

Release Notes: Version W.14.26 Software

for the HP ProCurve Series 2910al Switches

These release notes include information on the following:

- W.14.03 is supported on the following switches:
 - HP ProCurve 2910al-24G Switch (J9145A)
 - HP ProCurve 2910al-24G-PoE+ Switch (J9146A)
 - HP ProCurve 2910al-48G Switch (J9147A)
 - HP ProCurve 2910al-48G-PoE+ Switch (J9148A)
- Download switch software and documentation from the Web ([page 1](#))
- Support notes and known issues in releases W.14.03 through W.14.26 ([page 8](#))
- A listing of software enhancements in recent releases ([page 9](#))
- A listing of software fixes included in releases W.14.03 through W.14.26 ([page 18](#))

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

Publication Number

5900-0244

May, 2009

Applicable Product

HP ProCurve 2910al-24G Switch (J9145A)

HP ProCurve 2910al-24G-PoE+ Switch (J9146A)

HP ProCurve 2910al-48G Switch (J9147A)

HP ProCurve 2910al-48G-PoE+ Switch (J9148A)

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
Software Updates	1
Download Switch Documentation and Software from the Web	1
View or Download the Software Manual Set	1
Downloading Software to the Switch	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
ProCurve Switch, Routing Switch, and Router Software Keys	6
Minimum Software Versions for Series 2910al Switch Features	7
OS/Web/Java Compatibility Table	7
Known Issues	8
Release W.14.03	8
Enhancements	9
Release W.14.03 Enhancements	9
Release W.14.04 through W.14.07 Enhancements	9
Release W.14.08 through W.14.10 Enhancements	9
Release W.14.11 through W.14.13 Enhancements	9
Release W.14.14 Enhancements	9
Release W.14.15 Enhancements	9
SNTP-Client Authentication	9
Release W.14.16 Enhancements	17
Release W.14.17 through W.14.25 Enhancements	17
Release W.14.26 Enhancements	17
Software Fixes	18
Release W.14.03	18
Release W.14.04 through W.14.07	18

Release W.14.08 through W.14.10	18
Release W.14.11 through W.14.13	18
Release W.14.14	18
Release W.14.15	18
Release W.14.16	20
Release W.14.17 through W.14.25	20
Release W.14.26	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.

Download 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.

View or Download the Software Manual Set

Go to: www.procurve.com/manuals

You may want to bookmark this Web page for easy access in the future.

You can also register on the My ProCurve portal to receive a set of ProCurve switch manuals on CD-ROM. To register and request a CD, go to www.procurve.com and click on **My ProCurve Sign In**. After registering and entering the portal, click on **My Manuals**.

Downloading Software to the Switch

ProCurve Networking 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 it to the switch:

- For a TFTP transfer from a server, do either of the following:
 - Select **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:
 - Select **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).
- Use the USB port to download a software file from a USB flash drive.
- Use the download utility in ProCurve Manager Plus.

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. For more information, refer to the *Management and Configuration Guide* for your switch.

Downloading Software to the Switch

ProCurve Networking 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 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 3).
- Use the download utility in ProCurve Manager Plus.

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. 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 W_14_03x.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 W.14.03x.swi
The primary OS image will be deleted. continue [y/n]? Y
01403W
```

2. 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:

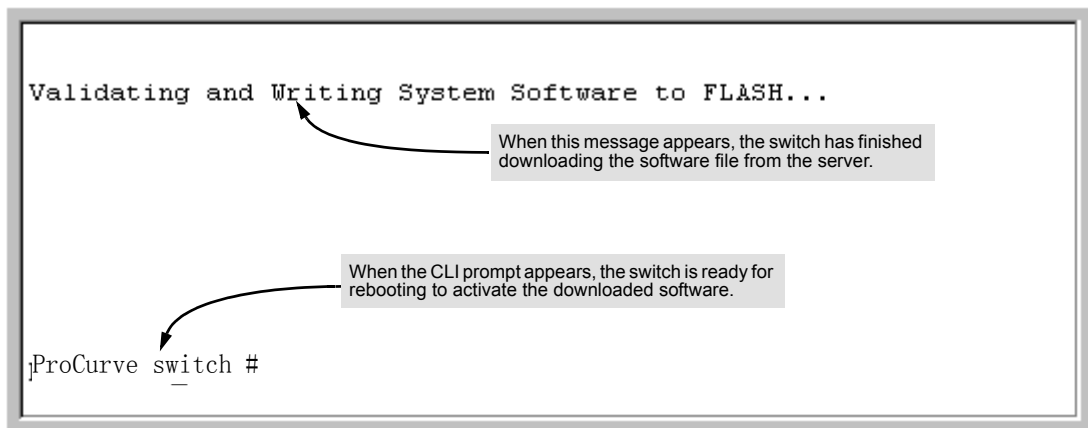


Figure 1. Message Indicating the Switch Is Ready To Activate the Downloaded Software

3. Reboot the switch.

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

Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port to a PC operating as a terminal. (Refer to the Installation and Getting Started Guide you received with the switch for information on connecting a PC as a terminal and running the switch console interface.)
- The switch software is stored on a disk drive in the PC.

- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the HyperTerminal application included with Windows NT, you would use the Send File option in the Transfer dropdown menu.)

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

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

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

```
ProCurve (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 # 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 to the Main Menu, press **[Y]** (for Yes) when you see the “save configuration” prompt:

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

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 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
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 2910al Switch Features

For Software Features. To view a tabular listing of major switch software features and the minimum software version each feature requires:

1. Visit the ProCurve Networking Web site at www.procurve.com.
2. Click on **Software updates**.
3. Click on **Minimum Software Version Required by Feature**.

For Switch 2910al Hardware Accessories.

ProCurve Device	Minimum Supported Software Version
HP ProCurve 2910al-24G Switch (J9145A)	W.14.03
HP ProCurve 2910al-24G-PoE+ Switch (J9146A)	W.14.03
HP ProCurve 2910al-48G Switch (J9147A)	W.14.03
HP ProCurve 2910al-48G-PoE+ Switch (J9148A)	W.14.03

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		

Known Issues

Release W.14.03

The following known issues are open as of Release W.14.03 software.

- **PoE (PR_0000016644)** — If the PoE portion of the power supply fails, the switch may still indicate that it is delivering PoE power to the ports when it is not.
- **Flow Control (PR_0000015824)** — Fiber ports do not notify the link partner of changes to the flow control configuration, resulting in a potential mismatch of flow control settings on each side of the link.
- **Redundant Power (PR_0000015519)** — When the switch is connected to Redundant Power Supply (RPS) only (the only part supported on the 2910al switches), and the power is removed from the HP ProCurve 620 RPS/EPS, power is lost to the PoE ports and is not restored when the HP ProCurve 620 is again powered up. A reload of the switch is required to restore PoE power delivery.
- **PoE (PR_0000014907)** — When a cable delivering 30W of class 4 power is physically disconnected from the switch, an over-current message is displayed. Note that the switch does remove power from the port appropriately, and the over-current counter for the port does not increase when this happens. The event log message is similar to the following.

00562 ports: port <number> PD Over Current indication.

Enhancements

Enhancements are listed in chronological order, oldest to newest software release.

Release W.14.03 Enhancements

No new enhancements; Initial release.

Release W.14.04 through W.14.07 Enhancements

No new enhancements, software never released.

Release W.14.08 through W.14.10 Enhancements

No new enhancements, software never built.

Release W.14.11 through W.14.13 Enhancements

No new enhancements, software never released.

Release W.14.14 Enhancements

No new enhancements, software never built.

Release W.14.15 Enhancements

Release W.14.15 includes the following enhancements.

- **Enhancement (PR_0000010201)** — Support was added for SNTP client authentication.

SNTP-Client Authentication

Overview

Enabling SNTP authentication allows network devices such as HP ProCurve switches to validate the SNTP messages received from an NTP or SNTP server before updating the network time. NTP or SNTP servers and clients must be configured with the same set of authentication keys so that the servers can authenticate the messages they send and clients (HP ProCurve switches) can validate the received messages before updating the time.

This enhancement provides support for SNTP client authentication on HP ProCurve switches, which addresses security considerations when deploying SNTP in a network.

For more information about SNTP operation in general, see the chapter “Time Protocols” in the *Management and Configuration Guide* for your switch.

Requirements

The following must be configured to enable SNTP client authentication on the switch.

SNTP Client Authentication Support

- Timesync mode must be SNTP. Use the **timesync sntp** command. (SNTP is disabled by default.)
- SNTP must be in unicast or broadcast mode.
- The MD5 authentication mode must be selected.
- An SNTP authentication key-identifier (**key-id**) must be configured on the switch and a value (**key-value**) must be provided for the authentication key. A maximum of 8 sets of **key-id** and **key-value** can be configured on the switch.
- Among the keys that have been configured, one key or a set of keys must be configured as trusted. Only trusted keys will be used for SNTP authentication.
- If the SNTP server requires authentication, one of the trusted keys has to be associated with the SNTP server.
- SNTP client authentication must be enabled on the ProCurve switch. If client authentication is disabled, packets are processed without authentication. All of the above steps are necessary to enable authentication on the client.

SNTP Server Authentication Support

Note

SNTP server is not supported on ProCurve products.

The following must be performed on the SNTP server:

- The same authentication key-identifier, trusted key, authentication mode and key-value that were configured on the SNTP client must also be configured on the SNTP server.
- SNTP server authentication must be enabled on the server.

If any of the parameters on the server are changed, the parameters have to be changed on all the SNTP clients in the network as well. The authentication check will fail on the clients otherwise, and the SNTP packets will be dropped.

Configuring the Key-Identifier, Authentication Mode, and Key Value

This command configures the **key-id**, **authentication-mode**, and **key-value**, which are required for authentication. It is executed in the global configuration context.

Syntax: `sntp authentication key-id <key-id> authentication-mode <md5> key-value <key-string> [trusted]`
`no sntp authentication key-id <key-id>`

Configures a key-id, authentication-mode (MD5 only), and key-value, which are required for authentication.

*The **no** version of the command deletes the authentication key.*

Default: No default keys are configured on the switch.

key-id: *A numeric key identifier in the range of 1-4,294,967,295 (2^{32}) that identifies the unique key value. It is sent in the SNTP packet.*

key-value <key-string>: *The secret key that is used to generate the message digest. Up to 32 characters are allowed for <key-string>.*

```
ProCurve(config)# sntp authentication key-id 55 authentication-mode md5 key-  
value secretkey1
```

Figure 1. Example of Setting Parameters for SNTP Authentication

Configuring a Trusted Key

Trusted keys are used in SNTP authentication. In unicast mode, a **trusted** key must be associated with a specific NTP/SNTP server. That key is used for authenticating the SNTP packet.

In unicast mode, a specific server is configured on the switch so that the SNTP client communicates with the specified server to get the date and time.

In broadcast mode, the SNTP client switch checks the size of the received packet to determine if it is authenticated. If the broadcast packet is authenticated, the key-id value is checked to see if the same key-id value is configured on the SNTP client switch. If the switch is configured with the same key-id value and the key-id value is configured as “trusted”, the authentication succeeds. Only trusted key-id value information is used for SNTP authentication.

If the packet contains key-id value information that is not configured on the SNTP client switch or the received packet contains no authentication information, it is discarded. The SNTP client switch expects packets to be authenticated if SNTP authentication is enabled.

When authentication succeeds, the time in the packet is used to update the time on the switch.

Enter the following command to configure a **key-id** as **trusted**.

Syntax: sntp authentication key-id <key-id> trusted
no sntp authentication key-id <key-id> trusted

*Trusted keys are used during the authentication process. The switch can be configured with up to eight sets of key-id/key-value pairs. One specific set must be selected for authentication; this is done by configuring the set as **trusted**.*

*The **key-id** itself must already be configured on the switch. To enable authentication, at least one **key-id** must be configured as **trusted**.*

*The **no** version of the command indicates the key is unreliable (not trusted).*

Default: No key is trusted by default.

Associating a Key with an SNTP Server

After a key is configured, it must be associated with a specific server.

Syntax: [no] sntp server priority <1-3> <ip-address | ipv6-address> <version-num> [key-id <1-4,294,967,295>]

*Configures a **key-id** to be associated with a specific server. The key itself must already be configured on the switch.*

*The **no** version of the command disassociates the key from the server. This does not remove the authentication key.*

Default: No key is associated with any server by default.

priority: *Specifies the order in which the configured servers are polled for getting the time. Value is between 1 and 3.*

<version-num> *Specifies the SNTP software version to use, and is assigned on a per-server basis. The version setting is backwards-compatible. For example, using version 3 means that the switch accepts versions 1 through 3.*

Default: 3; range: 1 - 7.

key-id: *Optional command. The key identifier (range 1-4,294,967,295) sent in the SNTP packet. This **key-id** will be associated with the SNTP server specified in the command.*

```
ProCurve(config)# sntp server priority 1 10.10.19.5 2 key-id 55
```

Figure 2. Example of Associating a Key-Id with a Specific Server

Enabling SNTP Client Authentication

The **sntp authentication** command enables SNTP client authentication on the switch. If SNTP authentication is not enabled, SNTP packets are not authenticated.

Syntax: [no] sntp authentication

Enables the SNTP client authentication

*The **no** version of the command disables authentication.*

Default: SNTP client authentication is disabled by default.

Configuring Unicast and Broadcast Mode

To enable authentication, either unicast or broadcast mode must be configured. When authentication is enabled, changing the mode from unicast to broadcast or vice versa is not allowed. You must disable authentication and then change the mode.

To set the SNTP mode or change from one mode to the other, enter the appropriate command.

Syntax: sntp unicast
sntp broadcast

Enables SNTP for either broadcast or unicast mode.

*Default: SNTP mode is disabled by default. SNTP does not operate even if specified by the CLI **timesync** command or by the menu interface **Time Sync Method** parameter.*

Unicast: *Directs the switch to poll a specific server periodically for SNTP time synchronization. The default value between each polling request is 720 seconds but can be configured. At least one manually configured server IP address is required.*

Note: *At least one **key-id** must be configured as **trusted** and it must be associated with one of the SNTP servers. To edit or remove the associated **key-id** information or SNTP server information. SNTP authentication must be disabled.*

Broadcast: *Directs the switch to acquire its time synchronization from data broadcast by any SNTP server to the network broadcast address. The switch uses the first server detected and ignores any others. However, if the Poll Interval (configurable up to 720 seconds) expires three times without the switch detecting a time update from the original server, the switch accepts a broadcast time update from the next server it detects.*

Displaying SNTP Configuration Information

The **show sntp** command displays SNTP configuration information, including any SNTP authentication keys that have been configured on the switch.

```
ProCurve(config)# show sntp

SNTP Configuration

SNTP Authentication : Enabled
Time Sync Mode: Sntp
SNTP Mode : Unicast
Poll Interval (sec) [720] : 720

Priority SNTP Server Address                Protocol Version KeyId
-----
1         10.10.10.2                        3                 55
2         fe80::200:24ff:fec8:4ca8          3                 55
```

Figure 3. Example of SNTP Configuration Information

To display all the SNTP authentication keys that have been configured on the switch, enter the **show sntp authentication** command.

```
ProCurve(config)# show sntp authentication

SNTP Authentication Information

SNTP Authentication : Enabled

Key-ID  Auth Mode  Trusted
-----
55      MD5        Yes
10      MD5        No
```

Figure 4. Example of show sntp authentication Command Output

To display the statistical information for each SNTP server, enter the **sntp statistics** command. The number of SNTP packets that have failed authentication is displayed for each SNTP server address.

```
ProCurve(config)# show sntp statistics
SNTP Statistics

Received Packets   : 0
Sent Packets       : 3
Dropped Packets    : 0

SNTP Server Address                      Auth Failed Pkts
-----
10.10.10.1                               0
fe80::200:24ff:fec8:4ca8                 0
```

Figure 5. Example of SNTP Authentication Statistical Information

Saving Configuration Files and the Include-Credentials Command

You can use the **include-credentials** command to store security information in the running-config file. This allows you to upload the file to a TFTP server and then later download the file to the ProCurve switches on which you want to use the same settings. For more information about the **include-credentials** command, see “Configuring Username and Password Security” in the *Access Security Guide* for your switch.

The authentication key values are shown in the output of the **show running-config** and **show config** commands only if the **include-credentials** command was executed.

When SNTP authentication is configured and **include-credentials** has not been executed, the SNTP authentication configuration is not saved.

```
ProCurve(config)# show config

Startup configuration:

.
.
.
timesync sntp
sntp broadcast
sntp 50
sntp authentication
sntp server priority 1 10.10.10.2 3 key-id 55
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4 key-id 55
.
.
```

SNTP authentication has been enabled and a key-id of 55 has been created.

Figure 6. Example of Configuration File with SNTP Authentication Information

In Figure 6, the **include-credentials** command has not been executed and is not present in the configuration file. The configuration file is subsequently saved to a TFTP server for later use. The SNTP authentication information is not saved and is not present in the retrieved configuration file, as shown in Figure 7.

```
ProCurve(config)#copy tftp startup-config 10.2.3.44 config1
.
.
.
Switch reboots...

Startup configuration
.
.
.
timesync sntp
sntp broadcast
sntp 50 sntp server priority 1 10.10.10.2 3
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4
.
.
.
```

The **sntp authentication** line and the **key-ids** are not displayed. You must reconfigure SNTP authentication.

Figure 7. Example of a Retrieved Configuration File When Include Credentials is not Configured

If **include-credentials** is configured, the SNTP authentication configuration is saved in the configuration file. When the **show config** command is entered, all of the information that has been configured for SNTP authentication displays, including the key-values.

```
ProCurve(config)# show config

Startup configuration:

.
.
.
include-credentials
timesync sntp
sntp broadcast
sntp 50
sntp authentication
sntp authentication key-id 55 authentication-mode md5 key-value "secretkey1"
trusted
sntp authentication key-id 2 authentication-mode md5 key-value "secretkey2"
sntp server priority 1 10.10.10.2 3 key-id 55
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4 key-id 55
sntp server priority 3 10.10.4.60 3
.
.
.
```

Include-credentials is configured.

All of the SNTP authentication information displays in the configuration file, including the key-values.

Figure 8. Example of Saved SNTP Authentication Information when include-credentials is Configured

Release W.14.16 Enhancements

No new enhancements, software not a public release.

Release W.14.17 through W.14.25 Enhancements

No new enhancements, software never built.

Release W.14.26 Enhancements

No new enhancements, software fixes only.

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 W.14.03 is the first software release for the HP ProCurve 2910al switches.

Release W.14.03

No software fixes; no new enhancements (Initial release).

Release W.14.04 through W.14.07

Versions W.14.08 through W.14.10 were never released.

Release W.14.08 through W.14.10

Versions W.14.08 through W.14.10 were never built.

Release W.14.11 through W.14.13

Versions W.14.11 through W.14.13 were never released.

Release W.14.14

Version W.14.14 was never built.

Release W.14.15

The following problems were resolved in release W.14.15. (Never released.)

- **Enhancement (PR_0000010201)** — Support was added for SNMP client authentication. For more information, see [“Release W.14.15 Enhancements” on page 9](#).
- **PoE (PR_0000016644)** — If the power supply fails, the switch may still indicate that it is delivering PoE power to the ports, when it is not.
- **Crash (PR_0000016665)** — If a transceiver is hot-swapped into the switch during switch initialization, the switch may reboot or restart a bank of ports.
- **sFlow (PR_0000016875)** — Packets sampled by sFlow are being forwarded twice by the switch.

- **Crash (PR_0000017018)** — The switch may reboot unexpectedly in response to an SNMP walk, depending on the specific switch configuration. The crash message may be similar to the following.

```
Software exception at ipamBttfSNetRoutes.c:339 -- in 'mIpAdmUpCt',  
task ID = 0x61d9e00
```

- **Crash (PR_0000017075)** — The switch may reboot unexpectedly after GVRP is disabled from a switch, displaying a message similar to the following.

```
Restricted Memory Exception number: 0xdead0100 HW Addr=0xe59ff094  
IP=0x10569748 Task='mGvrpCtrl'
```

- **Flow Control (PR_0000015824)** — Fiber ports do not notify the link partner of changes to the flow control configuration, resulting in a potential mismatch of flow control settings on each side of the link.

- **Rate-Limiting (PR_0000016255)** — The switch will not accept a Maximum Ingress Bandwidth value of zero.

- **Crash (PR_0000016124)** — The switch may reboot unexpectedly during a continuous SNMP MIB walk while SSH sessions are being created and ended.

- **Crash (PR_0000017015)** — When the switch is loading a configuration with the maximum number of IPv4 and IPv6 addresses and ACLs, the switch may reboot unexpectedly with an NMI event.

- **Crash (PR_0000017277)** — Configuration of a loopback address using a setmib may cause the switch to reboot unexpectedly with a message similar to the following.

```
Software exception at ipamMGhsApi.c:522 - in 'eRouteCtrl', task ID  
= 0xa965dc0
```

- **IPv6 (PR_0000017078)** — A valid IPv4 loopback address is required, at a minimum, for IPv6 addresses to be configured. This fix notifies the user of this caveat during configuration.

- **IGMP (PR_0000009415)** — The switch may intermittently fail to forward a multicast stream.

- **Crash (PR_0000016652)** — Disabling routing from the CLI using the command **no ip routing** may trigger an unexpected reboot (NMI event) on a switch with a large config.

- **Port Communication (PR_0000004568)** — An Intel NIC using the 82566DM chipset may send out-of-spec packets to the switch which results in the loss of communication on that port, regardless of a continuous connection. Symptoms may include one or more of the following behaviors.

- Rx Bytes counter does not increment
- CRC/alignment errors

- Duplex mismatch
- Collisions, runts
- Giants
- Other physical layer errors

Although this fix improves or resolves the switch response to the problem traffic, the trigger for the switch symptoms is resolved through updated NIC firmware and drivers, when they are available from the device manufacturer.

- **Spanning Tree (PR_0000017820)** — Path costs are not appropriately updated after addition or removal of distributed trunks from the configuration.
- **QoS (PR_0000009724)** — QoS Priority settings are not present in routed packets.
- **Crash (PR_0000015746)** — A very busy switch with a large configuration may experience multiple module resets, displaying event log messages similar to the following.

```
Lost Communications detected - Heart Beat Lost(51)
Msg loss detected - no ack for seq # 15803
Msg loss detected - no ack for seq # 16654
Msg loss detected - no ack for seq # 17472
Msg loss detected - no ack for seq # 19015
Lost Communications detected - Source Message System(48)
Lost Communications detected - Source Message System(50)
Lost Communications detected - Source Message System(55)
```
- **Loop Protection (PR_0000037759)** — Loop-Protect may detect a loop and report that the port is shut down when it is not. This allows the loop-protect packets to flood the network and potentially starve spanning-tree and other protocols.

Release W.14.16

The following problems were resolved in release W.14.16. (Not a public release.)

- **10-GbE (PR_0000038110)** — 10-GbE SFP+ transceivers may fail to form a stable link.
- **Crash (PR_0000017435)** — Configuring a switch using the CLI command **include-credentials** may cause an unexpected reboot, if the switch has never had the feature previously enabled. The crash message may vary.

Release W.14.17 through W.14.25

Versions W.14.17 through W.14.25 were never built.

Release W.14.26

The following problems were resolved in release W.14.26.

- **LLDP (PR_0000038230)** — The length of a CDP packet may prevent the switch from accepting the packet.
- **Proxy-ARP (PR_0000038934/0000038938)** — The switch may provide proxy-ARP replies to gratuitous-ARPs, which could be interpreted as a "duplicate IP address" by the original sending host.
- **Proxy-ARP (PR_0000038935)** — The switch may provide proxy-ARP replies to ARPs from a source IP address that is not within scope of the switch's IP address/subnet mask.
- **DHCP-Snooping (PR_0000019155)** — DHCP-Snooping does not correctly identify fragmented packets, and drops UDP Fragments if a hex value of 44 (68 Decimal) is present in the payload where the header is usually located (in a non-fragment).



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

May 2009
Manual Part Number
5900-0244