)

Problems Resolved in Release I.07.65

- **Other** — Added diagnostic code for isolating the "dead-port" issues at hot-site.

Release I.07.66

Problems Resolved in Release I.07.66

- **Dead Port PR_1*207174** — Reduces or eliminates the occurrences of the "dead-port" issue. "Dead-port" implies the following symptoms:
 - Some 2800 ports may not forward packets, while other ports continue to forward packets.
 - Link LED stays on when cable removed
 - Link LED stays off when cable attached.

Release I.07.67

Problems Resolved in Release I.07.67

- **Port Hang (PR_1000212920)** — Contains and automatically installs (after reboot) Boot ROM version I.08.05. This Boot ROM fixes the 'port hang' issue which can result in unpredictable switching and LED behavior.

Release I.07.68

Problems Resolved in Release I.07.68

- **Other PR_1000200341** — Added an exception handler to prevent a case where the system may hang.
- **Boot ROM** — Updated to version I.08.05

Release I.08.55

Problems Resolved in Release I.08.55

- **CLI PR_82258** — **sh ip igmp** command shows blank lines inter-mixed within the displayed table.
- **CLI PR_1*3169** — 2800: "port-security learn-mode configured " is shown as "static" in CLI.
- **CLI PR_1*11958** — Add CLI command to configure the outbound queue (2 or 4 queue).
- **CLI PR_1*18700** — **Show ip route** "IP Route Entries" not centered in output.
- **Config PR_92346** — Unable to delete empty VLAN.
- **Crash PR_91463** — Displays a crash message similar to the following:
Software exception at ip_util.c:413 -- in 'ifInfo', task ID = 0x143fb60
- **Crash PR_93791** — Displays a crash message similar to the following:
Software exception at bcmHwFeatures.c:108 -- in 'mAdMgrCtrl'
- **Crash PR_1*1537** — Memory leak on 2848, fatal exception in malloc_else_fatal().
- **Crash PR_1*5466** — Displays a crash message similar to the following:
Software exception in ISR at bcm56xxDmaPoll.c:623 (top-of-tree)
- **Crash PR_1*20805** — Displays a crash message similar to the following:
Software exception @ route.c:331 (attempting to free an already freed rtenry)
- **Crash PR_1*21853** — Displays a crash message similar to the following:
Software exception @ radix.c:922, route does not exist in the 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 on 2800 and 2600 have hotswap out problem.
- **LACP PR_1*6404** — Dynamic LACP: Standby mode problem.
- **MCAST PR_1*6552** — Multicast pkts flooded on a VLAN w/ igmp enabled; hw & sw out of sync.
- **Menu PR_94905** — 2848 Configuration screen shows only 32 VLANs of configured 48.
- **Ping PR_1*19945** — Unable to ping through default gateway.

- **Routing PR_1*5961** — Layer 3 connectivity lost when address is moved across ASIC port group.
- **Routing PR_1*20234** — 2800 / I.07.53 / I.07.52: DD IGMP Squelches EIGRP when triggered by SSDP Packet.
- **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 between 6108 and 2800.
- **VLAN PR_90884** — VLAN PORT_UNTAGGEDMAP config not being set correctly.
- **VLAN PR_92413** — Broadcasting is forwarded outside the VLAN.
- **Web PR_1*1216** — Web UI, log error.
- **Web PR_1*12103** — Garbage in the Web UI Status | Overview screen.
- **Web PR_1*21294** — Stack Management Screen is blank.
- **Web PR_1*21867** — Web UI VLAN Configuration is broken.

Release I.08.56

Problems Resolved in Release I.08.56

- **Port Hang (PR_1000207174)** — Reduces or eliminates the occurrence of "port hang" issues, where one or more ports may cease to forward traffic and the LEDs display status may be incorrect.

Release I.08.57

Problems Resolved in Release I.08.57

- **Port Hang (PR_1000212920)** — Unpredictable switching and LED behavior where one or more ports may cease to forward traffic.
- **SNMP (PR_1000190654)** — Some of the fault finder events in the SNMP traps list a 0.0.0.0 IP address in the URL.

Release I.08.58

Problems Resolved in Release I.08.58

- **802.1s (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.

Release I.08.60

Problems Resolved in Release I.08.60

- **ACL (PR_1000207620)** — The switch sometimes incorrectly permits TCP and UDP traffic in spite of an ACL configuration.
- **CLI (PR_1000202435)** — When IGMP fast-leave is configured via the CLI, the configuration is not displayed with the "show configuration" command.
- **CLI enhancement(no PR)** — Added "console local-terminal" for immediate session only mode (i.e. no "write mem" required as is for "console terminal" command). Useful for terminal scripts that require that Screen Control characters not be displayed in output
- **Config (PR_1000087886)** — The CLI will display error message "Value 1000-full is not applicable to port <port num>", when trying to download a startup-configuration with a Mini-GBIC module configured at 1000 full duplex.
- **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_1000200341)** — In some cases a protocol or feature may not function correctly.
- **Crash (PR_1000208530)** — Unpredictable results
- **Crash (PR_1000201614)** — When the switch is set with a 16 character manager password within the setup menu, a 'Bus error' crash may occur.
- **DHCP Enhancement (PR_1000207639)** — DHCP Option 82 implementation (DHCP Tracker).
- **DHCP Relay (PR_1000207419)** — The DHCP Relay agent was disabled by default in earlier Version 8 releases. With this fix, the DHCP Relay agent is enabled by default, as it was in I.07 releases.
- **IP Helper/DHCP Relay (PR_1000197046)** — The switch may not handle "DHCP Inform" relay messages properly from the client, resulting in a failed transaction.
- **Management enhancement (No PR)** — Non-Persistent console terminal mode.

- **Other PR_1000209839** — Memory corruption of dmaStats do to off array boundary error.
- **Other PR_1000200341** — Added an exception handler to prevent a case where the system may hang.
- **Open VLAN (PR_1000210932)** — Open VLAN mode (Unauthorized VLAN) does not work with any Port-Security Learn-Mode.
- **RMON (PR_1000196477)** — When RMON thresholds in the switch are exceeded no trap is generated.
- **SNMP (PR_1000196170)** — Traps are not buffered before the IP stack is initialized, causing the possibility of missing some traps generated during startup.
- **SNMP (PR_1000212170)** — The Switch transmits Warm and Cold Start traps with an agent address of 0.0.0.0.
- **Testmode (PR_1000212159)** — Added the testmode command 'memWatch'
- **Web Enhancement (NO PR)** — RADIUS for the Web browser interface.
- **Web UI/Port Security (PR_1000195894)** — The Web user interface does not allow the user to select multiple ports when configuring port-security.
- **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.
- **Web UI (PR_1000210110)** — Slow Web UI performance.

Release I.08.61

Problems Resolved in Release I.08.61

- **CLI (PR_1000214598)** — The switch does not accept the CLI command "spanning-tree 1 mode fast".
- **Config (PR_1000216051)** — Reloading a previously saved startup-configuration with command "stack join (mac address)" to a member switch of the IP stack breaks the membership of that same stack. Commander hangs with member "mismatched".
- **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 I.08.62

Problems Resolved in Release I.08.62

- **Crash (PR_1000207542)** — The switch may crash with a bus error or a task hang.
- **Crash (PR_1000215009)** — Software exception in ISR at `intr.c:595 -> FATAL SCHAN ERROR.`
- **Enhancement (PR_1000213492)** — QoS-Passthrough can be enabled at run time vs. requiring a write memory and reboot. (Enhancement documentation to be provided at a later time.)
- **Flow Control (PR_1000217576)** — Flow control/jumbo frame error messages not generated in event log.
- **Port Security (PR_1000203984)** — CLI port-security command - mac-address command will save more addresses than is configured.

Release I.08.63

Problems Resolved in Release I.08.63

- **Config (PR_1000207697)** — Loading a startup configuration file fails when file defines a new VLAN as a management VLAN.
- **Crash (PR_1000216170)** — The switch may crash with a Bus Error message similar to:

```
SubSystem 0 went down: 01/01/90 00:00:42 Bus error: HW
Addr=0x00000000 IP=0x00000000 Task='mftTask' Task ID=0x12be680 fp:
0xffffffffd sp:0x012bd968 lr:0xffffbfff .
```
- **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 I.08.64

Problems Resolved in Release I.08.64

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

Release I.08.67

Releases I.08.65 and I.08.66 were never released.

Problems Resolved in Release I.08.67

- **Authentication (PR_1000217338)** — Inconsistent authentication results with EAP-TLS and EAP-PEAP authorization types.
- **Config (PR_94943)** - Setup screen allows illegal configuration (Proxy-Arp). Using the 'Setup' CLI command and "setup" menu option, users can toggle the Proxy-ARP entry even though IP-routing is NOT enabled on the system.
- **Console/TELNET (PR_1000195647)** — When a console or TELNET session hangs, issuing the 'kill' command will also hang.
- **Counters (PR_1000219548)** — Collision counters do not increment accurately.
- **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.
```
- **IP Routing (PR_1000220668)** — Fatal exception when routing with more than 8 trunks configured. Configure more than 8 trunks and enable IP routing, then send routed traffic over the 9th, 10th trunk configured and the switch will crash.
- **Menu (PR_1000221018)** — When IP routing is disabled via the Menu, Proxy ARP remains in the configuration file and results in a configuration file that cannot be downloaded to the switch.
- **Syslog (PR_1000215699)** — Switch does not send all Event Log entries to the syslog server at switch boot up.
- **QoS (PR_1000200746)** — Switch truncates a newly created DSCP-map name after a reboot. Configure a dscp-map name that requires quotes such as "Code Point 0". Save this name in the configuration file and reboot the switch, the name is truncated to "Code".

- **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 I.08.68

Problems Resolved in Release I.08.68

- **802.1s (PR_1000233920)** — 802.1s blocks a port that is connected to an RSTP device.
- **802.1s (PR_1000227432)** — The learning flag is not set when Common Instance Spanning Tree (CIST) port states are transitioning.
- **Broadcast throttling (PR_1000240494)** — Broadcast throttling on Gigabit ports do not throttle above 18%.
- **Crash (PR_1000229656)** — The switch cannot reach the 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)** — In some cases, Web Authentication does not provide a login page to a second client.
- **Web/Stack Management (PR_1000239924)** — As an IP Stack Management Commander, the Switch does not display the device view (back of box) for a Switch 2626 which is a member.

Release I.08.69

Problems Resolved in Release I.08.69

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

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

Release I.08.70

Problems Resolved in Release I.08.70

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

Release I.08.71

Problems Resolved in Release I.08.71

- **Crash (PR_1000282197)** — On initial install, the 2848 switch may reboot with no crash history, simply the following message:

System reboot due to power failure.
- **SNMP (PR_1000003378)** — SNMP switch time may drift with event log updates occurring every 1.5 hours.
- **Boot ROM** — Updated to I.08.07 version to support fix for PR 1000282197.

Release I.08.72

Problems Resolved in Release I.08.72

- **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 deletes previously learned Members.

Release I.08.73

Problems Resolved in Release I.08.73

- **RSTP (PR_1000286883)** — Slow RSTP fail-over and fall-back time.
- **VLAN (PR_1000286883)** — When attempting to delete a VLAN listed as a management VLAN, the switch incorrectly leaves the management VLAN statement in the running configuration file.

Release I.08.74

Problems Resolved in Release I.08.74

- **MSTP (PR_1000286883)** — Slow MSTP fail-over and fall-back time.
- **FEC/CDP (PR_1000281734)** — FEC and CDP transmit removal.

- **LLDP (Enhancement)** — Added support for LLDP (Link Layer Discovery Protocol) IEEE 802.1AB.

Release I.08.81

Problems Resolved in Release I.08.81

- **Fault (PR_1000089786)** — Chassis fault LED stops blinking after a new OS image was 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.

Versions I.08.75 through I.08.79 were never built. Version I.08.80 was never released.

Release I.08.82

Problems Resolved in Release I.08.82

- **CDP (PR_1000239009)** — CDP transmit was re-enabled after a reload.
- **RSTP (PR_1000297195)** — The switch repeatedly flushes its MAC address table, resulting in intermittent flooding of all traffic.

Release I.08.83

Problems Resolved in Release I.08.83

- **Boot (PR_1000291806)** — Implemented "fastboot" option to skip diagnostic testing and allow system to reboot within 90 seconds.
- **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 I.08.84

Problems Resolved in Release I.08.84

- **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 I.08.85

Problems Resolved in Release I.08.85

- **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.
- **CLI (PR_1000292455)** — Enhancement— Rate display for ports on CLI. New command: "show interface port-utilization". Not available on Menu nor Web Interface.
- **Event Log (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: Unsupported feature "FEC" for trunk configuration;  
see release notes
```

Release I.08.86 (Limited release)

- **RSTP (No PR)** — Resolved broadcast storm caused by an unstable RSTP topology

Release I.08.87

Problems Resolved in Release I.08.87

- **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.
- **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 I.08.88

Problems Resolved in Release I.08.88 (never released)

- **STP (PR_1000307280)** — Inconsistent or incorrect STP data.
- **RSTP (PR_1000309683)** — Temporary routing or switching problems after RSTP is disabled.
- **Menu (PR_1000306213)** — When using the Menu to create a trunk, the new trunk ports will become disabled after a switch reboot.

Release I.08.89

Problems Resolved in Release I.08.89 (never released)

- **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 17](#) for details.
- **Port-Security (PR_1000304202)** — The port-security MAC address learn mode is not functioning correctly.
- **SNMP (PR_1000285195)** — Switch does not save the option to disable a Link up/down SNMP trap after a switch reboot.
- **SNMP (PR_1000310841)** — User can assign illegal values for CosDSCP Policy through SNMP.

Release I.08.90

Problems Resolved in Release I.08.90 (never released)

- **IP Lockdown Enhancement (PR_1000316142)** — Implemented the IP lockdown feature.
- **MSTP Enhancement (PR_1000313986)** — Implemented new CLI command, "spanning-tree legacy-mode". See [“MSTP Default Path Cost Controls” on page 17](#) for details.

- **RADIUS (PR_1000316158)** — After a switch reboot, the switch does not recognize a response from a RADIUS or TACACS server.
- **Show Tech Enhancement (PR_1000315018)** — Upgrade of 'show tech' statistics command to include internal ASIC port counters.

Release I.08.91

Problems Resolved in Release I.08.91 (never released)

- **Config (PR_1000298146)** — Enabling QoS-passthrough Mode causes incorrect information to be displayed in the "show configuration" command.

Release I.08.92

Problems Resolved in Release I.08.92 (never released)

- **802.1X (PR_1000304129)** — The Wireless Services Edge xl Module (J9001A) does not authenticate (802.1X) against the Switch.
- **Help (PR_1000317711)** — In the VLAN menu Help text, the word 'default' is spelled incorrectly.
- **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 are entering the switch syslog when a valid SNMPv3 'get' operation is initiated.
- **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 I.08.93

Problems Resolved in Release I.08.93 (never released)

- **Enhancement (PR_1000319920)** — Added support for DHCP Option 82, and added 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 I.08.94

Problems Resolved in Release I.08.94

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

Release I.08.95

Problems Resolved in Release I.08.95

- **Counters (PR_1000321097)** — Drop counters may display incorrect information.
- **Crash (PR_1000322009)** — The Switch may crash with a message similar to:
Software exception in ISR at queues.c:123.
- **Crash (PR_1000327132)** — The Switch may crash with a message similar to:
Software exception in ISR at btmDmaApi.c:304.
- **Enhancement (PR_1000242392)** — Enabled login banner "Message of the Day" (MOTD).
- **Enhancement (PR_1000290489)** — Enhancement to display Port Name along with Port number on the Web User Interface Status and Configuration screens.
- **Enhancement (PR_1000328716)** — Added new "show sFlow" commands.
- **ICMP (PR_1000235905)** — Switch does not send a 'destination unreachable' response message when trying to access an invalid UDP port.
- **sFlow (PR_1000321195)** — A network management application may incorrectly report traffic spikes when sFlow is first re-enabled.
- **SNMPv3 (PR_1000325021)** — Under some conditions, SNMPv3 lines are not written to the running-configuration file.

Release I.08.96 (Never released)

Release I.08.97

Problems Resolved in Release I.08.97

- **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 I.08.98

Problems Resolved in Release I.08.98

- **Crash (PR_1000335117)** — The Switch may crash with a message similar to:
FATAL SCAN ERROR S=13 D=15 OPC=20 (MEM_FAIL_NOTIFY) ECODE=0.
- **CLI (PR_1000334412)** — Person logged in with Operator level can save Manager privilege level changes to the configuration.
- **Log (PR_1000323790)** — The switch detects a non-genuine ProCurve mini-GBIC as a port self test failure and subsequently disables the link.

Release I.08.99

- **CLI (PR_1000330553)** — When issuing the CLI command "show snmp-server," unrecognizable characters are displayed in the output.
- **Crash (PR_1000339551)** — When using the Menu to disable IP routing, the Switch may crash with a message similar to:
PPC Bus Error exception vector 0x300: Stack-frame=0x0162e030
HW Addr=0x2e2e2e2d.
- **Menu (PR_1000319651)** — In the "Internet (IP) Service" menu screen, user is unable to use the "Save" function to exit the screen. User must use "Cancel" to exit from the screen.

- **STP (PR_1000335141)** — The output of the "show span" CLI command displays incorrect information.

Release I.08.100

- **CLI (PR_1000317554)** — The command "show version" does not display the full version number.
- **DHCP (PR_1000343149)** — Client cannot obtain an IP address when two DHCP servers are connected on different local networks.
- **Enhancement (PR_1000344652)** — Added support for Unidirectional Fiber Break Detection.
- **SNMPv3 Enhancement (PR_1000338847)** — Added support for the Advanced Encryption Standard (AES) privacy protocol for SNMPv3.
- **VLAN (PR_1000284852)** — The Switch may transmit packets with a VLAN ID that is out of range.

Release I.08.101

- **CLI (PR_1000334494)** — Issuing the "show vlans" command causes incorrect information to be displayed in the "VLAN ID" field.
- **Enhancement (PR_1000336169)** — Added support for STP Per Port BPDU Filtering and SNMP Traps. See ["Spanning Tree Per-Port BPDU Filtering" on page 35](#) for details.
- **Web UI (PR_1000340311)** — When using the web user interface and accessing the "Security" tab, the switch will request the manager username and password. Then select the "Port Access" button, a second log-in box appears and requests the same manager username and password multiple times, causing the IE browser to hang and requiring the browser to be reset.

Release I.08.102 (Never released)

Release I.08.103

- **Crash (PR_1000348454)** — The switch may reboot with an NMI event when a loop is formed on the network. The crash task may vary by switch configuration.

- **Radius EAP (PR_1000334731)** — PEAP/TLS EAP types fail to authenticate with Microsoft IAS Radius Server. The switch event log will report, "can't reach RADIUS server."

Release I.08.104

- **Crash (PR_1000352922)** — The switch may crash with a message similar to
Software exception at mstp_ptx_sm.c:118 -- in 'mMstpCtrl', task
ID = 0x8899e70.-> ASSERT: failed
- **Enhancement (PR_1000354065)** — DHCP Protection enhancement for switch 2800.

Release I.08.105

- **CLI (PR_1000342461)** — When a trunk is configured on an uplink port, the command "show lldp info remote <port number>" reports incorrect information for the remote management address.
- **CLI (PR_1000358129)** — The command line interface (CLI) becomes unresponsive after running RMON traps code.
- **Crash (PR_1000351410)** — When the switch IP address is pinged from a local serial console interface, the switch may crash with an error similar to the following.
PPC Bus Error exception vector 0x300: Stack-frame=0x067d40e8 HW
Addr=0x33cc33d2 IP=0x0056a8f8 Task='tNetTask' Task ID=0x67d4278
- **Crash (PR_1000352177)** — The switch may crash in response to repeatedly pinging an unreachable host, displaying a message similar to:
Software exception at alloc_free.c:362 -- in 'mLinkTest', task
ID = 0x5be24d0.
- **Hang (PR_1000346328)** — RMON alarms/events configuration files may become corrupt and prevent initialization, resulting in failure to boot.
- **LLDP (PR_1000310666)** — The command "show LLDP" does not display information learned from CDPv2 packets.

Known Software Issues and Limitations

Issues

None 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 hpSwitchIcmpPortFastLeaveState<.vlan number>
```

```
HPswitch# walkmib hpSwitchIcmpPortFastLeaveState.20
hpSwitchIcmpPortFastLeaveState.20.2 = 1
hpSwitchIcmpPortFastLeaveState.20.3 = 2
HPswitch# walkmib hpSwitchIcmpPortFastLeaveState.35
hpSwitchIcmpPortFastLeaveState.35.5 = 2
hpSwitchIcmpPortFastLeaveState.35.6 = 1
hpSwitchIcmpPortFastLeaveState.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)



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

September 2006 -B
Part Number
5990-6049