



# Release Notes:

## Version U.11.11 Software

*for the ProCurve 2510-48 Switches*

---

### **Release U.11.10 supports these switches:**

- ProCurve Switch 2510-48 (J9020A)

### **These release notes include information on the following:**

- Downloading Switch Documentation and Software from the Web ([page 1](#))
- Software enhancements available in releases U.11.11 ([page 14](#))
- A listing of software fixes included in releases U.11.11 ([page 15](#))

© Copyright 2001, 2008-2009  
Hewlett-Packard Development Company, LP.  
The information contained herein is subject to change  
without notice.

### Publication Number

Part Number 5991-2127  
January 2009

### Applicable Product

ProCurve Switch 2510-48 (J9020A)

### 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](http://www.procurve.com)

# Contents

---

## Software Management

Software Updates .....	1
Downloading Switch Documentation and Software from the Web .....	1

## Downloading Software to the Switch

TFTP Download from a Server .....	3
Xmodem Download From a PC or Unix Workstation .....	4
Saving Configurations While Using the CLI .....	5
ProCurve Switch, Routing Switch, and Router Software Keys .....	6
OS/Web/Java Compatibility Table .....	7
Minimum Software Versions .....	7

## Enforcing Switch Security

Switch Management Access Security .....	8
Default Settings Affecting Security .....	8
Local Manager Password .....	9
Inbound Telnet Access and Web Browser Access .....	9
Secure File Transfers .....	9
SNMP Access (Simple Network Management Protocol) .....	10
Front-Panel Access and Physical Security .....	11
Other Provisions for Management Access Security .....	12
Network Security Features .....	12
Web and MAC Authentication .....	12
Secure Shell (SSH) .....	12
Secure Socket Layer (SSLv3/TLSv1) .....	13

## Enhancements

Release U.11.04 Enhancements .....	14
Release U.11.08 Enhancements .....	14
Release U.11.09 Enhancements .....	14
Release U.11.10 Enhancements .....	14

Release U.11.11 Enhancements ..... 14

**Software Fixes**

Release U.11.04 ..... 15

Release U.11.08 ..... 15

Release U.11.09 ..... 15

Release U.11.10 ..... 18

Release U.11.11 ..... 19

# Software Management

---

## Software Updates

Check the ProCurve Networking Web site frequently for free software updates for the various ProCurve switches you may have in your network.

## Downloading Switch Documentation and Software from the Web

You can download software updates and the corresponding product documentation from HP's ProCurve web site as described below.


### **To Download a Software Version:**

1. Go to the ProCurve Networking Web site at:

<http://www.procurve.com/software>.

2. 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 HP's ProCurve web site at <http://www.procurve.com/manuals>.
2. Click on the name of the product for which you want documentation.
3. On the resulting web page, double-click on a document you want.
4. 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.

---

HP periodically provides switch software updates through the ProCurve Networking Web site <http://www.procurve.com/software>. After you acquire the new software file, you can use one of the following methods for downloading it 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 4).
- Use the download utility in ProCurve Manager Plus.
- A switch-to-switch file transfer

---

## Note

Downloading new software 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.

## 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 R\_11\_04.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
ProCurve # copy tftp flash 10.28.227.103 R_11_04.swi
The primary OS image will be deleted. continue [y/n]? Y
03125K
```

2. When the switch finishes downloading the software file from the server, it displays the progress message:

```
Validating and Writing System Software to FLASH.
```

When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software

3. Reboot the switch.

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

# Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port on a PC operating as a terminal. (Refer to the Installation 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 Microsoft Windows NT® terminal emulator, you would use the **Send File** option in the **Transfer** drop-down menu.)

**Syntax:**     **copy xmodem flash < unix | pc >**

For example, to download a software file from a PC:

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 57600 bits per second. (The baud rate must be the same in both devices.) For example, to change the baud rate in the switch to 57600, execute this command:

```
ProCurve(config)# console baud-rate 57600
```

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

2. Execute the following command in the CLI:

```
ProCurve # 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. The download can take several minutes, depending on the baud rate used in the transfer.
4. 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.

5. Use the following command to confirm that the software downloaded correctly:

```
ProCurve> show system
```

Check the **Firmware revision** line to verify that the switch downloaded the new software.

6. 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.

## 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 to the Main Menu, press **[Y]** (for Yes) when you see the “Do you want to save current configuration [y/n]?” prompt.

## ProCurve Switch, Routing Switch, and Router Software Keys

<b>Software Letter</b>	<b>ProCurve Networking Products</b>
<b>C</b>	1600M, 2400M, 2424M, 4000M, and 8000M
<b>CY</b>	Switch 8100fl Series (8108fl and 8116fl)
<b>E</b>	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
<b>F</b>	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
<b>G</b>	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
<b>H</b>	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
<b>I</b>	Switch 2800 Series (2824 and 2848)
<b>J</b>	Secure Router 7000dl Series (7102dl and 7203dl)
<b>K</b>	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G) and Switch 8212zl.
<b>L</b>	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
<b>M</b>	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 through M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2 ): M.08.51 through M.08.95, or M.08.99 to M.08.100 and greater.
<b>N</b>	Switch 2810 Series (2810-24G and 2810-48G)
<b>PA/PB</b>	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
<b>Q</b>	Switch 2510 Series (2510-24)
<b>R</b>	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
<b>T</b>	Switch 2900 Series (2900-24G, and 2900-48G)
<b>U</b>	Switch 2510-48
<b>VA/VB</b>	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
<b>WA</b>	ProCurve Access Point 530
<b>WS</b>	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
<b>WT</b>	ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module
<b>Y</b>	Switch 2510G Series (2510G-24 and 2510G-48)
<b>numeric</b>	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.)

## 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	
Windows Vista		

## Minimum Software Versions

### For ProCurve Series 2510-48 Switches and Hardware Features

ProCurve Device	Product Number	Minimum Supported Software Version
ProCurve 100-BX-D SFP-LC Transceiver	J9099B	U.11.10
ProCurve 100-BX-U SFP-LC Transceiver	J9100B	U.11.10
ProCurve 1000-BX-D SFP-LC Mini-GBIC	J9142B	U.11.10
ProCurve 1000-BX-U SFP-LC Mini-GBIC	J9143B	U.11.10

# Enforcing Switch Security

---

ProCurve switches are designed as “plug and play” devices, allowing quick and easy installation in your network. However, when preparing the switch for network operation, ProCurve strongly recommends that you enforce a security policy to help ensure that the ease in getting started is not used by unauthorized persons as an opportunity for access and possible malicious actions. Since security incidents can originate with sources inside as well as outside of an organization, your switch and network access security provisions must protect against internal and external threats while preserving the necessary network access for authorized clients and uses.

This section provides an overview of switch management and network access security features and applications. *However, the features and applications supported by your switch depend on your particular switch model.* For information on specific features supported, refer to the software manuals provided for your switch model.

---

## **Caution:**

In its default configuration, the switch is open to unauthorized access of various types. ProCurve recommends that you review this section to help ensure that you recognize the potential for unauthorized switch and network access and are aware of the features available to help prevent such access.

---

## Switch Management Access Security

This section outlines provisions for protecting access to the switch’s status information configuration settings. For more detailed information on these features, refer to the indicated manuals.

### Default Settings Affecting Security

In the default configuration, switch management access is available through the following methods:

- Telnet
- Web-browser interface (including the ability to launch Telnet access)
- SNMP access
- Front-Panel access (serial port access to the console, plus resets and clearing the password(s) or current configuration)

It is important to evaluate the level of management access vulnerability existing in your network and take steps to ensure that all reasonable security precautions are in place. This includes both configurable security options and physical access to the switch hardware.

## Local Manager Password

In the default configuration, there is no password protection. Configuring a local Manager password is a fundamental step in reducing the possibility of unauthorized access through the switch's web browser and console (CLI and Menu) interfaces. The Manager password can easily be set using the CLI **password manager** command, the Menu interface **Console Passwords** option, or the password options under the **Security** tab in the web browser interface.

## Inbound Telnet Access and Web Browser Access

The default remote management protocols enabled on the switch, such as Telnet or HTTP, are plain text protocols, which transfer passwords in open or plain text that is easily captured. To reduce the chances of unauthorized users capturing your passwords, secure and encrypted protocols such as SSH and SSL must be used for remote access. This enables you to employ increased access security while still retaining remote client access.

- SSHv2 provides Telnet-like connections through encrypted and authenticated transactions
- SSLv3/TLSv1 provides remote web browser access to the switch via encrypted paths between the switch and management station clients capable of SSL/TLS operation.

Also, access security on the switch is incomplete without disabling Telnet and the standard web browser access. Among the methods for blocking unauthorized access attempts using Telnet or the Web browser are the following two commands:

- **no telnet-server:** This CLI command blocks inbound Telnet access.
- **no web-management:** This CLI command prevents use of the web browser interface through http (port 80) server access.

If you choose not to disable Telnet and web browser access, you may want to consider using RADIUS accounting to maintain a record of password-protected access to the switch.

## Secure File Transfers

Secure Copy and SFTP provide a secure alternative to TFTP and auto-TFTP for transferring sensitive information such as configuration files and log information between the switch and other devices.

## SNMP Access (Simple Network Management Protocol)

In the default configuration, the switch is open to access by management stations running SNMP management applications capable of viewing or changing usernames, passwords, configuration, and status data in the switch's MIB (Management Information Base). Thus, controlling SNMP access to the switch and preventing unauthorized SNMP access should be a key element of your network security strategy.

**General SNMP Access to the Switch.** The switch supports SNMP versions 1, 2c, and 3, including SNMP community and trap configuration. The default configuration supports versions 1 and 2c compatibility, which uses plain text and does not provide security options. ProCurve recommends that you enable SNMP version 3 for improved security. SNMPv3 includes the ability to configure restricted access and to block all non-version 3 messages (which blocks version 1 and 2c unprotected operation). SNMPv3 security options include:

- configuring device communities as a means for excluding management access by unauthorized stations
- configuring for access authentication and privacy
- reporting events to the switch CLI and to SNMP trap receivers
- restricting non-SNMPv3 agents to either read-only access or no access
- co-existing with SNMPv1 and v2c if necessary

### **SNMP Access to the Switch's Local Username and Password Authentication MIB Objects.**

A management station running an SNMP networked device management application such as ProCurve Manager Plus (PCM+) or HP OpenView can access the switch's management information base (MIB) for write access to the switch's local username and password configuration. In earlier software versions, SNMP access to the switch's local authentication configuration (hpSwitchAuth) MIB objects was not allowed. However, beginning with software release U.11.04, the switch's default configuration allows SNMP access to the local username and password MIB objects in hpSwitchAuth. If SNMP access to these MIB objects is considered a security risk in your network, then you should implement the following security precautions when downloading and booting from software release U.11.04 or greater:

1. If SNMP write access to the switch's local username and password authentication configuration (hpSwitchAuth) MIB (described above is not desirable for your network, then immediately after downloading and booting from the U.11.04 or greater software for the first time, use the following CLI command to disable this feature:

**snmp-server mib hpswitchauthmib excluded**

---

## **Note on SNMP Access to Local Authentication MIB Objects**

Downloading and booting U.11.04 or later software versions for the first time enables SNMP access to the switch's local authentication configuration MIB objects (the default action). If SNMPv3 and other security safeguards are not in place, the local username and password MIB objects are exposed to unprotected SNMP access and you should use the preceding command to disable this access.

---

2. If you choose to leave the local authentication configuration MIB objects accessible, then you should do the following to help ensure that unauthorized workstations cannot use SNMP tools to change the settings:
  - Configure SNMP version 3 management and access security on the switch.
  - Disable SNMP version 2c on the switch.

## **Front-Panel Access and Physical Security**

Physical access to the switch allows the following:

- use of the console serial port (CLI and Menu interface) for viewing and changing the current configuration and for reading status, statistics, and log messages.
- use of the switch's Clear and Reset buttons for these actions:
  - clearing (removing) local password protection
  - rebooting the switch
  - restoring the switch to the factory default configuration (and erasing any non-default configuration settings)

Keeping the switch in a locked wiring closet or other secure space helps to prevent unauthorized physical access. As additional precautions, you can do the following:

- Disable or re-enable the password-clearing function of the Clear button.
- Configure the Clear button to reboot the switch after clearing any local usernames and passwords.
- Modify the operation of the Reset+Clear button combination so that the switch reboots, but does not restore the switch's factory default settings.
- Disable or re-enable password recovery.

## Other Provisions for Management Access Security

**Authorized IP Managers.** This feature uses IP addresses and masks to determine whether to allow management access to the switch through the network, and covers access through the following:

- Telnet and other terminal emulation applications
- The switch's Web browser interface
- SNMP (with a correct community name)

**Secure Management VLAN.** This feature creates an isolated network for managing the ProCurve switches that offer this feature. When a secure management VLAN is enabled, CLI, Menu interface, and web browser interface access is restricted to ports configured as members of the VLAN.

## Network Security Features

This section outlines provisions for protecting access through the switch to the network. For more detailed information on these features, refer to the indicated manuals.

### Web and MAC Authentication

These options are designed for application on the edge of a network to provide port-based security measures for protecting private networks and the switch itself from unauthorized access. Because neither method requires clients to run any special supplicant software, both are suitable for legacy systems and temporary access situations where introducing supplicant software is not an attractive option. Both methods rely on using a RADIUS server for authentication. This simplifies access security management by allowing you to control access from a master database in a single server. It also means the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN. Web authentication uses a web page login to authenticate users for access to the network. MAC authentication grants access to a secure network by authenticating device MAC address for access to the network.

### Secure Shell (SSH)

SSH provides Telnet-like functions through encrypted, authenticated transactions of the following types:

- **client public-key authentication:** uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a stored public key can gain access to the switch.

- **switch SSH and user password authentication:** this option is a subset of the client public-key authentication, and is used if the switch has SSH enabled without a login access configured to authenticate the client's key. In this case, the switch authenticates itself to clients, and users on SSH clients then authenticate themselves to the switch by providing passwords stored on a RADIUS or TACACS+ server, or locally on the switch.
- **secure copy (SC) and secure FTP (SFTP):** By opening a secure, encrypted SSH session, you can take advantage of SC and SFTP to provide a secure alternative to TFTP for transferring sensitive switch information.

### Secure Socket Layer (SSLv3/TLSv1)

This feature includes use of Transport Layer Security (TLSv1) to provide remote web access to the switch via authenticated transactions and encrypted paths between the switch and management station clients capable of SSL/TLS operation. The authenticated type includes server certificate authentication with user password authentication.

# Enhancements

---

Unless otherwise noted, each new release includes the features added in all previous releases. Enhancements are listed in chronological order, oldest to newest software release.

---

## Release U.11.04 Enhancements

*No new enhancements. Initial Release.*

## Release U.11.08 Enhancements

*Software fixes only; no new enhancements.*

## Release U.11.09 Enhancements

*Software fixes only; no new enhancements. (Never released.)*

## Release U.11.10 Enhancements

The following enhancement is included in the U.11.10 release.

- **Enhancement (PR\_0000010783)** — Support is added for the following products.

J9099B - ProCurve 100-BX-D SFP-LC Transceiver

J9100B - ProCurve 100-BX-U SFP-LC Transceiver

J9142B - ProCurve 1000-BX-D SFP-LC Mini-GBIC

J9143B - ProCurve 1000-BX-U SFP-LC Mini-GBIC

## Release U.11.11 Enhancements

*Software fixes only; no new enhancements.*

# Software Fixes

---

Software fixes are listed in chronological order, oldest to newest.

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

Release U.11.04 was the first software release for the ProCurve Series 2610 Series Switches.

---

## Release U.11.04

No Problems Reserved in Release U.11.04. Initial Release.

## Release U.11.08

The following problems were resolved in release U.11.08.

- **DST (PR\_1000467724)** — The DST change-over dates are incorrect for the Western-European time zone.
- **CLI (PR\_1000455370)** — Some commands may incorrectly display single ports as a range.
- **Config (PR\_1000464345)** — Certain characters present in port names may cause configuration corruption upon startup.
- **Config (PR\_1000757101)** — The configuration containing *ip arp-age* cannot be copied to the switch using TFTP.
- **LLDP (PR\_1000759396)** — LLDP packets are dropped and the switch does not learn adjacent devices.
- **100-FX (PR\_1000764546)** — The 100-FX transceiver (J9054B) is not recognized.

## Release U.11.09

The following problems were resolved in release U.11.09 (Never released).

- **Crash (PR\_1000768231)** — The switch may reboot unexpectedly when the administrator is removing a VLAN.
- **Web GUI (PR\_1000760153)** — A Java Error occurs when viewing the “Stack Closeup” page, causing a blank page to be displayed.

- **Authentication (PR\_1000454714)** — Concurrent 802.1X and MAC-authentication does not give the 802.1X value precedence. This fix gives 802.1X VLAN assignment precedence over MAC-authentication RADIUS VLAN assignment.
- **CLI (PR\_1000779621)** — If **show flash** is executed while the flash is being written, the file size is displayed. This corrects the behavior so that **show flash** shows a "0" until the writing has completed in order to avoid providing an indication that the download process has completed when it has not.
- **CLI (PR\_1000430534)** — CLI output from the show **port-access mac-based** command does not show the correct clients connected; some are omitted.
- **System Up-time (PR\_1000772402)** — The system up-time rolls back to zero after 49 days.
- **Config (PR\_1000790501)** — When any supported transceiver is present in a mini-GBIC port, the configuration (including port-VLAN assignment) is not maintained across a reboot.
- **Radius Authentication (PR\_1000779048)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. This allows the RADIUS server to reply with a large fragment which the switch does not process, causing the authentication process to fail. Workaround: set the Framed-MTU on the RADIUS server.
- **Crash (PR\_1000795039)** — The switch may crash while uploading the configuration file, if there are extra space(s) in the configuration file header. The message is similar to:

```
TLB Miss: Virtual Addr=0x00000000 IP=0x804cfd80 Task='mftTask' Task
ID=0x83357880 fp:0x83357678 sp:0x83357608 ra:0x804cfe10
sr:0x1000fc01
```

- **VLAN (PR\_000002103)** — The alteration of the VLAN/MSTP instance mapping in the pending configuration is not functioning properly. The attempt to remove any single VLAN ID (VID) from one MSTP instance and assign it to another MSTP instance fails, though specifying a VID range succeeds.
- **Crash (PR\_000002579)** — Attempting to manage the switch with the browser web management interface, may cause the switch to crash with a message similar to:

```
TLB Miss: Virtual Addr=0x00263f14 IP=0x00263f14 Task='tHttpd' Task
ID=0x85d76e70 fp:0x00000000 sp:0x85d76d30 ra:0x00263f14
sr:0x1000fc01
```

- **Configuration (PR\_1000786770)** — The switch may not reload as it should following an update of the configuration file via SCP. Sometimes, portions of the copied config are written to the running config. Event logs may show messages similar to the following.

```
01/01/90 20:49:34 ssh: scp session from 13.28.234.50
W 01/01/90 20:49:35 ssh: scp error: protocol error: unexpected <newline>
```

- **SSH (PR\_0000003592)** — Repeatedly performing crypto key generation tasks, and then connecting to the switch via SSH and executing a **show ip ssh** command may trigger a switch crash with a message similar to the following.

```
TLB Miss: Virtual Addr=0x10385720 IP=0x10385720 Task='mSnmpCtrl'  
Task ID=0x85cc0150 fp:0x85b93e60 sp:0x85cbff80 ra:0x10385720  
sr:0x1000fc01
```

- **Crash (PR\_0000003933)** — When the user attempts RADIUS authentication to the Web Management Interface, the switch may crash with a message similar to the following.

```
TLB Miss: Virtual Addr=0x0024c904 IP=0x0024c904 Task='tHttpd'  
Task ID=0x81e46eb0 fp:0x00000000 sp:0x81e46d70 ra:0x0024c904
```

- **GVRP/RADIUS (PR\_0000006051)** — RADIUS assigned VLANs are not propagated correctly in GVRP.

*Note:* This fix is associated with some new switch behavior: When only one port has learned of a dynamic VLAN, it will advertise that VLAN if an auth port has been RADIUS-assigned that dynamic VLAN, regardless of the unknown-VLANs configuration of that port. The fix accommodates RADIUS-assigned (and hpicfUsrProf MIB-assigned) tagged VLANs as well as untagged VLANs. These changes are enabled by default and are not configurable. This fix does not modify any other GVRP behavior.

- **TACACS+ (PR\_0000003839)** — The TACACS server configuration parameter accepts an address from an invalid/reserved IP range: 0.0.0.1 to 0.255.255.255.
- **802.1X (PR\_0000005358)** — The switch is unable to successfully authenticate users using 802.1X.
- **CLI (PR\_0000002815/1000406763)** — Output from the **show tech** CLI command was modified.
- **PC phone/authentication (PR\_0000008777)** — When using an IP phone in tandem with a PC connected to the phone, the phone will sometimes come up using untagged packets until acquiring its tagged VLAN and priority information. In this case the IP phones untagged MAC address will block the PC communicating to the port until the phone's MAC address expires (default 5 minutes).
- **802.1X (PR\_0000008780)** — 802.1X does not receive expiration notifications from port security if 802.1X is running alone, without WMA.
- **PC Phone/Authentication (PR\_0000007209)** — When an IP phone is used in tandem with a PC connected to the phone, if the phone is moved to a tagged VLAN, some phone manufactures send some traffic to the switch untagged. This may result in traffic disruption including the PC not being allowed to authenticate.
- **PC Phone/Authentication (PR\_0000009825)** — An IP phone connected in tandem with a PC, did not allow the PC user to be in an unauthenticated VLAN or authenticated using 802.1X, Web auth, or MAC authentication.
- **PC Phone/Authentication (PR\_0000010104)** — When using an IP phone in tandem with a PC, sometimes the VLAN assignment after authentication of the PC is delayed.

## Software Fixes

### Release U.11.10

- **802.1X (PR\_0000010275)** — For a port that is being authenticated via 802.1X, the user fails authentication if the **unauth vid** value is configured.
- **MDI-X (PR\_0000007246)** — MDI-X is not working properly; when MDI and MDI-X settings are explicitly configured, the port function is reversed.
- **CLI (PR\_0000010942)** — The CLI command output for **show run** does not display **aaa portaccess <port#>** when MAC-based authentication with mixed port access mode is configured. Other **show** commands may be affected as well.
- **CLI (PR\_0000010378)** — Session time (sec.) remains at zero in response to the CLI command **sh port-access authenticator <port> session-counters**; it should increment.
- **Crash (PR\_0000010107)** — When the switch is configured with SNMPv3 the switch crashes when a network management server communicates with it using SNMPv3. The crash message will be similar to the following.

```
TLBMiss:VirtualAddr=0x00000000 IP=0x800ab0f8 Task= 'mSnmpCtrl '  
Task ID=0x85d26d00 fp:0x00000000 sp:0x85d26a60 ra:0x800aad8  
sr:0x1000fc01
```
- **Selftest Failure (PR\_0000011448)** — The switch may experience intermittent or consistent power on self test (POST) failure with an `initialization halted` message at the console. Workaround: Power off the switch for a few minutes, then power it back on and update the software.
- **MAC Address (PR\_0000009750)** — If a client moves from one port or switch to another, the MAC address is not relearned on the new port until the MAC address timer expires on the original port.
- **LED/POST (PR\_0000006148)** — The switch may not light the self test LEDs in a consistent, predictable sequence during POST.

## Release U.11.10

The following problems were resolved in release U.11.10.

- **QoS (PR\_0000004576)** — Editing a configured QoS TCP-port to a new priority does not take effect until the switch is rebooted.

- **Enhancement (PR\_0000010783)** — Support is added for the following products.
  - J9099B - ProCurve 100-BX-D SFP-LC Transceiver
  - J9100B - ProCurve 100-BX-U SFP-LC Transceiver
  - J9142B - ProCurve 1000-BX-D SFP-LC Mini-GBIC
  - J9143B - ProCurve 1000-BX-U SFP-LC Mini-GBICFor more information, see [“Release U.11.10 Enhancements” on page 14](#).
- **Loop Protect (PR\_0000010897)** — The loop detection feature may not function properly on ports configured for MAC-Authentication.

## Release U.11.11

The following problems were resolved in release U.11.11.

- **CLI Help (PR\_0000010484)** — The CLI tab completion for the command parameter **[ethernet] PORT-LIST** should list the **all** option, but it does not.
- **802.1X (PR\_0000010850)** — If an **unauth-vid** is configured, and the client limit is reached on a switch port, a properly credentialed re-authentication following an improperly credentialed authentication attempt (for example, incorrect password) will leave the 802.1x client in the unauthorized VLAN instead of applying the appropriate authorized VLAN.
- **Config (PR\_0000002077)** — Presence of the valid CLI/configuration parameter **spanning-tree trap errant-bpdu** will trigger failure to upload a configuration, with the switch reporting an error similar to the following (in this example, the problem parameter was on line 16 of the configuration).

```
line: 16. trap: Error setting configuration.  
Corrupted download file.
```
- **Management (PR\_0000012818)** — The switch management interface may become unresponsive as a result of packet buffer depletion.
- **Port Communication (PR\_0000015750)** — A port may become unresponsive, resulting in the device connected to that port being unable to communicate on the network. Moving the client to another port restores the client communication, but only a reload of the switch restores communication on the affected port. This issue may be associated with any of the following symptoms in the affected ports.
  - Toggling (offline/online/offline)
  - Port may remain linked but Rx counters stop incrementing
  - Port may remain linked and receives small packets (errors may increment)
  - Physical layer errors may increment on a port (e.g. CRC errors, collisions, runts, giants)



© 2001, 2008-2009 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

January 2009  
Part Number 5992-3090