

Release Notes:

Version Y.11.12 Software

for the ProCurve 2510G-24 and 2510G-48 Switches

Releases Y.11.01 through Y.11.12 supports these switches:

- ProCurve Switch 2510G-24 (J9279A)
- ProCurve Switch 2510G-48 (J9280A)

These release notes include information on the following:

- Downloading Switch Documentation and Software from the Web ([page 1](#))
- Enforcing Switch Security ([page 8](#))
- Known Issues ([page 14](#))
- Software enhancements available in releases Y.11.01 through Y.11.12 ([page 15](#))
- A listing of software fixes included in releases Y.11.01 through Y.11.12 ([page 18](#))

© Copyright 2008-09
Hewlett-Packard Development Company, LP.
The information contained herein is subject to change
without notice.

Publication Number

Part Number 5992-3098
September 2009

Applicable Product

ProCurve Switch 2510G-24 (J9279A)
ProCurve Switch 2510G-48 (J9280A)

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

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

Known Issues

Release Y.11.01	14
Release Y.11.03	14
Release Y.11.12	14

Enhancements

Release Y.11.01 Enhancements	15
Release Y.11.02 Enhancements	15
Release Y.11.03 Enhancements	15
Release Y.11.04 through Y.11.06 Enhancements	15
Release Y.11.07 through Y.11.08 Enhancements	15
Release Y.11.09 Enhancements	15
Release Y.11.10 Enhancements	16
Release Y.11.11 Enhancements	16
Banner Enhancements	16
Console/Telnet Inactivity Timer	17
Release Y.11.12 Enhancements	17

Software Fixes in Releases Y.11.01 - Y.11.12

Release Y.11.01	18
Release Y.11.02	18
Release Y.11.03	18
Release Y.11.04 through Y.11.06	18
Release Y.11.07	19
Release Y.11.08	19
Release Y.11.09	19
Release Y.11.10	20
Release Y.11.11	21
Release Y.11.12	21

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

Downloading Software to the Switch

Caution

The startup-config file generated by the latest software release may not be backward-compatible with the same file generated by earlier software releases.

HP periodically provides switch software updates through the ProCurve Networking Web site (<http://www.procurve.com>). After you acquire the new software file, you can use one of the following methods for downloading 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 Y_11_01.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 Y_11_01.swi
The primary OS image will be deleted. continue [y/n]? Y
03173K
```

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. Reload 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

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, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G), Switch 8200zl Series (8206zl and 8212zl) and Switch 6600 Series (6600-24G, 6600-24G-4XG, 6600-24XG).
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)
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
R	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
T	Switch 2900 Series (2900-24G and 2900-48G)
U	Switch 2510-48
W	Switch 2910al Series (2910al-24G, 2910al-24G-PoE+, 2910al-48G, and 2910al-48G-PoE+)
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
WA	ProCurve Access Point 530
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
WT	ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module
Y	Switch 2510G Series (2510G-24 and 2510G-48)

Software Letter	ProCurve Networking Products
<i>numeric</i>	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

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, SP2 and 7.0	Sun Java 2 Runtime Environment: – Version 1.5.0_11, Version 1.6.0
Windows Server SE 2003 SP2		
Windows Vista		

Minimum Software Versions

For the ProCurve 2510G-24 and 2510G-48 Switches and Hardware Features

ProCurve Device	Minimum Supported Software Version
ProCurve 100-BX-D SFP-LC Transceiver (J9099B)	Y.11.03
ProCurve 100-BX-U SFP-LC Transceiver (J9100B)	Y.11.03
ProCurve 1000-BX-D SFP-LC Mini-GBIC (J9142B)	Y.11.03
ProCurve 1000-BX-U SFP-LC Mini-GBIC (J9143B)	Y.11.03

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.

Known Issues

Release Y.11.01

The following problems are known issues in release Y.11.01.

- **RADIUS/Web Management (PR_1000811781)** — 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 sr:0x1000fc01
```

Release Y.11.03

The following problems are known issues in release Y.11.03.

- **Menu (PR_0000003963)** — In the TELNET menu interface, under Switch Configuration - > Port/Trunk Settings, the BX transceivers may be displayed as 100GEN or 1000GEN in the Type column, rather than 100BX-U, 100BX-D, 1000BX-U, or 1000BX-D.
- **BX Mini-GBIC/Transceiver (PR_0000010525)** — A 100BX transceiver or 1000BX mini-GBIC may fail self test under certain circumstances, such as insertion of an SFP in both port 49 and port 50 at exactly the same time. Workaround: re-insertion of the SFP device should allow proper initialization and function.

Release Y.11.12

The following problem is a known issue in release Y.11.12.

- **Crash (PR_0000041599)** — The presence of **snmp-server** CLI commands in an uploaded configuration file may cause the switch to reboot unexpectedly with one of the following crash messages.

```
'TLB Miss: Virtual Addr=0x00000000 IP=0x80618fc0 Task= 'mftTask'  
  
PPC Bus Error exception vector 0x300: Stack-frame=0x0124cc40  
HW Addr=0x025aalcc IP=0x00538808 Task='mftTask' Task ID=0x124dcb0  
fp: 0x012d5c30 sp:0x0124cd00 lr:0
```

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 Y.11.01 Enhancements

No new enhancements. Initial Release.

Release Y.11.02 Enhancements

No new enhancements. Never Released.

Release Y.11.03 Enhancements

Release Y.11.03 includes the following enhancements:

- **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 Y.11.04 through Y.11.06 Enhancements

No new enhancements. Never Released.

Release Y.11.07 through Y.11.08 Enhancements

No new enhancements.

Release Y.11.09 Enhancements

No new enhancements. Not a public release.

Release Y.11.10 Enhancements

No new enhancements. Not a public release.

Release Y.11.11 Enhancements

Release Y.11.11 includes the following enhancements. Not a public release.

- **Enhancement (PR_0000016739)** — Banner Size Increase to 1280 characters.
- **Enhancement (PR_0000018513)** — Banner enhancements were made, including the removal of "press any key to continue" when a password has been configured and removal of HP disclaimer containing the switch model and firmware version.

Banner Enhancements

The enhancements to the Message of The Day (MOTD) banner apply to the following authentication types:

- Local
- RADIUS
- TACACS

The enhancements are:

- The MOTD banner size is increased to 1280 characters.
- If the MOTD is configured, the copyright, switch identification, and software version are not displayed on the splash screen; only the customer-defined banner is displayed.
- When passwords are configured on the switch, there will not be a prompt to "press any key to continue". This prompt will still appear if a password is not configured.

Example Banner Configurations

Default Banner with No Password Configured. When the MOTD is not configured and there is no password, the default login page displays. The information includes the switch identification, software version, copyright statement and default banner. The "press any key to continue" prompt displays. When any key is pressed, the banner is cleared and the CLI prompt displays.

Default Banner with Password Configured. When passwords are configured on the switch, but the MOTD is not configured, the default login page displays. A prompt for the password appears. After a correct password is entered, the default banner clears and the CLI prompt displays.

Customized Banner without Password Configured. When a custom MOTD banner is configured and there is no password required, the custom MOTD banner displays followed by the “press any key to continue” prompt. When any key is pressed, the custom banner is cleared and the CLI prompt displays.

Customized Banner with Password Configuration. When a custom MOTD banner is configured on the switch and a password is required, the custom banner displays, followed by the password prompt. Entering the correct password clears the banner and displays the CLI prompt.

- **Enhancement (PR_0000001641)** — Set Console Inactivity Time Out without Reboot

Console/Telnet Inactivity Timer

This enhancement allows you to configure the inactivity timer and have the new value take effect immediately, without a reboot of the system.

Syntax: console inactivity-timer <minutes>

If the console port has no activity for the number of minutes configured, the switch terminates the session. A value of zero indicates the inactivity timer is disabled.

Default: 0 (zero)

For example:

```
ProCurve(config)# console inactivity-timer 20
```

Release Y.11.12 Enhancements

No new enhancements.

Software Fixes in Releases Y.11.01 - Y.11.12

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 Y.11.01 was the first software release for the ProCurve 2510G-24 and 2510G-48 switches.

Release Y.11.01

No Problems Resolved in Release Y.11.01. (Initial Release.)

Release Y.11.02

No Problems Resolved in Release Y.11.02. (Never Released.)

Release Y.11.03

The following problems were resolved in build Y.11.03.

- **Crash (PR_0000002579)** — Attempting to manage the switch using the Web Management Interface may cause the switch to crash with a message similar to the following.

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

- **Crash (PR_1000811781)** — When the user attempts RADIUS authentication to access 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  
sr:0x1000fc01
```

- **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 Y.11.04 through Y.11.06

No Problems Resolved in Releases Y.11.04 through Y.11.06. (Never Built.)

Release Y.11.07

No Problems Resolved in Release Y.11.07. (Not a Production Build.)

Release Y.11.08

The following problems were resolved in build Y.11.08.

- **MAC Address (PR_000009750)** — 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.
- **STP (PR_000009592)** — Spanning Tree BPDUs are not processed when all VLANs on a given port are tagged. This may result in multiple root bridges and a Layer 2 loop when redundant physical paths exist.
- **Transceivers (PR_000010525)** — Intermittent self test failure may occur if transceivers are hot-swapped in and out of the switch in too short a time frame. Note that even with this fix, transceivers should always be allowed to initialize fully prior to removal and subsequent re-insertion.

Best Practice Tip: Upon hot insertion of a transceiver, the mode LED will come on for two seconds. Once this LED has extinguished, it is once again safe to remove the transceiver.

Release Y.11.09

The following problems were resolved in build Y.11.09. Not a public release.

- **Config (PR_000002077)** — 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.
```
- **Loop Protect (PR_000010897)** — The loop detection feature may not function properly on ports configured with any combination of MAC-Authentication, spanning-tree, and bpdu-protection.
- **Management (PR_000005902)** — The switch management may become unresponsive, resulting in loss of Telnet, Web Management, and console access functionality of the switch.
- **SNMP (PR_000002764)** — The SNMP MIB object that allows authenticator functionality on a port to be enabled or disabled (hpicfDot1xPaePortAuth) can be set to an invalid value.

Software Fixes in Releases Y.11.01 - Y.11.12

Release Y.11.10

- **802.1X (PR_0000012568)** — There is a problem with the switch login error message.
- **Management (PR_0000012818)** — The switch management interface may become unresponsive as a result of packet buffer depletion.
- **Config (PR_0000007953)** — The config line **spanning-tree instance <n> vlan <vid>** is truncated in some cases, causing loss of configuration after reload of the config file.
- **BPDU-Protection (PR_0000012541)** — The presence of a trunk group in a switch with STP BPDU-protection configured may trigger the switch to block the wrong port when a BPDU is received.
- **Controlled Direction (PR_0000009818)** — The switch does not properly enable or edit the controlled direction parameter (in the config line **aaa port-access controlled-direction <inloutboth>**) in the configuration.
- **CLI (PR_0000010942)** — The CLI command output for **show run** does not display **aaa port-access <port#>** when MAC-based authentication with mixed port access mode is configured. Other **show** commands may also be affected.
- **SNMP (PR_0000002409)** — Several supported OIDs return 'No such variable' in response to the CLI command **walkmib <OID>**. Affected OIDs include the following.

```
1.3.6.1.4.1.11.2.14.11.5.1.32 (hpSwitchAutzServicePrimaryMethod)
1.3.6.1.4.1.11.2.14.5.1.35 (hpicfInstMonTrapEnable)
```
- **VLAN (PR_0000013388)** — A switch with trunks not configured for VLAN <x> still accepts tagged frames for VLAN <x> and forwards them to other ports configured for VLAN <x>.
- **802.1X (PR_0000008780)** — 802.1X does not receive expiration notifications from port security if 802.1X is running alone (without Web or MAC Authentication).
- **802.1X (PR_0000015662/0000011718)** — When AAA Authentication with 802.1X using PEAP is configured, the port status does not change appropriately to 802.1X, leading to client 802.1X authentication failure.

Release Y.11.10

The following problems were resolved in build Y.11.10. Not a public release.

- **RADIUS Accounting (PR_0000017732)** — RADIUS accounting is incrementing the wrong counter in response to a dropped (invalid) packet from the RADIUS server.
- **MAC Authentication (PR_0000015520)** — Traffic from unauthenticated clients may be allowed during the process of authenticating clients under heavy loads.

- **Authentication (PR_0000013472)** — Port-access authentication may not occur when there is a combination of tagged and untagged port membership in the same VLAN (as the auth-vid, unauth-vid, or a RADIUS-assigned VLAN). This fix prevents untagged VLAN assignment to be applied to a port if that port is a tagged member of the same VLAN. *Best Practice Tip:* Configure different VLANs for the **auth-vid** and **unauth-vid** roles.
- **MSTP (PR_0000011865)** — The spanning-tree port priority reported by the CLI command **show span instance <x>** incorrectly reports 0 for the priority instead of 128 (the default/mean value). If a valid port priority value is manually configured, the switch properly reports the assigned value.
- **Xmodem (PR_0000038807)** — Transfer of a configuration file to the switch via Xmodem fails after 384 bytes when the console inactivity timer is configured. When this occurs, the switch reports an error, `Ambiguous input:snm`
- **Config (PR_0000017930)** — Preconfiguration of an SFP port followed by a save of the configuration, power down of the switch, insertion of a mini-GBIC, and then power up the switch causes the port configuration to return to default values.
- **Config (PR_0000010713)** — The configuration line **aaa port-access web-based dhcp-addr <IP address> <subnet mask>** cannot be removed via the CLI.

Release Y.11.11

The following problems were resolved in build Y.11.11. Not a public release.

- **Enhancement (PR_0000016739)** — Banner Size Increase to 1280 characters. For more information, please see [“Banner Enhancements” on page 16](#).
- **Enhancement (PR_0000018513)** — Banner enhancements were made, including the removal of "press any key to continue" when a password has been configured and removal of HP disclaimer containing the switch model and firmware version. For more information, please see [“Banner Enhancements” on page 16](#).
- **Enhancement (PR_0000001641)** — Set Console Inactivity Time Out without Reboot. For more information, please see [“Console/Telnet Inactivity Timer” on page 17](#).

Release Y.11.12

The following problems were resolved in build Y.11.12.

- **Unauthenticated VLAN (PR_0000010533)** — The switch allows an inherent configuration conflict; an unauthenticated VLAN (**unauth-vid**) can be configured concurrently for both 802.1X and Web/MAC authentication. This fix will not allow concurrent configuration of an **unauth-vid** for the **aaa port-access authenticator** and **aaa port-access web-based** or **aaa port-**

access mac-based functions. Software versions that contain this fix will not allow this configuration conflict at the CLI. *Existing configurations will be altered by this fix*, and an error will be reported at the switch CLI and event log.

Best Practice Tip: 802.1X should not have an unauthenticated VLAN setting when it works concurrently with Web-based or MAC-based authentication if the unauth-period in 802.1X is zero (the default value). Recall that the unauth-period is the time that 802.1X will wait for authentication completion before the client will be authorized on an unauthenticated VLAN. If 802.1X is associated with an unauthenticated VLAN when the unauth-period is zero, Web- or MAC-auth may not get the opportunity to initiate authentication at all if the first packet from the client is an 802.1X packet. Alternatively, if the first packet sent was not 802.1X, Web- or MAC-auth could be initiated before 802.1X places the user in the unauthenticated VLAN and when Web- or MACauth completes successfully, it will be awaiting traffic (to enable VLAN assignment) from the client but the traffic will be restricted to the unauthenticated VLAN, and thus the client will remain there.

If a MAC- or Web-based configuration on a port is associated with an unauth-VID, and an attempt is made to configure an unauth-VID for 802.1X (port-access authenticator), the switch with this fix will reject the configuration change with a message similar to one of the following.

Message 1 (when an unauth-vid config is attempted on a port with an existing Web- or MAC-auth unauth-vid):

```
Configuration change denied for port <number>. Only Web or
MACauthenticator can have unauthenticated VLAN enabled if 802.1X
authenticator is enabled on the same port. Please disable Web and
MAC authentication on this port using the following commands:
```

```
"no aaa port-access web-based <PORT-LIST>" or
"no aaa port-access mac-based <PORT-LIST>"
```

```
Then you can enable 802.1X authentication with unauthenticated
VLAN. You can re-enable Web and/or MAC authentication after you
remove the unauthenticated VLAN from 802.1X. Note that you can
set unauthenticated VLAN for Web or MAC authentication instead.
```

Message 2 (when an unauth-vid config is attempted on a port with an existing 802.1X unauth-vid):

```
Configuration change denied for port <number>. Only Web or MAC-
authenticator can have unauthenticated VLAN enabled if 802.1X
authenticator is enabled on the same port. Please remove the
unauthenticated VLAN from 802.1X authentication on this port using
the following command:
```

```
"no aaa port-access authenticator <PORT-LIST> unauth-vid"
```

```
Note that you can set unauthenticated VLAN for Web or MAC
authentication instead.
```

Message 3:

Configuration change denied for port <number>. Only Web or MAC-authenticator can have unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port. Please use unauthenticated VLAN for Web or MAC authentication instead.

Event log message when the configuration is changed:

mgr: Disabled unauthenticated VLAN on port <number> for the 802.1X. Unauthenticated VLAN cannot be simultaneously enabled on both 802.1X and Web or MAC authentication.

- **Crash (PR_0000039959)** — When a port is configured for limited-continuous learn mode (**port-security <port number> learn-mode limited-continuous**), MAC-address timeouts followed by port-access activity may cause the switch to reboot unexpectedly with a message similar to one of the following.

```
Software exception at exception.c:373 -- in 'm8021xCtrl', task ID =
0x17ff538
-> Memory system error at 0x16c9370 - memPartFree

NMI event SW:IP=0x005906a8 MSR:0x0000b032 LR:0x00350144
Task='m8021xCtrl' Task D=0x17fb968
cr: 0x48000042 sp:0x017fb270 xer:0x20000000

PPC Bus Error exception vector 0x300:
Stack-frame=0x017f6350 HW Addr=0x6d6d3434 IP=0x0059069c
Task='m8021xCtrl' Task ID=0x17f6698
fp: 0x017f6410 sp:0x017f6410 l
```

- **CLI (PR_000008217)** — The **copy flash** CLI command does not allow the user to specify a source OS location (primary/secondary).
- **802.1X (PR_0000041041)** — The switch may reach a point at which it will no longer be able to authenticate 802.1X clients until it is reloaded. The speed at which this occurs is dependent on the rate of 802.1X connection attempts.
- **Crash (PR_0000015095)** — The switch may reboot unexpectedly when it receives a certain type of traffic. A message similar to the following may be present in the switch event and crash logs.

```
Unaligned Access: Virtual Addr=0xa7fb7aa3 IP=0x803628ac
Task='eDrvPoll'
```

- **Xmodem (PR_000008697)** — Xmodem file transfers require in excess of an hour, even at the highest supported baud rate.

- **Config (PR_0000039026)** — The switch reloads into a configuration that is copied to the startup configuration, even if the downloaded config is identical to the one the switch has stored. This fix will remove the need to reload in that case, and return a message at the CLI: `Downloaded file identical to current, no update performed.`
- **Authentication (PR_0000011138)** — If the Radius server becomes unavailable, the **eap-radius authorized** option allows the switch to authenticate devices. If the response time of the RADIUS subsystem is greater than the server-timeout value on the switch or the device supplicant then the switch will not be able to authenticate devices, and no warning of this failure will be displayed. This fix triggers the display of the following CLI message.

```
The RADIUS connection timeout must be less than the authentication
server timeout for the switch to authenticate automatically when the
RADIUS server is unavailable.
```

- **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.



© 2008-09 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

Part Number 5992-3098
September 2009