



## Release Notes:

### Version T.12.52 Software

*for the ProCurve Series 2900 Switches*

---

The T.12.51 software supports these switches:

- ProCurve Switch 2900-24G (J9049A) and 2900-48G (J9050A)

These release notes include information on the following:

- Downloading switch software and documentation from the Web ([page 1](#))
- Clarification of operating details for certain software features ([page 7](#))
- A listing of software enhancements in recent releases ([page 8](#))
- A listing of software fixes included in releases T.11.10 through T.12.52 ([page 43](#))

#### **Related Publications**

For the latest version of any of the publications listed below, visit the ProCurve Networking Web site at [//www.procurve.com](http://www.procurve.com). Click on **Technical support**, then **Product manuals**.

© Copyright 2006-2008  
Hewlett-Packard Development Company, LP.  
The information contained herein is subject to change  
without notice.

## Publication Number

5991-4790  
January 2008

## Applicable Products

ProCurve Switch 2900-24G (J9049A)  
ProCurve Switch 2900-48G (J9050A)

## 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

[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

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

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

## 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

<b>Software Management</b> .....	<b>1</b>
Software Updates .....	1
Downloading Switch Documentation and Software from the Web .....	1
Downloading Software to the Switch .....	2
TFTP Download from a Server .....	3
Xmodem Download From a PC or Unix Workstation .....	4
Saving Configurations While Using the CLI .....	5
ProCurve Switch, Routing Switch, and Router Software Keys .....	6
OS/Web/Java Compatibility Table .....	7
<b>Clarifications</b> .....	<b>7</b>
<b>Enhancements</b> .....	<b>8</b>
Release T.11.10 through T.11.12 Enhancements .....	8
Release T.11.13 Enhancements .....	8
Release T.12.01 Enhancements .....	8
Advanced Traffic Management Guide .....	8
Management and Configuration Guide .....	9
Multicast and Routing Guide .....	9
Security Guide .....	9
Release T.12.02 Enhancements .....	10
Release T.12.03 Enhancements .....	10
Release T.12.04 Enhancements .....	11
Release T.12.05 Enhancements .....	11
How RADIUS-Based Authentication Affects VLAN Operation .....	11
Release T.12.06 Enhancements .....	17
Saving Security Credentials in a Configuration File .....	17
Release T.12.07 Enhancements .....	32
Release T.12.08 Enhancements .....	32
show vlan ports CLI Command Enhancement .....	32
Release T.12.09 Enhancements .....	34

RADIUS Accounting with IP Attribute .....	35
Release T.12.10 Enhancements .....	35
Send SNMP v2c Informs .....	35
Release T.12.11 Enhancements (Never released.) .....	37
RADIUS Server Unavailable .....	37
Release T.12.12 Enhancements (Never released.) .....	40
Release T.12.40 Enhancements (Never released.) .....	40
Release T.12.50 Enhancements .....	41
Telephone Attached to PC Auth .....	41
Release T.12.51 Enhancements .....	42
Release T.12.52 Enhancements .....	42
<b>Software Fixes in Release T.11.10 - T.12.52 .....</b>	<b>43</b>
Release T.11.10 .....	43
Release T.11.11 .....	44
Release T.11.12 .....	44
Release T.11.13 .....	45
Release T.12.01 .....	46
Release T.12.02 .....	47
Release T.12.03 .....	48
Release T.12.04 .....	48
Release T.12.05 .....	49
Release T.12.06 .....	49
Release T.12.07 .....	49
Release T.12.08 .....	50
Release T.12.09 .....	51
Release T.12.10 .....	51
Release T.12.11 (Never released.) .....	51
Release T.12.12 (Never released.) .....	52
Release T.12.13 .....	53
Release T.12.40 (Never released.) .....	53
Release T.12.50 .....	54

Release T.12.51 .....	55
Release T.12.52 .....	56

# 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 the ProCurve Networking Web site as described below.

### To Download a Software Version:

1. Go to the ProCurve Networking Web site at:  
[www.procurve.com](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 the ProCurve Networking Web site at [www.procurve.com](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. For the ProCurve Series 2900 switches, the link for the manuals pages is: [www.hp.com/rnd/support/manuals/2900.htm](http://www.hp.com/rnd/support/manuals/2900.htm)
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

ProCurve Networking periodically provides switch software updates through the ProCurve Networking Web site ([www.procurve.com](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:
  - 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 4).
- 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 T\_11\_1x.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 T_11_1x.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...
```

3. When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:
4. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
5. Reboot the switch from the flash area that holds the new software (primary or secondary).

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. (ProCurve 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. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
6. Reboot the switch from the flash area that holds the new software (primary or secondary).

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] ?
```
- When the startup config is different than the running config, use of the **show config** command may cause the switch to crash.

## Software Management

ProCurve Switch, Routing Switch, and Router Software Keys

# ProCurve Switch, Routing Switch, and Router Software Keys

Software Letter	ProCurve Networking Products
<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, and 5400zl Series (5406zl, 5406zl-48G, 5412zl, and 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 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.
<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>T</b>	Switch 2900 Series (2900-24G, and 2900-48G)
<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>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	

## Clarifications

---

The following clarifications apply to series 2900 switch documentation as of the T.12.00 release.

■ **Enabling Jumbo Frames and Flow Control**

The 2900 series switches support simultaneous use of Jumbo Frames and Flow Control, and the switch allows flow control and jumbo packet capability to co-exist on a port. (The earlier version of the Management and Configuration Guide incorrectly stated that these features could not be enabled at the same time.)

■ **TACACS+ Encryption Key Exclusion from TFTP Copies**

When using the copy command to transfer a configuration to a TFTP server, any server-specific or global encryption keys in the TACACS+ configuration will not be included in the transferred file. Otherwise, a security breach could occur, allowing access to the TACACS+ username/password information.

# Enhancements

---

Unless otherwise noted, each new release includes the enhancements added in all previous releases. Enhancements are listed in chronological order, oldest to newest software release. For the latest enhancements since the last general release was published, go to “[Release T.12.07 Enhancements](#)” on page 32.

Descriptions and instructions for enhancements included in Release T.12.00 or earlier are included in the latest release of manuals for the ProCurve 2900 Series switches (February 2007), available on the web at [www.hp.com/rnd/support/manuals](http://www.hp.com/rnd/support/manuals)

Release T.11.01 was the first production software release for the ProCurve 2900 Series switches. Releases T.11.02 through T.11.09 were never built.

Release T.11.13 is the last release of the T.11.xx software. The switch 2900 series software code was rolled to the T.12.01 code branch with no intervening releases.

---

## Release T.11.10 through T.11.12 Enhancements

*No new enhancements, software fixes only.*

### Release T.11.13 Enhancements

The following enhancements are included in the T.11.13 release.

- Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.
- Historical information about MAC addresses that have been moved has been added to the "show tech" command output.

### Release T.12.01 Enhancements

The following enhancements are included in the T.12.01 release documentation. The enhancements are listed by the title of the switch guide that includes the full description and instructions for that enhancement.

#### Advanced Traffic Management Guide

- **Loop Protection**—Detects the formation of loops when there is an unmanaged device on the network by transmitting loop protection protocol packets.

- **Qos Queue Config**—Allows you to reduce the number of outbound queues that all switch ports will use to buffer packets for 802.1p user priorities.
- **BPDU Protection**—A security feature designed to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain.
- **BPDU Filtering**—Allows control of spanning-tree participation on a per-port basis. It can be used to exclude specific ports from becoming part of spanning tree operations.

## Management and Configuration Guide

- **Unidirectional Link Detection (UDLD)**—Monitors a link between two ProCurve switches and blocks the ports on both ends of the link if the link fails at any point between the two devices. This feature is particularly useful for detecting failures in fiber links and trunks.
- **Loopback Interface**—A virtual interface that is always up and reachable as long as at least one of the IP interfaces on the switch is operational. By default, each switch has an internal loopback interface (**lo0**). You can configure up to seven other loopback interfaces on the switch.
- **sFlow**— can be configured via the CLI for up to three distinct sFlow instances. Once enabled, an sFlow receiver/destination can be independently configured for full flow-sampling and counter-polling. (Introduced in Software Release K.11.34)
- **Clear Logging Command**—Causes event log entries to be hidden from display when using the standard **show logging** command.
- **Reload After/At Command**—**after**: Schedules a warm reboot of the switch after a given amount of time has passed.  
**at**: Schedules a warm reboot of the switch at a given time.

## Multicast and Routing Guide

- **DHCP Option 82 Enhancement**—Specifies the IP address of the (optional) Management VLAN configured on the routing switch.
- **RIP**—the Routing Exchange Protocol (RIP) is now supported. RIP is an IP route exchange protocol that uses a *distance vector* (a number representing distance) to measure the cost of a given route.

## Security Guide

- **RADIUS AAA**—Allows you to limit the services for a user by enabling AAA RADIUS authorization. The NAS uses the information set up on the RADIUS server to control the user's access to CLI commands.

## Enhancements

### Release T.12.02 Enhancements

- **Client-based Access Control**—provides client-level security that allows LAN access to individual 802.1X clients (up to 8 per port), where each client gains access to the LAN by entering valid user credentials. This operation improves security by opening a given port only to individually authenticated clients, while simultaneously blocking access to the same port for clients that cannot be authenticated.
- **Controlled Directions 802.1X and Web/MAC Auth**— allows you to use the **aaa port-access controlled-directions** command to configure how a port transmits traffic before it successfully authenticates a client and enters the authenticated state. Available for 802.1X and Web/MAC authorization. (Added in T.11.10, now documented)

The following enhancements included in Release T.12.01 are not covered in the February 2007 version of the switch 2900 series documentation.

- **Enhancement (PR\_1000298920)** — A ping request issued to a VLAN which is down will now return a more specific message; instead of "request timed out," the message "The destination address is unreachable" will be displayed.
- **Enhancement (PR\_1000373226)** — Support was added for the J9054B 100-FX SFP-LC.
- **Enhancement (PR\_1000376626)** — Enhanced CLI **qos dscp-map help** help and **show dscp-map** text to warn the user that inbound classification based on DSCP codepoints only occurs if **qos type-of-service diff-services** is also configured.

---

## Release T.12.02 Enhancements

The following enhancements are included in the T.12.02 release.

- **Enhancement (PR\_1000379804)** — Historical information about MAC addresses that have been moved has been added to the **show tech** command output.

---

## Release T.12.03 Enhancements

The following enhancements are included in the T.12.03 release (never released).

- **Enhancement (PR\_1000404544)** — Provides TCP/UDP port range prioritization in the **qos** command; the **range** option assigns an 802.1p priority to (IPv4) TCP or UDP packets associated with a range of TCP/UDP ports. The **range** option requires two port numbers that specify the range.

```
qos <udp-port | tcp-port> <tcp/udp port number | range <tcp/udp port number> <tcp/udp port number>> priority < 0 - 7>
```

For more information, refer to “QoS UDP/TCP Priority” in the *Advanced Traffic Management Guide*.

- **Enhancement (PR\_1000398393)** — For the **interface <port-list> speed-duplex** command, added the **auto-10-100** configuration option to constrain a link to 10/100 Mbps speed and allow a more rapid linkup process when 1000 Mbps operation is not possible.

---

## Release T.12.04 Enhancements

*No new enhancements, software fixes only.*

---

## Release T.12.05 Enhancements

The following enhancement is included in the T.12.05 release (never released).

- **Enhancement (PR\_1000408960)** — RADIUS-Assigned GVRP VLANs. For more information, see [“How RADIUS-Based Authentication Affects VLAN Operation”](#) below.

### How RADIUS-Based Authentication Affects VLAN Operation

Using a RADIUS server to authenticate clients, you can provide port-level security protection from unauthorized network access for the following authentication methods:

- 802.1X: Port-based or client-based access control to open a port for client access after authenticating valid user credentials.
- MAC address: Authenticates a device’s MAC address to grant access to the network.
- Web-browser interface: Authenticates clients for network access using a web page for user login.

---

### Note

You can use 802.1X (port-based or client-based) authentication and either Web or MAC authentication at the same time on a port, with a maximum of 8 clients allowed on the port. (The default is one client.) Web authentication and MAC authentication are mutually exclusive on the same port. Also, you must disable LACP on ports configured for any of these authentication methods. For more information, refer to the “Configuring Port-Based and Client-Based Access Control (802.1X)” and “Web and MAC Authentication” chapters of the *Access Security Guide*.

---

## VLAN Assignment on a ProCurve Port

Following client authentication, VLAN configurations on a ProCurve port are managed as follows when you use 802.1X, MAC, or Web authentication:

- The port resumes membership in any tagged VLANs for which it is already assigned in the switch configuration. Tagged VLAN membership allows a port to be a member of multiple VLANs simultaneously.
- The port is temporarily assigned as a member of an untagged (static or dynamic) VLAN for use during the client session according to the following order of options.
  - a. The port joins the VLAN to which it has been assigned by a RADIUS server during client authentication.
  - b. If RADIUS authentication does not include assigning the port to a VLAN, then the switch assigns the port to the authorized-client VLAN configured for the authentication method.
  - c. If the port does not have an authorized-client VLAN configured, but is configured for membership in an untagged VLAN, the switch assigns the port to this untagged VLAN.

## Operating Notes

- During client authentication, a port assigned to a VLAN by a RADIUS server or an authorized-client VLAN configuration is an untagged member of the VLAN for the duration of the authenticated session. This applies even if the port is also configured in the switch as a tagged member of the same VLAN. The following restrictions apply:
  - If the port is assigned as a member of an untagged *static* VLAN, the VLAN must already be configured on the switch. If the static VLAN configuration does not exist, the authentication fails.
  - If the port is assigned as a member of an untagged *dynamic* VLAN that was learned through GVRP, the dynamic VLAN configuration must exist on the switch at the time of authentication and GVRP-learned dynamic VLANs for port-access authentication must be enabled

If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic VLAN for authentication sessions on the switch, the authentication fails.

- To enable the use of a GVRP-learned (dynamic) VLAN as the untagged VLAN used in an authentication session, enter the **aaa port-access gvrp-vlans** command, as described in [“Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions” on page 16](#).
- Enabling the use of dynamic VLANs in an authentication session offers the following benefits:
  - You avoid the need of having static VLANs pre-configured on the switch.
  - You can centralize the administration of user accounts (including user VLAN IDs) on a RADIUS server.

For information on how to enable the switch to dynamically create 802.1Q-compliant VLANs on links to other devices using the GARP VLAN Registration Protocol (GVRP), refer to the “GVRP” chapter in the *Advanced Traffic Management Guide*.

- For an authentication session to proceed, a ProCurve port must be an untagged member of the (static or dynamic) VLAN assigned by the RADIUS server (or an authorized-client VLAN configuration). The port temporarily drops any current untagged VLAN membership.

If the port is not already a member of the RADIUS-assigned (static or dynamic) untagged VLAN, the switch temporarily reassigns the port as an untagged member of the required VLAN (for the duration of the session). *At the same time, if the ProCurve port is already configured as an untagged member of a different VLAN, the port loses access to the other VLAN for the duration of the session.* (A port can be an untagged member of only one VLAN at a time.)

When the authentication session ends, the switch removes the temporary untagged VLAN assignment and re-activates the temporarily disabled, untagged VLAN assignment.

- If GVRP is already enabled on the switch, the temporary untagged (static or dynamic) VLAN created on the port for the authentication session is advertised as an existing VLAN.

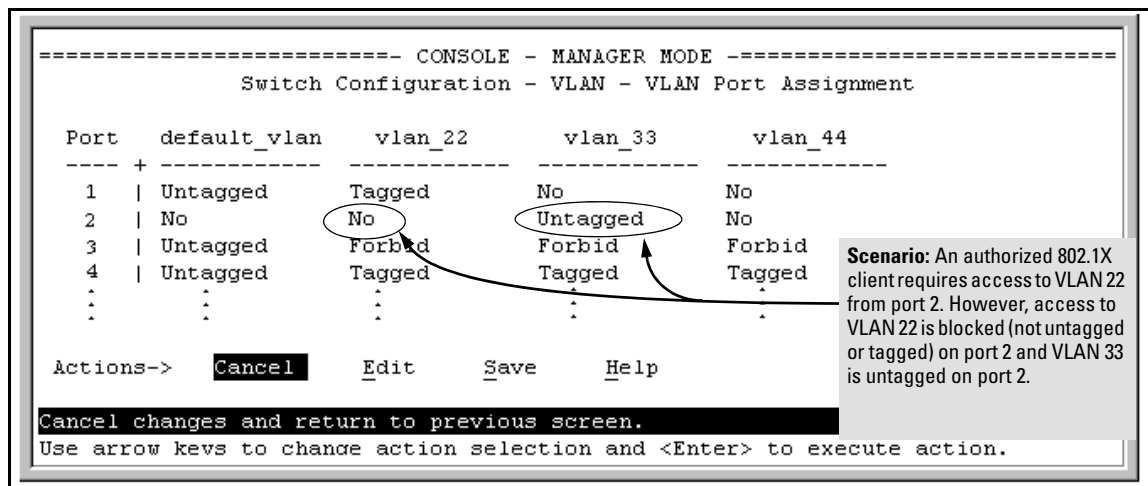
If this temporary VLAN assignment causes the switch to disable a different untagged static or dynamic VLAN configured on the port (as described in the preceding bullet and in [“Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session” on page 14](#)), the disabled VLAN assignment is not advertised. When the authentication session ends, the switch:

- Removes the temporary untagged VLAN assignment and stops advertising it.
  - Re-activates and resumes advertising the temporarily disabled, untagged VLAN assignment.
- If you modify a VLAN ID configuration on a port during an 802.1X, MAC, or Web authentication session, the changes do not take effect until the session ends.
  - When a switch port is configured with RADIUS-based authentication to accept multiple 802.1X and/or MAC or Web authentication client sessions, all authenticated clients must use the same port-based, untagged VLAN membership assigned for the earliest, currently active client session.

Therefore, on a port where one or more authenticated client sessions are already running, all such clients are on the same untagged VLAN. If a RADIUS server subsequently authenticates a new client, but attempts to re-assign the port to a different, untagged VLAN than the one already in use for the previously existing, authenticated client sessions, the connection for the new client will fail. For more on this topic, refer to “802.1X Open VLAN Mode” in the “Configuring Port-Based and Client-Based Access Control (802.1X)” chapter in the *Access Security Guide*.

## Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session

The following example shows how an untagged static VLAN is temporarily assigned to a port for use during an 802.1X authentication session. In the example, an 802.1X-aware client on port 2 has been authenticated by a RADIUS server for access to VLAN 22. However, port 2 is not configured as a member of VLAN 22 but as a member of untagged VLAN 33 as shown in [Figure 1](#).



**Figure 1. Example of an Active VLAN Configuration in the Menu Interface View**

In [Figure 1](#), if RADIUS authorizes an 802.1X client on port 2 with the requirement that the client use VLAN 22, then:

- VLAN 22 becomes available as Untagged on port 2 for the duration of the session.
- VLAN 33 becomes unavailable to port 2 for the duration of the session (because there can be only one untagged VLAN on any port).

To view the temporary VLAN assignment as a change in the active configuration, use the **show vlan <vlan-id>** command as shown in [Figure 2](#), where **<vlan-id>** is the (static or dynamic) VLAN used in the authenticated client session.

```

ProCurve(config)# show vlan 22
Status and Counters - VLAN Information - Ports - VLAN 22
802.1Q VLAN ID : 22
Name : VLAN 22
Status : Port-based
Voice : No
Jumbo : No

Port Information Mode      Unknown VLAN Status
-----
1                Tagged      Learn      Up
2                802.1X     Learn      Up
4                Tagged      Learn      Up
.                .           .           .
.                .           .           .
.                .           .           .

Overridden Port VLAN configuration

Port Mode
-----
2        No
  
```

In the **show** command output, port 2 is temporarily configured as untagged on VLAN 22 for an 802.1X session. This temporary configuration change is necessary to accommodate an 802.1X client's access, authenticated by a RADIUS server, in which the server included an instruction to assign the client session to VLAN 22.

**Note:** In the current VLAN configuration, port 2 is only listed as a member of VLAN 22 in **show vlan 22** output when an 802.1X session with an authenticated client is active. Otherwise, port 2 is not listed.

**Figure 2. Active Configuration for VLAN 22 Temporarily Changes for the 802.1X Session**

However, as shown in [Figure 1](#), VLAN 33 is configured as untagged on port 2 and because a port can be untagged on only one VLAN, port 2 loses access to VLAN 33 for the duration of the 802.1X session on VLAN 22.

You can verify the temporary loss of port 2 access to VLAN 33 by entering the **show vlan 33** command as shown in [Figure 3](#).

```

ProCurve# show vlan 33
Status and Counters - VLAN Information - Ports - VLAN 33
802.1Q VLAN ID : 33
Name : VLAN33
Status : Port-based
Voice : No
Jumbo : No

Port Information Mode      Unknown VLAN Status
-----
4                Tagged      Learn      Up

Overridden Port VLAN configuration

Port Mode
-----
2        Untagged
  
```

Although port 2 is configured as Untagged on VLAN 33 (in [Figure 1](#)), port 2 is not listed in **show vlan 33** output during the 802.1X session that uses VLAN 22 in Untagged mode. However, when the 802.1X session on VLAN 22 ends, the active configuration restores port 2 as an untagged member of VLAN 33.

**Figure 3. Active Configuration for VLAN 33 Temporarily Drops Port 2 for the 802.1X Session**

When the 802.1X client session on port 2 ends, the port removes the temporary untagged VLAN membership. The static VLAN (VLAN 33) that is “permanently” configured as untagged on the port becomes available again. Therefore, when the RADIUS-authenticated 802.1X session on port 2 ends, VLAN 22 access on port 2 also ends, and the untagged VLAN 33 access on port 2 is restored as shown in Figure 4.

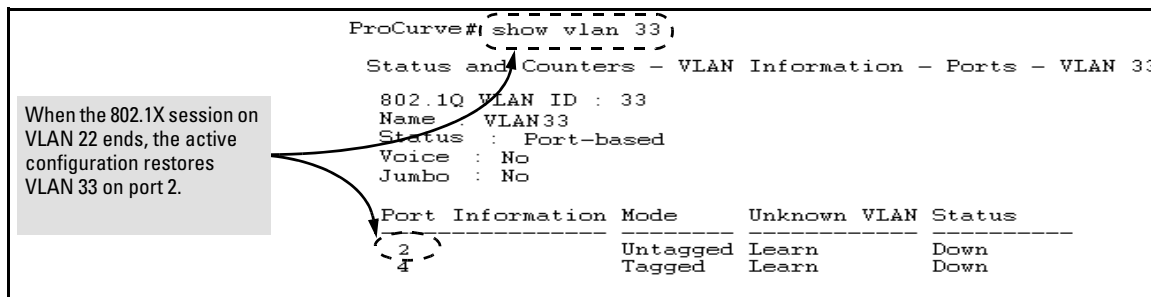


Figure 4. The Active Configuration for VLAN 33 Restores Port 2 After the 802.1X Session Ends

## Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions

**Syntax:** aaa port-access gvrp-vlans

*Enables the use of dynamic VLANs (learned through GVRP) in the temporary untagged VLAN assigned by a RADIUS server on an authenticated port in an 802.1X, MAC, or Web authentication session.*

*Enter the **no** form of this command to disable the use of GVRP-learned VLANs in an authentication session.*

*For information on how to enable a switch to dynamically create 802.1Q-compliant VLANs, refer to the “GVRP” chapter in the Access Security Guide.*

**Notes:**

*1. If a port is assigned as a member of an untagged dynamic VLAN, the dynamic VLAN configuration must exist at the time of authentication and GVRP for port-access authentication must be enabled on the switch.*

*If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic VLAN for authentication sessions on the switch, the authentication fails.*

*(Continued)*

**Syntax:** `aaa port-access gvrp-vlans` (*Continued*)

2. After you enable dynamic VLAN assignment in an authentication session, it is recommended that you use the **interface unknown-vlans** command on a per-port basis to prevent denial-of-service attacks. The **interface unknown-vlans** command allows you to:

- Disable the port from sending advertisements of existing GVRP-created VLANs on the switch.
- Drop all GVRP advertisements received on the port.

For more information, refer to the “GVRP” chapter in the *Advanced Traffic Management Guide*.

3. If you disable the use of dynamic VLANs in an authentication session using the **no aaa port-access gvrp-vlans** command, client sessions that were authenticated with a dynamic VLAN continue and are not deauthenticated.

(This behavior differs from how static VLAN assignment is handled in an authentication session. If you remove the configuration of the static VLAN used to create a temporary client session, the 802.1X, MAC, or Web authenticated client is deauthenticated.)

However, if a RADIUS-configured dynamic VLAN used for an authentication session is deleted from the switch through normal GVRP operation (for example, if no GVRP advertisements for the VLAN are received on any switch port), authenticated clients using this VLAN are deauthenticated.

For information on how static and dynamic VLANs are assigned in a RADIUS-based 802.1X, MAC, or Web authentication session, refer to the “How RADIUS/802.1X Authentication Affects VLAN Operation” section in the “Configuring Port-Based and Client-Based Access Control (802.1X)” chapter of the *Access Security Guide*.

---

---

## Release T.12.06 Enhancements

Release T.12.06 includes the following enhancement:

- **Enhancement (PR\_1000308332)**— Passwords (hashed) can be saved to the configuration file.

### Saving Security Credentials in a Configuration File

In software release T.12.06 and greater, you can store and view the following security settings in the running-config file associated with the current software image by entering the **include-credentials** command. Earlier software releases store these security configuration settings only in internal flash memory and do not allow you to include and view them in the running-config file.

- Local manager and operator passwords and (optional) user names that control access to a management session on the switch through the CLI, menu interface, or web browser interface
- SNMP security credentials used by network management stations to access a switch, including authentication and privacy passwords
- Port-access passwords and usernames used as 802.1X authentication credentials for access to the switch
- TACACS+ encryption keys used to encrypt packets and secure authentication sessions with TACACS+ servers
- RADIUS shared secret (encryption) keys used to encrypt packets and secure authentication sessions with RADIUS servers
- Secure Shell (SSH) public keys used to authenticate SSH clients that try to connect to the switch.

### **Benefits of Saving Security Credentials**

The benefits of including and saving security credentials in a configuration file are as follows:

- After making changes to security parameters in the running configuration, you can experiment with the new configuration and, if necessary, view the new security settings during the session. After verifying the configuration, you can then save it permanently by writing the settings to the startup-config file.
- By permanently saving a switch's security credentials in a configuration file, you can upload the file to a TFTP server or Xmodem host, and later download the file to the ProCurve switches on which you want to use the same security settings without having to manually configure the settings (except for SNMPv3 user parameters) on each switch.
- By storing different security settings in different files, you can test different security configurations when you first download a new software version that supports multiple configuration files by changing the configuration file used when you reboot the switch.

For more information about how to experiment with, upload, download, and use configuration files with different software versions, refer to the following chapters:

- “Switch Memory and Configuration” and “File Transfers” in the *Management and Configuration Guide*
- “Configuring Username and Password Security” in the *Access Security Guide*

### **Security Settings that Can Be Saved**

This section describes the security settings that can be saved to a configuration file in software release T.12.06 and greater:

- Local manager and operator passwords and user names
- SNMP security credentials, including SNMPv1 community names and SNMPv3 usernames, authentication, and privacy settings
- 802.1X port-access passwords and usernames
- TACACS+ encryption keys
- RADIUS shared secret (encryption) keys
- Public keys of SSH-enabled management stations that are used by the switch to authenticate SSH clients that try to connect to the switch

### **Local Manager and Operator Passwords**

In software releases earlier than T.12.06, the manager and operator passwords and user names used to start a management session on the switch are treated as follows:

- You set the passwords and (optional) user names using the CLI or menu interface as described in “Configuring Local Password Security” in the *Access Security Guide*.
- Only the following information is saved to the running configuration:

```
password manager [user-name <name>]  
password operator [user-name <name>]
```

## Enhancements

### Release T.12.06 Enhancements

In software release T.12.06 and greater, you cannot view the configured local password settings in plain text. However, by entering the **include-credentials** command described later, you can view a hash of the local password settings in the running-config file, in the format:

```
password manager [user-name <name>] <hash-type> <pass-hash>
password operator [user-name <name>] <hash-type> <pass-hash>
```

Where:

<name> is an alphanumeric string for the user name assigned to the manager or operator.

<hash-type> indicates the type of hash algorithm used: SHA-1.

<pass-hash> is the SHA-1 authentication protocol's hash of the password.

For example, a manager username and password may be stored in a running-config file as follows:

```
password manager user-name Spock SHA1
2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
```

If you permanently save password configurations in the startup-config file by entering the **write memory** command, the passwords take effect when a switch boots with the software version associated with the configuration file.

---

## Caution

If a startup configuration file does not contain a manager or operator password, the switch will not have password protection and can be accessed through Telnet, the serial port, or web interface with full manager privileges.

---

## Password Command

In software release T.12.06 and greater, the **password** command in the CLI is enhanced to support the following syntax:

**Syntax:** [no] password <manager | operator | port-access> [user-name <name>] <hash-type> <password>

Where:

- **manager** configures access to the switch with manager-level privileges.
- **operator** configures access to the switch with operator-level privileges.
- **port-access** configures access to the switch through 802.1X authentication with operator-level privileges.
- **user-name <name>** is the (optional) text string of the user name associated with the password.

- The **<hash-type>** parameter specifies the type of algorithm (if any) used to hash the password. Valid values are **plaintext** or **sha-1**.
- The **<password>** parameter is the clear ASCII text string or SHA-1 hash of the password.  
You can enter a manager/operator password in clear ASCII text or hashed format, while the port-access password must be clear ASCII text only. Manager and operator passwords are displayed and saved in a configuration file only in hashed format; port-access passwords are displayed and saved only as plain ASCII text.

After you enter the complete command syntax that includes the password, the password is set and you are not prompted to enter the password a second time.

This command enhancement allows you to configure manager, operator, and 802.1X port-access passwords using the CLI in only one step (instead of entering the **password** command and then being prompted twice to enter the actual password, as in software releases earlier than T.12.06).

- For more information about configuring local manager and operator passwords, refer to the “Configuring Username and Password Security” chapter in the *Access Security Guide*.
- For more information about configuring a port-access password for 802.1X client authentication, see [“802.1X Port-Access Credentials” on page 22](#).

## SNMP Security Credentials

In software releases earlier than T.12.06, SNMP security credentials are saved in a configuration file as follows:

- SNMPv1 community names and write-access settings are saved as shown in the following example:

```
snmp-server community "vulcan" Unrestricted
```

- SNMPv3 authorization and privacy protocols and passwords used with each SNMPv3 user are not saved. However, SNMPv3 user names are saved; for example:

```
snmpv3 user "initial"
```

In software release T.12.06 and greater, SNMPv1 community names and write-access settings, and SNMPv3 usernames are still saved in the running configuration when you enter the **include-credentials** command.

In addition, the following SNMPv3 security parameters are also saved:

```
snmpv3 user "<name>" [auth <md5|sha> "<auth-pass>"] [priv "<priv-pass>"]
```

Where:

**<name>** is the name of an SNMPv3 management station.

**auth <md5 | sha>** is the (optional) authentication method used for the management station.

**<auth-pass>** is the hashed authentication password used with the configured authentication method. **priv** "**<priv-pass>**" is the (optional) hashed privacy password used by a privacy protocol to encrypt SNMPv3 messages between the switch and the station.

The following example shows the additional security credentials for SNMPv3 users that can be saved in a running-config file:

```
snmpv3 user boris \  
auth md5 "9e4cfef901f21cf9d21079debeca453" \  
priv "82ca4dc99e782db1a1e914f5d8f16824"  
  
snmpv3 user alan \  
auth sha "8db06202b8f293e9bc0c00ac98cf91099708ecdf" \  
priv "5bc4313e9fd7c2953aaa9406764fe8bb629a538"
```

**Figure 5. Security Credentials for SNMPv3**

Although you can enter an SNMPv3 authentication or privacy password in either clear ASCII text or the SHA-1 hash of the password, the password is displayed and saved in a configuration file only in hashed format, as shown in the preceding example.

For more information about the configuration of SNMP security parameters, refer to the “Configuring for Network Management Applications” chapter in the *Management and Configuration Guide*.

### 802.1X Port-Access Credentials

In software release T.12.06 and greater, 802.1X authenticator (port-access) credentials can be stored in a configuration file.

802.1X *authenticator* credentials are used by a port to authenticate supplicants requesting a point-to-point connection to the switch. 802.1X *supplicant* credentials are used by the switch to establish a point-to-point connection to a port on another 802.1X-aware switch. Only 802.1X authenticator credentials are stored in a configuration file. For information about how to use 802.1X on the switch both as an authenticator and a supplicant, refer to the “Configuring Port-Based and Client-Based Access Control (802.1X)” chapter in the *Access Security Guide*.

In software release T.12.06 and greater, the local password configured with the **password** command is no longer accepted as an 802.1X authenticator credential. A new configuration command (**password port-access**) is introduced to configure the local operator username and password used as 802.1X authentication credentials for access to the switch.

The **password port-access** values are now configured separately from the manager and operator passwords configured with the **password manager** and **password operator** commands and used for management access to the switch. For information on the new **password** command syntax, see “[Password Command](#)” on page 20.

After you enter the complete **password port-access** command syntax, the password is set. You are not prompted to enter the password a second time.

### **TACACS+ Encryption Key Authentication**

You can use TACACS+ servers to authenticate users who request access to a switch through Telnet (remote) or console (local) sessions. TACACS+ uses an authentication hierarchy consisting of:

- Remote passwords assigned in a TACACS+ server
- Local manager and operator passwords configured on the switch.

When you configure TACACS+, the switch first tries to contact a designated TACACS+ server for authentication services. If the switch fails to connect to any TACACS+ server, it defaults to its own locally assigned passwords for authentication control if it has been configured to do so.

For improved security, you can configure a global or server-specific encryption key that encrypts data in TACACS+ packets transmitted between a switch and a RADIUS server during authentication sessions. The key configured on the switch must match the encryption key configured in each TACACS+ server application. (The encryption key is sometimes referred to as “shared secret” or “secret” key.) For more information, refer to the “TACACS+ Authentication” chapter in the *Access Security Guide*.

In software releases earlier than T.12.06, the global and server-specific TACACS+ encryption keys cannot be saved in a configuration file that can be copied from the switch. These keys are stored only in flash memory and can be viewed by using the **show tacacs** command.

In software release T.12.06 and greater, TACACS+ shared secret (encryption) keys can be saved in a configuration file with the following syntax:

```
tacacs-server key <keystring>
```

Where:

**<keystring>** is the encryption key (in clear text) used for secure communication with all or a specific TACACS+ server.

### **RADIUS Shared-Secret Key Authentication**

You can use RADIUS servers as the primary authentication method for users who request access to a switch through Telnet, SSH, Web interface, console, or port-access (802.1X). The shared secret key is a text string used to encrypt data in RADIUS packets transmitted between a switch and a RADIUS server during authentication sessions. Both the switch and the server have a copy of the key; the key is never transmitted across the network. For more information, refer to the “RADIUS Authentication and Accounting” chapter in the *Access Security Guide*.

In software releases earlier than T.12.06, the global and server-specific RADIUS encryption keys cannot be saved in a configuration file that can be copied from the switch. These keys are stored only in flash memory and can be viewed by using the **show radius** command.

In software release T.12.06 and greater, RADIUS shared secret (encryption) keys can be saved in a configuration file with the following syntax:

```
radius-server key <keystring>
```

Where:

**<keystring>** is the encryption key (in clear text) used for secure communication with all or a specific RADIUS server.

## SSH Client Public-Key Authentication

Secure Shell version 2 (SSHv2) is used by ProCurve switches to provide remote access to SSH-enabled management stations. Although SSH provides Telnet-like functions, unlike Telnet, SSH provides encrypted, two-way authenticated transactions. SSH client public-key authentication is one of the types of authentication used.

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 public key stored on the switch can gain access at the manager or operator level. For more information about how to configure and use SSH public keys to authenticate SSH clients that try to connect to the switch, refer to the “Configuring Secure Shell” chapter in the *Access Security Guide*.

In software releases earlier than T.12.06, client public-keys that are used to authenticate SSH clients are only stored in flash memory, not in the running-config file. You can view the SSH public keys stored on a switch by entering the **show crypto client-public-key** command. The only SSH security credential that is stored in the running configuration are the following commands:

```
aaa authentication ssh login public-key  
aaa authentication ssh enable public-key
```

- The **aaa authentication ssh login public-key** command allows operator access using SSH public-key authentication.
- The **aaa authentication ssh enable public-key** command allows manager access using SSH public-key authentication.

In software release T.12.06 and greater, the SSH security credential that is stored in the running configuration is the syntax of the **ip ssh public-key** command used to authenticate SSH clients for manager or operator access, along with the hashed content of each SSH client public-key. The syntax of the **ip ssh public-key** command is as follows:

```
ip ssh public-key <manager/operator> <keystring>
```

Where:

**manager** allows manager-level access using SSH public-key authentication.

**operator** allows operator-level access using SSH public-key authentication.

**<keystring>** is a legal SSHv2 (RSA or DSA) public key. The text string for the public key must be a single quoted token.

If the keystring contains double-quotes, it can be quoted with single quotes ('*keystring*'). The following restrictions for a keystring apply:

- A keystring cannot contain both single and double quotes.
- A keystring cannot have extra characters, such as a blank space or a new line. However, to improve readability, you can add a backslash at the end of each line.

---

## Note

In software release K.12.01 and earlier, you can add up to ten SSH client public-keys to the switch only by using the **copy** command; for example:

```
$ copy tftp public-key ip-addr filename <manager/operato> [append]
```

If you enter the optional **append** keyword, the transmitted public-keys are added to existing SSH public-key configurations. If you omit the **append** keyword, the transmitted keys overwrite existing SSH public-key configurations.

In software release T.12.06 and greater, the **ip ssh public-key** command allows you to configure only one SSH client public-key at a time. (This command behavior differs from the **copy** command, which in earlier software releases allows you to load up to ten SSH client public-key configurations at once if they are stored in a single file on a TFTP server.) Therefore, the **ip ssh public-key** command behavior includes an implicit append that never overwrites existing public-key configurations on a running switch.

In all software releases, if you download a software configuration file that contains SSH client public-key configurations, the downloaded public-keys overwrite any existing keys, as happens with any other configured values.

---

To display the SSH public-key configurations (72 characters per line) stored in a configuration file, enter the **show config** or **show running-config** command. The following example shows the SSH public keys configured for manager access, along with the hashed content of each SSH client public-key, that are stored in a configuration file:

```
...
include-credentials
ip ssh public-key manager "ssh-dss \
AAAAB3NzaC1kc3MAAACBAPwJHSJmTRtpZ9BUNC+ZrsxhMuZEXQhaDME1vc/ \
EvYnTKxQ31bWvr/bT7W58NX/YJ1ZKTV2GZ2QJCicUUZVWjNfJCSa0v03XS4 \
BhkXjtHhz6gD701otgizUOO6/Xzf4/J9XkJHkOCnbHIqtB1sbRYBTxj3Nza \
KlymvIaU09X5TDAAAAFQCpWkxnbwFfTPasXnxfvDuLSxaC7wAAAIASBwxUP \
pv2scqPPXQghgaTkdpWGGtdFW/+K4xRskAnIaxuG0qLbnekohi+ND4TkKZd \
EeidgDh7qHusBhOFXM2g73RpE2rNqQnSf/QV95kdNwWIbxuusBAzvfajptd \
gca6cYR4xS4TuBcaKiorYj60kk144E1fkDwieQx8zABQAAAIEAu7/lkVodS \
G0vE0eJD23TLXvu94plXhRKCUAyvy2UyK+piG+Q1ellw9zSMaxPA1XJzSY/ \
imEp4p6WXEMc10lpXMRnkhnuMmpaMaQUT8NJTnu6hqf/LdQ2kqZjUuIyV9 \
LWyLg5ybs1kFLeOt0oo2Jbpy+U2e4jh2Bb77sX3G5C0= spock@sfc.gov" \
ip ssh public-key manager "ssh-rsa \
AAAAB3NzaC1yc2EAAAADAQABAAQGDyO9RDD52JZP8k2F2YZXubgwRAN0R \
JRslEov6y1RK3XkmgVatz1+mspiEmPS4wNK7bX/IoXNdGrGkoE8tPklZOZ \
oqGCf5Zs50PlnkxXvAidFs55AWqOf4MhfCqvtQCelnt6LFh4ZMig+YewgQG \
M6HlgeCSLÜbXXScipdPHysakw== "TectiaClientKey [1024-bit rsa, \
nobody@testmachine, Mon Aug 15 2005 14:47:34]"
ip ssh public-key manager "ssh-rsa \
AAAAB3NzaC1yc2EAAAABIwAAAIEAlKk9sVQ9LJOR6XO/hCMPxbiMNOK8C/ay \
+SQ10qGw+K9m3w3TmCfjh0ud9hivgbFT4F99AgnQkvm2eVsgoTtLRnff7uw \
NmpzqOqpHjD9YzItUgSKluPuFwXMCHKUGKa+G46A+EWxDAIypwVIZ697QmM \
qPFj1zdI4sIo5bDett2d0= joe@hp.com"
...
```

**Figure 6. Example of Hashed Content of an SSH Client Public Key**

If a switch configuration contains multiple SSH client public keys, each public key is saved as a separate entry in the configuration file. You can configure up to ten SSH client public-keys on a switch.

## Enabling the Storage and Display of Security Credentials

To enable the security settings described in [“Security Settings that Can Be Saved” on page 18](#) to be included and viewed in the running configuration on the switch, enter the **include-credentials** command.

**Syntax:** [no] include-credentials

*Enables the inclusion and display of the currently configured manager and operator usernames and passwords, RADIUS shared secret keys, SNMP and 802.1X authenticator (port-access) security credentials, and SSH client public-keys in the running configuration. (Earlier software releases store these security configuration settings only in internal flash memory and do not allow you to include and view them in the running-config file.)*

*To view the currently configured security settings in the running configuration, enter one of the following commands:*

- **show running-config:** *Displays the configuration settings in the current running-config file.*
- **write terminal:** *Displays the configuration settings in the current running-config file. For more information, refer to the “Switch Memory and Configuration” chapter in the Management and Configuration Guide.*

*To copy the contents of the running-config file from the switch to a USB flash memory device, enter the **copy running-config usb** command. For more information, refer to the “File Transfers” appendix in the Management and Configuration Guide.*

*The “no” form of the command disables only the display and copying of these security parameters from the running configuration, while the security settings remain active in the running configuration.*

**Default:** *The security credentials described in [“Security Settings that Can Be Saved” on page 18](#) are not stored in the running configuration.*

## Operating Notes

---

### Caution

- When you first enter the **include-credentials** command to save the additional security credentials to the running configuration, these settings are moved from internal storage on the switch to the running-config file.

You are prompted by a warning message to perform a **write memory** operation to save the security credentials to the startup configuration. The message reminds you that if you do not save the current values of these security settings from the running configuration, they will be lost the next time you boot the switch and will revert to the values stored in the startup configuration.

- When you boot a switch with a startup configuration file that contains the **include-credentials** command, any security credentials that are stored in internal flash memory are ignored and erased. The switch will load only the security settings in the startup configuration file, if any.
- In software releases earlier than T.12.06, configuration changes to some security credentials (described in [“Security Settings that Can Be Saved” on page 18](#)) are applied immediately and saved in internal storage (flash memory) on the switch. They do not require you to enter the **write memory** command to permanently save them in the startup configuration.

However, in software release T.12.06 and greater, this switch behavior changes. Security settings are no longer automatically saved internally in flash memory and loaded with the startup configuration when a switch boots up. The configuration of all security credentials requires that you use the **write memory** command to save them in the startup configuration in order for them to not be lost when you log off or reboot the switch. A warning message reminds you to permanently save a security setting, which was formerly automatically saved in internal flash, after you configure it.

---

- After you enter the **include-credentials** command, the currently configured manager and operator usernames and passwords, RADIUS shared secret keys, SNMP and 802.1X authenticator (port-access) security credentials, and SSH client public-keys are saved in the running configuration.

Use the **no include-credentials** command to disable the display and copying of these security parameters from the running configuration (using the **show running-config** and **copy running-config** commands), without disabling the configured security settings on the switch.

After you enter the **include-credentials** command, you can toggle between the non-display and display of security credentials in **show** and **copy** command output by alternately entering the **no include-credentials** and **include-credentials** commands.

- After you permanently save security configurations to the current startup-config file using the **write memory** command, you can view and manage security settings with the following commands:
  - **show config**: Displays the configuration settings in the current startup-config file.
  - **copy config <source-filename> config <target-filename>**: Makes a local copy of an existing startup-config file by copying the contents of the startup-config file in one memory slot to a new startup-config file in another, empty memory slot.
  - **copy config tftp**: Uploads a configuration file from the switch to a TFTP server.
  - **copy tftp config**: Downloads a configuration file from a TFTP server to the switch.
  - **copy config xmodem**: Uploads a configuration file from the switch to an Xmodem host.
  - **copy xmodem config**: Downloads a configuration file from an Xmodem host to the switch.

For more information, refer to the “Switch Memory and Configuration” chapter in the *Management and Configuration Guide*.

- The switch supports the storage of up to three configuration files. Each configuration file contains its own security credentials and these security configurations may differ. It is the responsibility of the system administrator to ensure that the appropriate security credentials are contained in the configuration file that is loaded with each software image.
  - When you load a configuration file associated with a software release earlier than T.12.06 on a switch running software release T.12.06 or greater, all security credentials in the configuration file are supported.
  - When you load a configuration file associated with a software release T.12.06 or greater on a switch running a software release earlier than T.12.06, all security credentials saved with the **include-credentials** command are rejected as invalid configurations by the earlier software.
- If you have already enabled the storage of security credentials (including local manager and operator passwords) by entering the **include-credentials** command, the **Reset-on-clear** option is disabled. When you press the Clear button on the front panel, the manager and operator usernames and passwords are deleted from the running configuration. However, the switch does not reboot after the local passwords are erased. (The **reset-on-clear** option normally reboots the switch when you press the Clear button.)

For more information about the **Reset-on-clear** option and other front-panel security features, refer to the “Configuring Username and Password Security” chapter in the *Access Security Guide*.

- If you upgrade ProCurve software on a switch from an earlier software release to software release T.12.06 or greater and then enter the **include-credentials** command, security passwords are managed as follows:
  - The manager password (if any) in the earlier software version is copied into the running configuration. The other two configuration files, if configured, will not have a manager password configured.
  - The operator password (if any) in the earlier software version is copied into the running configuration. The other two configuration files, if configured, will not have an operator password configured.
  - No port-access password for 802.1X authentication is configured. The operator password in the earlier software version is not automatically copied as the new port-access password. To configure password access to the switch through 802.1X authentication, use the **password port-access** command as described in [“Password Command” on page 20](#). (It is not recommended that you use the same password for operator console access and for 802.1X port-access authentication.)
  - The SSH client public-keys for manager and operator access are copied from flash memory into the running configuration.
  - The RADIUS shared secret and TACACS+ encryption keys for access to authentication servers are already included in the running configuration.
  - SNMPv3 user credentials are already included in the running configuration.
- If you downgrade ProCurve software on a switch and use a software release earlier than T.12.06, security passwords are managed as follows:
  - Because SNMPv3 user credentials, RADIUS shared secret keys, and TACACS+ encryption keys are already included in the startup configuration, these security credentials are not lost. They continue to be used in the earlier software version.
  - The local manager and operator passwords are not recognized by an earlier software version and are not saved in the running configuration. However, passwords in inactive configuration files remain stored there. Although they are not displayed in **show config** command output, they are not automatically erased.
  - Although the hashed SSH client public-keys (for manager and operator access) are not recognized by an earlier software version, they remain stored so that they are immediately reloaded if you upgrade back to software release T.12.06 or greater.
  - As in a software upgrade, no port-access (operator) password for 802.1X authentication is saved from software release T.12.06 or greater.

## Restrictions

The following restrictions apply when you enable security credentials to be stored in the running configuration with the **include-credentials** command:

- The private keys of an SSH host cannot be stored in the running configuration. Only the public keys used to authenticate SSH clients can be stored. An SSH host's private key is only stored internally; for example, on the switch or on an SSH client device.
- SNMPv3 security credentials saved to a configuration file on a switch cannot be used after downloading the file on a different switch. The SNMPv3 security parameters in the file are only supported when loaded on the same switch for which they were configured.

The reason is that when SNMPv3 security credentials are saved to a configuration file, they are saved with the engine ID of the switch as shown here:

```
snmpv3 engine-id 00:00:00:0b:00:00:08:00:09:01:10:01
```

If you download a configuration file with saved SNMPv3 security credentials on a switch, when the switch loads the file with the current software version, the SNMPv3 engine ID value in the downloaded file must match the engine ID of the switch in order for the SNMPv3 users to be configured with the authentication and privacy passwords in the file. (To display the engine ID of a switch, enter the **show snmpv3 engine-id** command. To configure authentication and privacy passwords for SNMPv3 users, enter the **snmpv3 user** command.)

If the engine ID in the saved SNMPv3 security settings in a downloaded configuration file does not match the engine ID of the switch:

- The SNMPv3 users are configured, but without the authentication and privacy passwords. You must manually configure these passwords on the switch before the users can have SNMPv3 access with the privileges you want.
- Only the **snmpv3 user <user\_name>** credentials from the SNMPv3 settings in a downloaded configuration file are loaded on the switch; for example:

```
snmpv3 user boris  
snmpv3 user alan
```

- In software release T.12.06 and greater, you can store 802.1X authenticator (port-access) credentials in a configuration file. However, 802.1X supplicant credentials cannot be stored.
- In software release T.12.06 and greater, the local operator password configured with the **password** command is no longer accepted as an 802.1X authenticator credential. A new configuration command (**password port-access**) is introduced to configure the username and password used as 802.1X authentication credentials for access to the switch. You can store the **password port-access** values in the running configuration by using the **include-credentials** command.

Note that the **password port-access** values are configured separately from local operator username and passwords that are configured with the **password operator** command and used for management access to the switch. For more information about how to use the **password port-access** command to configure operator passwords and usernames for 802.1X authentication, refer to the “Configuring Port-Based and Client-Based Access Control (802.1X)” chapter in the *Access Security Guide*.

---

## Release T.12.07 Enhancements

The following enhancement is included in the T.12.07 release.

- **Enhancement (PR\_1000413764)** — System Location and Contact fields sizes increased.

---

## Release T.12.08 Enhancements

The following enhancements are included in the T.12.08 release.

- **Enhancement (PR\_1000419653)** — The **show vlan** command was enhanced to display separately each port in the VLAN, display the friendly port name, if configured, and display the VLAN mode for each port.

### **show vlan ports** CLI Command Enhancement

The **show vlan ports** command has been enhanced with an option (detailed) to display VLAN memberships on a per-port basis when a range of ports is specified in the command. In addition, user-specified port names will be displayed (if assigned), along with tagged or untagged membership modes.

#### **Displaying the VLAN Membership of One or More Ports**

This command shows VLAN memberships associated with a port or a group of ports.

**Syntax** show vlan ports < port-list > [detailed]

Displays VLAN information for an individual port or a group of ports, either cumulatively or on a detailed per-port basis.

**port-list:** Specify a single port number, a range of ports (for example, **a1-a16**), or **all**.

**detailed:** Displays detailed VLAN membership information on a per-port basis.

Descriptions of items displayed by the command are provided below.

**Port name:** The user-specified port name, if one has been assigned.

**VLAN ID:** The VLAN identification number, or VID.

**Name:** The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of **VLAN-x** where “x” matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of **GVRP\_x** where “x” matches the applicable VID.

**Status:**

**Port-Based:** Port-Based, static VLAN

**Protocol:** Protocol-Based, static VLAN

**Dynamic:** Port-Based, temporary VLAN learned through GVRP.

**Voice:** Indicates whether a (port-based) VLAN is configured as a voice VLAN.

**Jumbo:** *Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, refer to the chapter titled “Port Traffic Controls” in the Management and Configuration Guide for your switch.*

**Mode:** *Indicates whether a VLAN is tagged or untagged.*

The follow examples illustrate the displayed output depending on whether the **detailed** option is used.

```
ProCurve# show vlan ports a1-a33

Status and Counters - VLAN Information - for ports A1-A33

VLAN ID  Name                | Status      Voice Jumbo
-----  -
1         DEFAULT_VLAN          | Port-based  No   No
10        VLAN_10               | Port-based  Yes  No
20        VLAN_20               | Protocol    No   No
33        GVRP_33               | Dynamic     No   No

ProCurve#
```

**Figure 7. Example of “Show VLAN Ports” Cumulative Listing**

```
ProCurve# show vlan ports a1-a4 detailed

Status and Counters - VLAN Information - for ports A1

Port name: Voice_Port
VLAN ID  Name                | Status      Voice Jumbo Mode
-----  -
1        DEFAULT_VLAN          | Port-based  No   No   Untagged
10       VLAN_10                | Port-based  Yes  No   Tagged

Status and Counters - VLAN Information - for ports A2

Port name: Uplink_Port
VLAN ID  Name                | Status      Voice Jumbo Mode
-----  -
1        DEFAULT_VLAN          | Port-based  No   No   Untagged
20       VLAN_20                | Protocol   No   No   Tagged
33       GVRP_33              | Dynamic    No   No   Tagged

Status and Counters - VLAN Information - for ports A3

VLAN ID  Name                | Status      Voice Jumbo Mode
-----  -
1        DEFAULT_VLAN          | Port-based  No   No   Untagged

Status and Counters - VLAN Information - for ports A4

VLAN ID  Name                | Status      Voice Jumbo Mode
-----  -
1        DEFAULT_VLAN          | Port-based  No   No   Untagged

ProCurve#
```

Figure 1. Example of “Show VLAN Ports” Detailed Listing

- **Enhancement (PR\_1000423357)**— Passwords can be saved to the config file in plain text.

---

## Release T.12.09 Enhancements

The following enhancement is included in the T.12.09 release.

- **Enhancement (PR\_1000427592)** — Radius Accounting with Client IP attributes.

## RADIUS Accounting with IP Attribute

The IP address of the client is included in the RADIUS accounting packet sent by the switch to the RADIUS server. The client obtains the IP address through DHCP, so DHCP snooping must be enabled for the VLAN of which the client is a member.

---

## Release T.12.10 Enhancements

The following enhancement is included in the T.12.10 release.

- **Enhancement (PR\_1000428642)** — Switch now sends SNMP informs in addition to traps.

### Send SNMP v2c Informs

#### Enabling and Configuring SNMP Informs

You can use the **snmp-server informs** command (SNMPv2c and SNMPv3 versions) to send notifications when certain events occur. When an SNMP Manager receives an informs request, it can send an SNMP response back to the sending agent. This lets the agent know that the informs request reached its destination and that traps can be sent successfully to that destination.

Informs requests can be sent several times until a response is received from the SNMP manager or the configured retry limits are reached. The request may also timeout.

To enable SNMP informs, enter this command:

Syntax: **[no] snmp-server enable informs**

Enables or disables the informs option for SNMP.

Default: Disabled

To configure SNMP informs request options, use the following commands.

Syntax: **[no] snmp-server informs [retries<retries>] [timeout<seconds>] [pending <pending>]**

Allows you to configure options for SNMP informs requests.

**retries:** Maximum number of times to resend an informs request. Default: 3

**timeout:** Number of seconds to wait for an acknowledgement before resending the informs request. Default: 30 seconds

**pending:** *Maximum number of informs waiting for acknowledgement at any one time. When the maximum configured number is reached, older pending informs are discarded. Default: 25*

To specify the manager that receives the informs request, use the **snmp-server host** command.

Syntax: `snmp-server host < ip-address >[<traps | informs>] [version <1 | 2c | 3>]< community-string >`

Using community name and destination IP address, this command designates a destination network-management station for receiving SNMP event log messages from the switch. If you do not specify the event level, then the switch does not send event log messages as traps. You can specify up to 10 trap receivers (network management stations).

**Note:** *In all cases, the switch sends any threshold trap(s) or informs to the network management station(s) that explicitly set the threshold(s).*

[traps | informs>]

Select whether SNMP traps or informs are sent to this management station. For more information on SNMP informs, see [“Enabling and Configuring SNMP Informs” on page 35](#).

[version <1 | 2c | 3>]

Select the version of SNMP being used.

**Note:** SNMP informs are supported on version 2c or 3 only.

[<none | all | non-info | critical | debug>]

Options for sending switch Event Log messages to a trap receiver. The levels specified with these options apply only to Event Log messages, and not to threshold traps.

You can see if informs are enabled or disabled with the **show snmp-server** command as shown in Figure 8.

```
ProCurve(config)# show snmp-server
SNMP Communities
  Community Name      MIB View Write Access
  -----
  public              Manager  Unrestricted
Trap Receivers
  Link-Change Traps Enabled on Ports [All] : All
  Send Authentication Traps [No] : No
  [ Informs [Yes] : Yes ]
  [ ----- ]
  Address              | Community      Events Sent in Trap
  -----
--
Excluded MIBs

Snmp Response Pdu Source-IP Information
  Selection Policy    : Default rfc1517
Trap Pdu Source-IP Information
  Selection Policy    : Default rfc1517
```

**Figure 8. Example Showing SNMP Informs Option Enabled**

---

## Release T.12.11 Enhancements (Never released.)

The following enhancements are included in the T.12.11 release.

- **Enhancement (PR\_1000428213)** — RADIUS Server Unavailable Authentication. When the RADIUS server is unavailable, clients can be allowed access.

### RADIUS Server Unavailable

#### Overview

In certain situations, RADIUS servers can become isolated from the network. Users are not able to access the network resources configured with RADIUS access protection and are rejected. To address this situation, configuring the “**authorized**” secondary authentication method allows users unconditional access to the network when the primary authentication method fails because the RADIUS servers are unreachable.

## Enhancements

Release T.12.11 Enhancements (Never released.)

### Configuring RADIUS Authentication

You can configure the switch for RADIUS authentication through the following access methods:

- **Console:** Either direct serial-port connection or modem connection.
- **Telnet:** Inbound Telnet must be enabled (the default).
- **SSH:** To use RADIUS for SSH access, first configure the switch for SSH operation.
- **Web:** Enables RADIUS authentication for web browser interface access to the switch.

You can configure **radius** as the primary password authentication method for the above access methods. You also need to select either **local**, **none**, or **authorized** as a secondary, or backup, method..

Syntax: `aaa authentication < console | telnet | ssh | web > < enable | login > radius`

Configures RADIUS as the primary password authentication method for console, Telnet, SSH, and the web browser interface. (The default primary **< enable | login >** authentication is **local**.)

`[< local | none | authorized >]`

Provides options for secondary authentication (default: **none**).

---

### Caution

Configuring **authorized** as the secondary authentication method used when there is a failure accessing the RADIUS servers allows clients to access the network unconditionally. Use this method with care.

---

You can configure **local**, **chap-radius** or **eap-radius** as the primary password authentication method for the port-access method. You also need to select **none** or **authorized** as a secondary, or backup, method.

Syntax: `aaa authentication port-access <chap-radius | leap-radius | local>`

Configures **local**, **chap-radius**, or **eap-radius** as the primary password authentication method for port-access. The default primary authentication is **local**.

`[<none | authorized >]`

Provides options for secondary authentication. The **none** option specifies that a backup authentication method is not used. The **authorized** option allows access without authentication. (default: **none**).

You can configure **chap-radius** as the primary password authentication method for web-based or mac-based port-access methods. You also need to select **none or authorized** as a secondary, or backup, method.

Syntax: `aaa authentication <mac-based | web-based> chap-radius`

Configures **chap-radius** as the primary password authentication method for mac-based or web-based port access.

[<none | authorized >]

Provides options for secondary authentication. The **none** option specifies that a backup authentication method is not used. The **authorized** option allows access without authentication. (default: **none**).

Figure 1 shows an example of the **show authentication** command displaying **authorized** as the secondary authentication method for port-access, Web-auth access, and Mac-auth access. Since the configuration of **authorized** means no authentication will be performed and the client has unconditional access to the network, the “Enable Primary” and “Enable Secondary” fields are not applicable (N/A).

```
ProCurve(config)# show authentication

Status and Counters - Authentication Information

Login Attempts : 3
Respect Privilege : Disabled
```

Access Task	Login Primary	Login Secondary	Enable Primary	Enable Secondary
Console	Local	None	Local	None
Telnet	Local	None	Local	None
Port-Access	Local	Authorized	N/A	N/A
Webui	Local	None	Local	None
SSH	Local	None	Local	None
Web-Auth	ChapRadius	Authorized	N/A	N/A
MAC-Auth	ChapRadius	Authorized	N/A	N/A

The access methods with secondary authentication configured as **authorized** allows the client access to the network even if the RADIUS server is unreachable.

**Figure 9. Example of AAA Authentication Using Authorized for the Secondary Authentication Method**

### Specifying the MAC Address Format

The MAC address format command has been enhanced to allow upper-case letters to be used for the hexadecimal numbers when indicating the MAC address in RADIUS packets for MAC-based authentication.

Syntax: `aaa port-access mac-based addr-format <no-delimiter | single-dash | multi-dash | multi-colon | no-delimiter-uppercase | single-dash-uppercase | multi-dash-uppercase | multi-colon-uppercase>`

## Enhancements

Release T.12.12 Enhancements (Never released.)

Specifies the MAC address format to be used in the RADIUS request message. This format must match the format used to store the MAC addresses in the RADIUS server. (*Default: no-delimiter*)

**no-delimiter** — *specifies an aabbccddeeff format.*

**single-dash** — *specifies an aabbcc-ddeeff format.*

**multi-dash** — *specifies an aa-bb-cc-dd-ee-ff format.*

**multi-colon** — *specifies an aa:bb:cc:dd:ee:ff format.*

**no-delimiter-uppercase** — *specifies an AABCCDDEEFF format.*

**single-dash-uppercase** — *specifies an AABCC-DDEEFF format*

**multi-dash-uppercase** — *specifies an AA-BB-CC-DD-EE-FF format*

**multi-colon-uppercase** — *specifies an AA:BB:CC:DD:EE:FF format.*

For example, using the multi-colon-uppercase option, the MAC address would appear as follows:

AA:BB:CC:DD:EE:FF

- **Enhancement (PR\_1000438486)** — When using the **port-access mac-based** CLI command, the client MAC address can now be sent in upper or lowercase to the RADIUS server. New parameters are available to support this: **aaa port-access mac-based addr-format**.

---

## Release T.12.12 Enhancements (Never released.)

The following enhancements are included in the T.12.12 release.

- **Enhancement (PR\_1000374051)** — The switch is not seeing packets from an Avaya G700 PBX due to negotiation issues. The switch can now run at 100Mbps using the 1000Base-T Mini-GBIC (J8177B). The port containing the 1000Base-T Mini-GBIC can be configured with new speed options of "auto-100," "100-full," and "100-half." Setting these options will resolve negotiation issues.
- **Enhancement (PR\_1000443026)** — Support is added for the new C rev transceiver in the CLI **show tech**.

---

## Release T.12.40 Enhancements (Never released.)

*No new enhancements, software fixes only.*

## Release T.12.50 Enhancements

The following enhancements are included in the T.12.50 release.

- **Enhancement (PR\_1000456271)** — PC attached to telephone.

### Telephone Attached to PC Auth

#### Overview

This feature will allow a PC to connect with its RADIUS-assigned VLAN after an attached IP phone has authenticated on the authenticating port. Previously, when an IP phone and a PC were on the same authentication port, and the IP phone authenticated first, the IP phone's authentication caused the assigned, untagged VLAN of the port (usually the default statically-configured untagged VLAN) to be "locked down". When the PC tried to authenticate on that port after the phone had authenticated, and its RADIUS-assigned, untagged VLAN was different from the locked-down, untagged VLAN, authentication failed.

---

#### Note

The locked-down, untagged VLAN criteria priority when the first client authenticates is:

1. RADIUS-assigned VLAN
2. Configured, authorized VLAN
3. Statically configured, untagged VLAN

#### Allowing Authentication

In order for the PC to authenticate successfully after the phone has authenticated, it is necessary to prevent the port's untagged VLAN from being locked down by the phone's authentication. To accomplish this, the MAC address/VLAN information is not entered into the MAC address/VLAN port-security table when the phone authenticates. When the PC tries to authenticate, the port-security table is checked to see if any other clients are using the same untagged VLAN as is assigned to the PC. If the untagged VLAN is not in the port-security table, then no other clients are using it. The PC's RADIUS-assigned untagged VLAN is allowed to override the locked-down untagged VLAN of the port. Both the PC and the IP phone are authenticated on the port.

However, the port-security table may contain a MAC address/VLAN pair for the current untagged VLAN on the port if the switch received a BPDU from an authenticated MAC address on the untagged VLAN. The switch can distinguish BPDU traffic from other traffic and locks the VLAN down only if it receives non-BPDU traffic from the authenticated MAC address on the untagged VLAN.

## Enhancements

### Release T.12.51 Enhancements

Any additional clients authenticating after the PC authenticates are locked down to the same untagged VLAN used by the PC. The untagged VLAN for the port cannot change unless all clients currently active on the untagged VLAN deauthenticate.

### Supported Phones

Phones supported include those using:

- Dual stage DHCP
- Manual VLAN setting
- LLDP-MED auto-config

For Dual stage DHCP, the IP phone accesses the untagged default VLAN for a few seconds, and then does not access the untagged VLAN again until it reboots.

For manual VLAN settings or LLDP-MED autoconfig, the IP phone requires tagged VLANs.

---

### Note

For Dual stage DHCP, a PC with a dynamically-assigned VLAN may fail temporarily while the phone is accessing the untagged VLAN, but it will succeed as soon as the phone accesses the tagged VLAN.

- **Enhancement (PR\_10004570598)** — An improved version of the MSTP-VLAN mapping enhancement referenced in PR\_1000457691 was added. This enhancement allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch.

---

## Release T.12.51 Enhancements

*No new enhancements, software fixes only.*

---

## Release T.12.52 Enhancements

*No new enhancements, software fixes only.*

# Software Fixes in Release T.11.10 - T.12.52

---

Software fixes are listed in chronological order, oldest to newest. To review the list of fixes included since the last general release that was published, go to [“Release T.12.07” on page 49](#).

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

Release T.11.01 was the first production software release for the ProCurve 2900 Series switches.

Releases T.11.02 through T.11.09 were never built.

Release T.11.13 is the last release of the T.11.xx software. The switch 2900 series software code was rolled to the T.12.01 code branch with no intervening releases.

---

## Release T.11.10

The following problems were resolved in release T.11.10 (never released)

- **802.1X (PR\_1000359976)** — Changed the maximum number of 802.1X users to 8.
- **802.1x (PR\_1000358534)** — For the Controlled Directions feature of 802.1X to operate correctly, spanning tree must be enabled and authenticator ports must be set as edge ports.
- **CLI (PR\_1000345301)** — The output from the "show config state" CLI command doesn't always report changes made to the configuration.
- **Crash (PR\_1000346971)** — When stacking is disabled, the switch may crash with a message similar to:

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack Frame=0x08895e48  
HW Addr=0x39200000 IP=0x007132f8 Task='mSnmprCtrl'
```
- **Crash (PR\_1000357083)** — The switch may crash with a message similar to:

```
Software exception at ngDmaTx.c:722 -- in 'tDevPollTx', task ID = 0x4305c504  
-> HW DMA DRIVER unable.
```
- **Enhancement (PR\_1000358903)** — 802.1X Controlled Directions enhancement. With this enhancement, administrators can use “Wake-on-LAN” with computers that are connected to ports configured for 802.1X authentication. No further information on using this feature is available at this time.
- **Enhancement (PR\_1000351445)** — The "show tech transceiver" CLI command output now contains the HP part number and revision information for all transceivers on the switch.
- **Hang (PR\_1000359640)** — Switch hangs on initialization and becomes unresponsive.

## Software Fixes in Release T.11.10 - T.12.52

### Release T.11.11

- **Management VLAN (PR\_1000299387)** — The management VLAN does not allow connectivity from valid IP addresses.
- **SNMP (PR\_1000358129)** — The command line interface (CLI) becomes unresponsive after running RMON traps code.
- **sFlow (PR\_1000361604)** — Changed the maximum sFlow skipcount to 24 bits.

## Release T.11.11

The following problems were resolved in release T.11.11

- **802.1X (PR\_1000367404)** — CLI allows configuration of more 802.1X users per port than the eight per port supported by the switch.

## Release T.11.12

The following problems were resolved in release T.11.12

- **802.1p QoS (PR\_1000368188)** — 802.1p prioritization may not work once a trunk is enabled on a module, unless the user issues the commands "qos type-of service ip-precedence" or "qos type-of service diff-services".
- **ACL (PR\_1000368901)** — Outbound access control lists (ACLs) do not function after a reboot.
- **Authorization (PR\_1000365285)** — IP Authorized Managers behaves incorrectly with regard to telnet access.
- **CLI (PR\_1000313916)** — The CLI output for the "show ip" command is misaligned; the proxy-arp column is shifted over to the left by one.
- **CLI (PR\_1000368900)** — VLAN names over 12 characters in length cause "show ip route" to be displayed incorrectly.
- **Crash (PR\_1000356446)** — When traffic monitoring is in use, the switch may crash with a message similar to this.

```
Data Bus Error: Addr=0x704a6114 Data=0x00000011 flags=0x10000751,
IP=0x4012eaac Task='mEaseUpdt' TaskID=0x42fef338
```

- **Crash (PR\_1000368540)** — The switch may crash with a message similar to:

```
Software exception at parser.c:8012 -- in 'mSess2', task ID = 0x90e10e0
-> ASSERT: failed.
```

- **Crash (PR\_1000372604)** — When multiple of instances of sFlow have been configured via the CLI, the switch may crash with an error similar to:  

```
Software exception at sflow.c:1170 -- in 'mEaseCtrl', task ID =  
0x80e5fe0-> ASSERT: failed.
```
- **Menu/Event Log (PR\_1000319407)** — Disabling of event log numbers, via the "no log-numbers" CLI command, doesn't work properly when viewing the event log via the Menu. Using the 'next' and 'prev' buttons causes the log numbers to reappear.
- **Routing (PR\_1000350144)** — Adding a VLAN and assigning an IP address to that VLAN through the menu interface takes routing information protocol (RIP) offline in all VLANs.
- **RADIUS (PR\_1000358525)** — Attributes that were overridden by RADIUS (CoS, Rate, and ACL) remain active if an authenticated user fails to send EAP-LOGOFF.
- **sFlow (PR\_1000361604)** — Changed the maximum sFlow skipcount to 24 bits.
- **Traffic Monitoring/Performance Degradation (PR\_1000370061)** — The switch is affected by ProCurve Manager (PCM) traffic monitoring, causing throughput degradation.
- **VLAN (PR\_1000356062)** — When configuring from the menu interface, the 3500yl series switches will not allow the following name format for a new VLAN: "VLANx" (where "x" is a VLAN number).

## Release T.11.13

The following problems were resolved in release T.11.13 (not a general release)

- **CLI (PR\_1000377318)** — The output from the CLI command, 'show dhcp-relay' is truncated.
- **CLI (PR\_1000379455)** — The output from some CLI "show" commands produces incorrectly formatted output on the screen.
- **Enhancement (PR\_1000376406)** — Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.
- **Enhancement (PR\_1000379804)** — Historical information about MAC addresses that have been moved has been added to the "show tech" command output.
- **Event Log (PR\_1000373796)** — Selecting "Save", within the IP Configuration screen of the Menu causes unnecessary Event Log messages.
- **Menu/Counters (PR\_1000370619)** — The Menu Interface does not reflect changes to SNMP OIDs for "IP Mgmt - Tx/Rx" counters; the counter always reads "0."

## Software Fixes in Release T.11.10 - T.12.52

### Release T.12.01

- **sFlow/Flow-Control (PR\_1000375851)** — To protect performance, egress sFlow sampling will be disabled on all ports if Flow-Control is enabled on any one or more ports, and a CLI/Event Log message will be generated.
- **Syslog (PR\_1000379802)** — Forwarding of event log messages to a configured syslog server is not disabled when a specific event log message has been disabled via MIB.
- **Web/RADIUS (PR\_1000368520)** — Web Authentication does not authenticate clients due to a failure to send RADIUS requests to the configured server.

## Release T.12.01

The following problems were resolved in release T.12.01

- **CLI (PR\_1000332352)** — The output of a "show int brief" command should show the negotiated flow control status rather than the flow control configuration setting.
- **Crash (PR\_1000378804)** — The switch may crash when the maximum number of QoS rules is exceeded.
- **Crash (PR\_1000392105)** — Specific actions in the port status screen of the menu interface may trigger a crash. Scrolling down to the ports on a module in slot L and pressing [enter] may cause the switch to crash with a message similar to:

```
Software exception at exception.c:424 -- in 'mSess1', task ID =
0x8dd1ab0 -> Memory system error at 0x881a480 - memPartFree
```
- **Enhancement (PR\_1000373226)** — Support was added for the J9054B 100-FX SFP-LC transceiver.
- **Enhancement (PR\_1000298920)** — A ping request issued to a VLAN which is down will now return a more specific message; instead of "request timed out," the message "The destination address is unreachable" will be displayed.
- **Enhancement (PR\_1000376626)** — Enhance CLI "qos dscp-map he" help and "show dscp-map" text to warn the user that inbound classification based on DSCP codepoints only occurs if "qos type-of-service diff-services" is also configured.
- **Routing (PR\_1000359162)** — When the user configures a static route that overlaps with a local subnet configured on the switch, the router will not respond to packets destined for its own IP address. The packets for its own IP address will be routed using the configured static route.

## Release T.12.02

The following problems were resolved in release T.12.02

- **CLI (PR\_1000373443)** — The CLI **update** command help text and confirmation message is misleading and confusing.
- **Crash (PR\_1000398746)** — The switch may crash with the task "swInitTask". This could result in repeated crashes until the switch configuration is cleared.
- **Crash/Traffic Monitoring (PR\_1000396662)** — When Traffic Monitoring is enabled on the switch by a network management station (such as PCM) the switch may crash with a message similar to:

```
Data Bus Error: Addr=0x704a613c Data=0xffffffff flags=0x10000750,  
IP=0x4012fa80 Task='tSvcWorkQ' TaskID=0x44b42ad0 cpsr=0x80000013
```

- **Crash (PR\_1000392863)** — Switch may crash when "setmib tcpConnState" is used, with a message similar to:

```
NMI event SW:IP=0x0079f4a0 MSR:0x00029210 LR:0x006dca60  
Task='eTelnetd' Task ID=0x8a7cbb0 cr: 0x20000042 sp:0x08a7c871
```

- **Crash (PR\_1000399448)** — Changes to traffic monitoring settings may trigger the switch to crash with a message similar to:

```
Software exception at ease_ctrl.c:575 -- in 'mEaseCtrl', task ID =  
0x8347160
```

- **Daylight Savings (PR\_1000364740)** — Due to the passage of the Energy Policy Act of 2005, Pub. L. no. 109-58, 119 Stat 594 (2005), starting in March 2007 daylight time in the United States will begin on the second Sunday in March and end on the first Sunday in November.
- **DHCP (PR\_1000397753)** — A unicast DHCP request that has already been relayed by another router is sometimes dropped.
- **Hang (PR\_1000397964)** — The switch appears to hang where all routing stops, the switch cannot ping anything, even addresses configured locally.
- **Enhancement (PR\_1000379804)** — Historical information about MAC addresses that have been moved has been added to the **show tech** command output.
- **Proxy-ARP (PR\_1000393571)** — Proxy-ARP sends responses to gratuitous ARPs.
- **RIP (PR\_1000393366)** — The switch does not process RIP (v2) responses containing subnets with a classful subnet mask, when the receiving RIP switch has a connected VLSM network defined that would fall within that classful range.

## Release T.12.03

The following problems were resolved in release T.12.03 (never released).

- **Enhancement (PR\_1000404544)** — Provides TCP/UDP port range prioritization in the **qos** command; the **range** option assigns an 802.1p priority to (IPv4) TCP or UDP packets associated with a range of TCP/UDP ports. For more information, see [“Release T.12.07 Enhancements” on page 32](#).
- **Enhancement (PR\_1000398393)** — For the **interface <port-list> speed-duplex** command, added the **auto-10-100** configuration option to constrain a link to 10/100 Mbps speed and allow a more rapid linkup process when 1000 Mbps operation is not possible.

## Release T.12.04

The following problems were resolved in release T.12.04 (never released).

- **ACL (PR\_1000395595)** — Removing a VLAN via SNMP does not remove the related ACL relationship to that VLAN.
- **ACL (PR\_1000402901)** — The ACL resequencing feature may discard some ACEs in a random fashion.
- **BootROM (PR\_1000402707)** — BootROM does not upgrade to latest version when upgrading code to primary flash.
- **CLI (PR\_1000403104)** — Executing the **erase startup-configuration** command and rebooting does not clean up the RMON 'alarm' table.
- **Crash (PR\_1000405465)** — Use of dynamically assigned ACLs may cause the switch to reboot with the following error:

```
Software exception at aclBttfMUtils.c:1208 -- in 'midmCtrl',
task ID = 0x85f6a60 -> internal error
```
- **MSTP (PR\_1000369492)** — Update of MSTP implementation to the latest IEEE P802.1Q-REV/D5.0 specifications to stay in sync with the protocol evolution.
- **sFlow (PR\_1000408145)** — sFlow samples for routed packets do not occur bidirectionally; inbound packets are dropped and only outbound packets are sampled.
- **Traceroute (PR\_1000379199)** — The reported **traceroute** time is inaccurate; it is one decimal place off.

## Release T.12.05

The following problems were resolved in release T.12.05 (never released).

- **Enhancement (PR\_1000408960)** — RADIUS-Assigned GVRP VLANs. For more information, see [“Release T.12.05 Enhancements” on page 11](#).
- **Menu (PR\_1000392862)** — The menu will allow invalid values (greater than 720 sec) to be entered for the SNMP poll interval.

## Release T.12.06

The following problems were resolved in release T.12.06.

- **Config (PR\_1000410790)** — Errors are returned when applying the **interface <port-list> speed-duplex auto-10-100** command to interfaces 45-48.
- **Config (PR\_1000405639)** — Various characters in configuration file names (including dash, ampersand, plus, and spaces within quotes) result in truncated names after reboot. This is not just a display issue; the command **erase configs <filename>** does not remove a file containing the problem characters.
- **Crash (PR\_1000410758)** — When the **interface <port-list> speed-duplex auto-10-100** command is issued on a range of ports, the switch may crash with a message similar to:  

```
NMI event HW:IP=0x0083f224 MSR:0x00029210 LR:0x0033c3c4
Task='tDevPollRx' Task ID=0x9137e50 cr: 0x20000022
sp:0x09137d78 xer:0x20000000
```
- **RIP (PR\_1000377789)** — RIP restrict filters are not working upon reboot.
- **RMON (PR\_1000410885)** — RMON alarms/thresholds set via SNMP are cleared after a reboot.
- **Enhancement (PR\_1000308332)** — Passwords (hashed) can be saved to the configuration file.

## Release T.12.07

The following problems were resolved in release T.12.07.

- **CLI (PR\_1000411450)** — When **show tech all** is executed, the command will only provide partial output.
- **Enhancement (PR\_1000413764)** — System Location and Contact fields sizes increased.

## Software Fixes in Release T.11.10 - T.12.52

### Release T.12.08

- **Crash (PR\_1000385844)** — With sFlow sampling enabled, the switch may crash with a message similar to:  

```
Software exception at ngDmaTx.c:729 - in 'tDevPollTx', task ID = 0x4305bba8 -> HW DMA DRIVER unable to transmit anymore
```
- **SNMP (PR\_1000374893)** — When retrieving the switch serial number via SNMP, the management module serial number is returned instead of the chassis serial number.

## Release T.12.08

The following problems were resolved in release T.12.08.

- **Crash (PR\_1000421322)** — When issuing config-related CLI commands (such as **show run** or **show tech**) or when PCM attempts to retrieve the configuration file via TFTP from a switch having a large configuration file, the switch may crash with a message similar to:  

```
Software exception at exception.c:373 - in 'tTftpDmn', task ID = 0x11cfaa8 -> Memory system error at 0x1175550 - memPartFree
```
- **Enhancement (PR\_1000419653)** — The **show vlan** command was enhanced to display separately each port in the VLAN, display the friendly port name, if configured, and display the VLAN mode for each port.
- **ARP (PR\_1000414347)** — The ARP table address learning is slow. Once the switch has its ARP table cleared, the clients will be unable to communicate for approximately 30 seconds.
- **Config (PR\_1000416508)** — The user cannot create an alternate startup-config file. Although **sho config files** shows an available slot, the switch does not allow copying from an existing config file to create a new config file in the vacant slot.
- **SNMP (PR\_1000422129)** — HP Fault Finder does not send the interface index with the SNMP trap, even though it is listed in the system log.
- **Enhancement (PR\_1000423357)** — Passwords can be saved to the config file in plain text.
- **Link LED (PR\_1000425143)** — Mini-GBIC link LED does not work after a mini-GBIC is hot-swapped.
- **Crash (PR\_1000420709)** — When entering a backslash at the CLI, the switch may crash with a message similar to:  

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack  
Frame=0x08e66508 HW Addr=0x00b4f2ac IP=0x0018a864 Task='mSess1' Task  
ID=0x8e67170 fp: 0x3be00000 sp:
```

## Release T.12.09

The following problems were resolved in release T.12.09.

- **Authentication (PR\_1000422933)** — The local password authentication grants access to an empty password.
- **Enhancement (PR\_1000427592)** — Radius Accounting with Client IP attributes.
- **Crash (PR\_1000407238)** — When the startup config is different than the running config, use of the **show config** command may cause the switch to crash.
- **SNMP (PR\_1000406398)** — The URL embedded SNMP traps are sent as plain text when SSL is enabled. This may result in the trap receiver or PCM not being able to display the URL.
- **Crash (PR\_1000427674)** — The switch may crash with a message similar to:  

```
Slot A ACL Int status=0x10000000 28=0x800016b2 : Task=tDevPollRx Task  
ID=0x4305c9b8 IP=0x401ab590
```

## Release T.12.10

The following problems were resolved in release T.12.10.

- **Crash (PR\_1000428582)** — Typing non-alphanumeric characters at the CLI prompt may cause the switch to crash with a message similar to:  

```
PPC Data Storage (Bus Error) exception vector 0x300:Stack  
Frame=0x08e36878 HW Addr=0x00b4f2ec IP=0x0018a974 Task='mSess1' Task  
ID=0x0fp: 0x18020800 sp:
```
- **Enhancement (PR\_1000428642)** — Switch now sends SNMP informs in addition to traps.
- **STP (PR\_1000420442)** — The configuration of spanning tree parameters for a given port in a trunk (LAG) results in the switch rejecting the TFTP transfer of the configuration as corrupt.
- **CLI (PR\_1000429474)** — The **all** option is missing from **password** command.
- **Radius (PR\_1000432556)** — The Framed-IP-Address attribute is not added to RADIUS accounting packets.

## Release T.12.11 (Never released.)

The following problems were resolved in build T.12.11.

- **CLI (PR\_1000419379)** — Interface command is missing under the VLAN context.

**Software Fixes in Release T.11.10 - T.12.52**  
Release T.12.12 (Never released.)

- **Crash (PR\_1000428582)** — Typing non-alphanumeric characters at the CLI prompt may cause the switch to crash with a message similar to:  

```
PPC Data Storage (Bus Error) exception vector 0x300:Stack  
Frame=0x08e36878 HW Addr=0x00b4f2ec IP=0x0018a974 Task='mSess1' Task  
ID=0x0fp: 0x18020800 sp:
```
- **Hang (PR\_1000434809)** — The switch can hang, causing all of the port LEDs to remain lit and the ports to stop transmitting traffic.
- **Enhancement (PR\_1000428213)** — RADIUS Server Unavailable Authentication. When the RADIUS server is unavailable, clients can be allowed access.
- **Crash (PR\_1000436274)** — Typing a question mark (?) at the multi-line input prompt (>) may cause the switch to crash.
- **CLI (PR\_1000433948)** — If using AAA Radius, **show tech** fails at **show tech buffer** command.
- **Enhancement (PR\_1000438015)** — The banner MOTD size is increased.
- **CLI (PR\_1000431350)** — The **port-utilization** option is missing from the **show interface** CLI command string.
- **ACL (PR\_1000432563)** — ACLs with "permit" on L4 ports and using operators 'gt'/'lt'/'range' do not function as expected. The ACL does not drop traffic with un-permitted L4 ports. Instead, all traffic with any L4 ports are forwarded.
- **Enhancement (PR\_1000438486)** — When using the **port-access mac-based** CLI command, the client MAC address can now be sent in upper or lowercase to the RADIUS server. New parameters are available to support this: **aaa port-access mac-based addr-format**.

## Release T.12.12 (Never released.)

The following problems were resolved in release T.12.12.

- **CLI (PR\_1000342461)** — The command **show lldp info remote <port number>** reports incorrect information for remote management address.
- **Enhancement (PR\_1000374051)** — The switch is not seeing packets from an Avaya G700 PBX due to negotiation issues. The switch can now run at 100Mbps using the 1000Base-T Mini-GBIC (J8177B). The port containing the 1000Base-T Mini-GBIC can be configured with new speed options of "auto-100," "100-full," and "100-half." Setting these options will resolve negotiation issues.
- **Crash (PR\_1000434888)** — A switch module may crash with a message similar to:  

```
ACL Int status=0x10000000 28=0x80002f3a : Task=tDevPollTx Task  
ID=0x4305c504 IP=0x400693e8.
```

- **Routing (PR\_1000432449)** — If the switch is configured with port-security and routing, a physical port transition on the host may prevent the switch from transmitting routed traffic to that host.
- **Enhancement (PR\_1000443026)** — Support is added for the new C rev transceiver in the CLI **show tech**.
- **Crash (PR\_1000415534)** — While running the **lockout-mac** CLI command, the switch may crash with a message similar to:  

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack  
Frame=0x0ab9a738 HW Addr=0x00b3f104 IP=0x00801d2c Task='eDrvPoll' Task  
ID=0xab9ad20 fp: 0x0f3808c0 sp
```

## Release T.12.13

The following problems were resolved in release T.12.13.

- **AAA/CLI (PR\_1000445886)** — The syntax changed for **aaa authentication <port-access | mac-based | web-based>** commands to remove login keyword.
- **Broadcast-limit (PR\_1000429594)** — The broadcast-limit feature incorrectly limits multicast traffic.
- **MSTP (PR\_1000439775)** — The switch generates a topology change when a port goes off-line and MSTP is enabled and all ports are auto-edge-ports.
- **Crash (PR\_1000444112)** — Downloading a config file to the switch may cause the switch to crash with a message similar to:  

```
Software exception at cli_config_action.c:5479 - in 'mftTask'
```
- **SNMP (PR\_1000448463)** — The SNMP Engine ID Discovery is broken causing SNMPv3 functionality to fail.

## Release T.12.40 (Never released.)

The following problems were resolved in build T.12.40. (Never released.)

- **STP (PR\_1000449365)** — ARP & MAC tables get out of sync after a spanning tree (MSTP or RSTP) re-convergence. An ARP entry fails to be associated to the port even though the MAC entry exists. This may result in an unexpected ping failure.
- **SSH (PR\_1000453226)** — Configuration of SSH login to the manager mode (**aaa authentication ssh enable public-key <enter>**) triggers an error “Not legal combination of authentication methods,” but it should be a valid command syntax.

**Software Fixes in Release T.11.10 - T.12.52**  
Release T.12.50

- **SNMP (PR\_1000389902)** — The switch is not sending an "embedded URL" within the SNMP trap for an FFI event to the PCM server monitoring traps. The embedded URL, if sent, would allow someone looking at the log event on the PCM server to simply click on the URL and be immediately connected to the switch.
- **SNMP (PR\_1000444744)** — An SNMP set of **hpicfDot1xPaePortauth** or an SNMP set **hpicfDot1xPaePortSupp** of an invalid value may cause the switch to crash with a message similar to the following:  

```
ASSERT at aaa8021x_dyn_reconfig.c.
```
- **SSH (PR\_1000461002)** — Issue with authentication when SSH is configured.
- **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 auth RADIUS VLAN assignment.
- **Crash (PR\_1000456340)** — Switch may crash with a message similar to:  

```
No message buffers: alloc_free.c:435.
```
- **Telnet hang (PR\_1000457765)** — If **Ctrl+S** is typed and then the telnet window is closed, the telnet session may become unresponsive and fail to reset by the **kill** command issued at the console prompt. This may require the switch to be reloaded to become active again.
- **CLI (PR\_1000417447)** — Some of the instrumentation monitoring parameters (e.g. arp reply monitoring) are not functioning.

## Release T.12.50

The following problems were resolved in release T.12.50.

- **Enhancement (PR\_1000456271)** — PC attached to telephone.
- **Enhancement (PR\_10004570598)** — An improved version of the MSTP-VLAN mapping enhancement referenced in PR\_1000457691 was added. This enhancement allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch.
- **Routing (PR\_1000424308)** — A static route that points to a deleted VLAN may cause other routing table errors.
- **CLI (PR\_1000473468)** — Removing a VLAN range from an MSTP instance (e.g., no spanning-tree instance 2 VLAN 10-20) fails to delete the VLANs. Listing individually the VLANs desired for deletion will correctly remove the VLANs.

## Release T.12.51

The following problems were resolved in release T.12.51.

- **Crash (PR\_1000472846)** — Rebooting the switch with an active Telnet session and while remote mirroring is in use may cause the switch to crash with a message similar to the following. There may also be other, unknown triggers that cause this crash.

```
0x4001bf18 in fatal_exception (file=0x400a8b8c "ngDmaRx.c", line=1413,  
errorcode=256, str=0x400a8b7c "ASSERT: failed.")
```

- **xSTP (PR\_1000715227)** — When there is no module and transceiver inserted in the target slot, attempts to set up a unique path cost on the transceiver port results in an "invalid input" error.

- **TFTP (PR\_1000427390)** — When the configuration of a 6200yl switch is copied to a TFTP server, the config shows a line with the following description: module 1 type JFIXME. If that line is removed from the config and then the config is transferred back to the switch, the transfer will fail with the switch reporting, "corrupted config." This fix results in the fixed switch ports being described as: module 1 type J8992A.

- **Crash (PR\_1000716461)** — Loading a configuration file that uses up all the ACL resources may cause the switch to crash with a message similar to:

```
NMI event SW: IP=0x007c755c MSR: 0x00029210 LR: 0x007c7544  
Task= 'mftTask' Task ID=0x8a60920cr: 0x24024442 sp: 0x08a5f850 xer:  
0x20000000
```

- **Link Speed (PR\_1000432419)** — Ports 1-24 on the ProCurve 2900 24G and ports 25-48 on the ProCurve 2900 24G switches may link at 10/100 speeds rather than the gigabit speed that they support.

- **TFTP (PR\_1000419582)** — The switch CLI counter displays the wrong size of the file being transferred when uploading from switch flash to TFTP server. The file that is actually transferred is the correct size. This CLI display is in error.

- **CLI (PR\_1000447529)** — The CLI output of the command **show rate-limit all** is corrupted.

- **Manufacturing (PR\_1000740632)** — Upon reload, the manufacturing information is zeroed out.

- **CLI (PR\_1000340826)** — The CLI output from a **show interface** command truncates counters that have large values.

- **CLI (PR\_1000742974)** — The CLI had some initial limitations within the interface context for configuration of uninserted modules and transceivers. This fix addresses the interface context for spanning-tree, aaa port-access, DHCP snooping, loop protection and several other features.

## Release T.12.52

The following problems were resolved in release T.12.52.

- **Daylight Savings Time (PR\_1000467724)** — This change corrects the schedule for Western Europe Time Zone: DST to start the last Sunday in March and DST to end the last Sunday in October.
- **SSH/SCP (PR\_1000742969)** — The following issues with using SSH/SCP were fixed.
  1. In show ip ssh, sessions 3 & 4 may display "console" instead of "inactive," when those sessions are not in use.
  2. The switch does not send an appropriate exit-status message to the client. This corrects the symptom that occurs in some applications, which reports a message similar to:  

```
Fatal error: Server unexpectedly closed connection.
```
  3. The SSH client application does not get a command prompt (or equivalent) back from the switch until the OS is verified and burned to flash.
  4. The show flash command incorrectly shows an OS image present in flash before the OS has completely copied to flash.
- **Routing (PR\_1000744325)** — When a PC is using the switch as its default gateway, and that switch is set with a default route to another device on the same VLAN, duplication of packets may occur. Symptoms may include seeing TCP packets out of order due to retransmission.
- **802.1X (PR\_1000741874)** — Entering invalid 802.1X credentials (triggering failed authentication) and then trying again with valid credentials may cause the switch may crash with a message similar to the following. Symptoms and triggers for this problem may vary.  

```
Software exception at aaa8021x_util.c:2290 -- in 'm8021xCtrl', task ID = 0x85db0 -> ASSERT: failed.
```
- **Web GUI (PR\_1000472572)** — Unable to configure port mirroring via web browser interface.
- **IP Helper Address (PR\_1000751623)** — If the IP address on a VLAN interface is changed, any previously configured IP Helper address stops working.
- **CLI (PR\_1000455370)** — Commands that display portmaps may have corrupted output.
- **RIP (PR\_1000751858)** — Some static routes may not be correctly distributed by RIPv1 or RIPv2.
- **Crash (PR\_1000759046)** — Using the "\" character along with other character combinations may cause the switch to crash with a message similar to:  

```
Software exception at parser.c:2653 -- in 'mSess1', task ID = 0x898e6a0-> ASSERT: failed
```
- **Protocol Starvation (PR\_1000758853)** — Write to flash causes BPDU protocol starvation.

- **Enhancement (PR\_1000308332)**— Passwords (hashed) can be saved to the configuration file. For more information, see [“Release T.12.06 Enhancements”](#) on page 17.



© 2006-2008

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

January 2008

Manual Part Number

5991-4790 Edition 2