

## Release Notes:

### Version T.13.71 Software

*for the ProCurve Series 2900 Switches*

---

The T.13.71 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 17](#))
- A listing of software enhancements in recent releases ([page 21](#))
- A listing of software fixes included in releases T.11.10 through T.13.71 ([page 61](#))
- Support Notes, Known and Open Issues for updates from T.11.10 through T.13.71 ([page 16](#))

---

### Support Notices:

**CAUTION - Updating to Version T.13.xx:** . It is important that you update to T.13.xx from a configuration that has not been previously converted from a pre-T.13.xx format and subsequently rolled back to T.12.xx. If you have updated to T.13.xx and rolled back to T.12.xx to workaround an issue, you should load a saved T.12.xx configuration to the switch and boot to it prior to updating to T.13 again. Archive Pre-T.13.xx configuration files before updating! A configuration file saved under version T.13.xx software is not backwards-compatible with previous software versions. Please see “[Best Practices for Major Software Updates](#)” on [page 6](#) in the Release Notes for more information.

**BootROM Update!** All ProCurve 2900 Series Switches running T.12.50 system software or earlier will have the BootROM updated to K.12.12 by this new version of system software. Following the file copy to the switch flash and initiation of the reload, no additional user intervention is needed. **Do not interrupt power to the switch during this important update.**

**Related Publications.** For the latest version of any of the publications listed below, visit the ProCurve Networking Web site at [//www.procurve.com/manuals](http://www.procurve.com/manuals).

---

© Copyright 2006-2009 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

## Publication Number

5991-4790  
October 2009

## 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
Best Practices for Major Software Updates	6
Updating the Switch: Overview	6
Updating the Switch: Detailed Steps	7
Rolling Back Switch Software	11
Viewing or Transferring Alternate Configuration Files	12
HP ProCurve Switch, Routing Switch, and Router Software Keys	14
OS/Web/Java Compatibility Table	15
Minimum Software Versions	15
<b>Support Notes</b>	<b>16</b>
<b>Clarifications</b>	<b>17</b>
<b>Known Issues</b>	<b>18</b>
Release T.13.63	18
Release T.13.08	18
Release T.13.03	19
<b>Enhancements</b>	<b>21</b>
Release T.11.10 through T.11.12 Enhancements	21
Release T.11.13 Enhancements	21
Release T.12.01 Enhancements	21
Advanced Traffic Management Guide	21
Management and Configuration Guide	22
Multicast and Routing Guide	22

Security Guide .....	22
Release T.12.02 Enhancements .....	23
Release T.12.03 Enhancements .....	23
Release T.12.04 Enhancements .....	24
Release T.12.05 Enhancements .....	24
How RADIUS-Based Authentication Affects VLAN Operation .....	24
Release T.12.06 Enhancements .....	30
Saving Security Credentials in a Configuration File .....	30
Release T.12.07 Enhancements .....	45
Release T.12.08 Enhancements .....	45
show vlan ports CLI Command Enhancement .....	45
Release T.12.09 Enhancements .....	47
RADIUS Accounting with IP Attribute .....	48
Release T.12.10 Enhancements .....	48
Send SNMP v2c Informs .....	48
Release T.12.11 Enhancements (Never released.) .....	50
Release T.12.12 Enhancements (Never released.) .....	50
Release T.12.40 Enhancements (Never released.) .....	51
Release T.12.50 Enhancements .....	51
Release T.12.51 Enhancements .....	51
Release T.12.52 Enhancements .....	51
Release T.13.02 Enhancements .....	51
Release T.13.03 through T.13.04 Enhancements .....	53
Release T.13.05 Enhancements .....	53
Copy TFTP Command with Show Tech Option .....	53
Release T.13.06 through T.13.14 Enhancements .....	54
Release T.13.15 Enhancements .....	54
Console/Telnet Inactivity Timer .....	54
Release T.13.16 Enhancements .....	55
Release T.13.17 Enhancements .....	55
Release T.13.18 Enhancements .....	55
Release T.13.19 through T.13.23 Enhancements .....	56

Release T.13.24 through T.13.26 Enhancements .....	56
Release T.13.27 through T.13.44 Enhancements .....	56
Release T.13.45 Enhancements .....	56
Release T.13.46 through T.13.56 Enhancements .....	56
Release T.13.57 Enhancements .....	56
Release T.13.58 through T.13.59 Enhancements .....	56
Release T.13.60 Enhancements .....	57
Release T.13.61 through T.13.62 Enhancements .....	57
Release T.13.63 Enhancements .....	57
Release T.13.64 Enhancements .....	57
Release T.13.65 Enhancements .....	57
Release T.13.66 Enhancements .....	57
Release T.13.67 Enhancements .....	57
Release T.13.68 Enhancements .....	57
Release T.13.69 Enhancements (Never released.) .....	57
Release T.13.70 Enhancements (Never built.) .....	58
Release T.13.71 Enhancements .....	58
Access Control Debug Logging .....	58

## **Software Fixes in Release T.11.10 - T.13.71 .....61**

Release T.11.10 .....	61
Release T.11.11 .....	62
Release T.11.12 .....	62
Release T.11.13 .....	63
Release T.12.01 .....	64
Release T.12.02 .....	65
Release T.12.03 .....	66
Release T.12.04 .....	66
Release T.12.05 .....	66
Release T.12.06 .....	66
Release T.12.07 .....	67
Release T.12.08 .....	67

Release T.12.09 .....	68
Release T.12.10 .....	69
Release T.12.11 (Never released.) .....	69
Release T.12.12 (Never released.) .....	70
Release T.12.13 .....	70
Release T.12.40 (Never released.) .....	71
Release T.12.50 .....	72
Release T.12.51 .....	72
Release T.12.52 .....	73
Release T.13.02 .....	74
Release T.13.03 .....	75
Release T.13.04 .....	75
Release T.13.05 .....	75
Release T.13.06 .....	77
Release T.13.07 .....	77
Release T.13.08 .....	78
Release T.13.09 .....	78
Release T.13.10 through T.13.13 (Never built) .....	78
Release T.13.14 (Never released) .....	79
Release T.13.15 (Never released) .....	81
Release T.13.16 (Not a public release) .....	81
Release T.13.17 (Never released) .....	82
Release T.13.18 (Never released) .....	82
Release T.13.19 - T.13.21 (Never built) .....	83
Release T.13.22 (Never released) .....	83
Release T.13.23 .....	84
Release T.13.24 .....	84
Release T.13.25 .....	86
Release T.13.26 .....	87
Release T.13.27 - T.13.44 (Never built) .....	88
Release T.13.45 .....	88

Release T.13.46 - T.13.56 (Never built) .....	88
Release T.13.57 .....	88
Release T.13.58 - T.13.59 (Never built) .....	92
Release T.13.60 .....	92
Release T.13.61 .....	96
Release T.13.62 .....	96
Release T.13.63 .....	97
Release T.13.64 .....	98
Release T.13.65 .....	98
Release T.13.66 .....	99
Release T.13.67 .....	102
Release T.13.68 .....	103
Release T.13.69 .....	103
Release T.13.70 (Never built) .....	107
Release T.13.71 .....	107





# 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/software](http://www.procurve.com/software).
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/manuals](http://www.procurve.com/manuals).
2. Click on the name of the product for which you want documentation.
3. On the resulting web page, double-click on a document you want.
4. When the document file opens, click on the disk icon  in the Acrobat® toolbar and save a copy of the file.

## Downloading Software to the Switch

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 drop-down 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.

## Best Practices for Major Software Updates

Major software updates contain new features and enhancements, and are designated by an increment to the major release version number. That is, T.12.xx represents a major update to software version(s) T.11.xx, and T.13.xx represents a major update to T.12.xx, and so forth. To mitigate against potential migration issues when performing such an update, this section documents best practices for updating the switch, including contingency procedures for rolling back to previous software versions and saved configurations.

---

### Caution

Before you update the switch software to a major new version, ProCurve strongly recommends that you save off a copy of your config file to an external location. ProCurve advises against rolling back (going from a newer software version to an older software version) without copying on a backup config file to the device.

---

### Updating the Switch: Overview

To perform a major update to your switch software, follow the steps below (see page 7 for details):

1. Download the image to your TFTP server.
2. Save your current configuration (Config1) to a backup configuration file (configT1252).
3. Save your current configuration to an external tftp server.
4. Backup your current running image (Primary) to the secondary image.
5. Set your secondary image to boot with ConfigT1252.
6. Download the new image to the switch's primary image.
7. Verify that your images and configuration are set correctly.
8. Reload the switch.

After following these steps, you should end up with the following results:

- Primary image will hold the new software image you want to install (for example, T.13.09)
- Secondary image will hold the image you are currently running (for example, T.12.52)
- Primary image will boot with config1 (config file corresponding to new software version—in this example, T.13.09)
- Secondary image will boot with config2\* (config file corresponding to previous software version—in this example, T.12.52)

\* The current config file must be copied to configT1252, or you will be unable to revert if the need arises.

---

**Note:**

You might opt to use a different methodology in which the new software will be installed as the secondary and not the primary image, in which case you would use the commands **boot system flash secondary**, and/or **boot set-default flash secondary** to change the location of the default boot. However, since you will still need to take precautions to allow you to revert to your previous configuration, ProCurve strongly recommends you follow the methods that are proposed in our update process. This will ensure that you can use our proposed roll back procedures should the need arise.

---

## Updating the Switch: Detailed Steps

The following detailed steps shows how to update the switch software from an existing version to a major new release (in the example provided here, from version T.12.52 to version T.13.09).

1. Download the latest release software image to your TFTP server from the ProCurve Web site.:<http://www.hp.com/rnd/software/switches.htm>
2. Save your current configuration (Config1) to backup configuration file (Config2).
  - a. Before copying the config, verify the current state of your system using the **show version**, **show flash**, and **show config** files commands. For example:

```
ProCurve Switch 2900-24G# show version
```

```
Image stamp:      /sw/code/build/mbm(t2g)
```

```
Jan  9 2008 12:29:32
```

```
T.12.52
```

```
2253
```

```
Boot Image:      Primary
```

```
ProCurve Switch 2900-24G# show flash
```

```
Image            Size(Bytes)    Date    Version
```

```
-----
```

```
Primary Image    : 6241116      01/09/08 T.12.52
```

```
Secondary Image  : 6234196      11/15/07 T.12.51
```

```
Boot Rom Version: K.12.12
```

```
Default Boot     : Primary
```

```
ProCurve Switch 2900-24G# show config files
```

Configuration files:

id	act	pri	sec	name
1	*	*	*	config1
2				
3				

b. Create a backup configuration file and verify the change.

```
ProCurve Switch 2900-24G# copy config config1 config configT1252
```

```
Switch1# show config files
```

Configuration files:

id	act	pri	sec	name
1	*	*	*	config1
2				configt1252
3				

3. Save the current config to a tftp server using the **copy tftp** command. For example:

```
ProCurve Switch 2900-24G# copy startup-config tftp 10.1.1.60
```

```
Switch1_config_T_12_52.cfg
```

---

## Note

This step is necessary because ProCurve does not support roll back (going from a newer software version to an older software version) without the ability to copy a backup config file onto the device. Backup your current running image (primary) to the secondary image.

---

```
ProCurve Switch 2900-24G# copy flash flash secondary
```

```
ProCurve Switch 2900-24G# show flash
```



Image	Size(Bytes)	Date	Version
-----	-----	-----	-----
Primary Image	: 6241116	01/09/08	T.12.52
Secondary Image	: 6241116	01/09/08	T.12.52
Boot Rom Version: K.12.12			
Default Boot	: Primary		

4. Backup Set your secondary image to boot with Config2.

```
ProCurve Switch 2900-24G# startup-default secondary config configt1252
ProCurve Switch 2900-24G# show config files
Configuration files:
```

id	act	pri	sec	name
1	*	*		config1
2			*	configT1252
3				

---

## Note

This step will enable you to revert from T\_13\_05 to your previous image with your previous configuration just by invoking the command **boot system flash secondary**.

---

5. Download the new primary image.

```
ProCurve Switch 2900-24G# copy tftp flash 192.168.1.60 T_13_09.swi
primary
```

The Primary OS Image will be deleted, continue [y/n]?

At the prompt, answer y, for yes, and the new image will be downloaded and written to the File system. Once tftp download has been completed you will see the following message:

Validating and Writing System Software to the Filesystem ...

6. Verify that your images and configuration are set correctly. For example, if you updated from T.12.52 to T.13.09, you should see the following outputs from the switch **show** commands:

```
ProCurve Switch 2900-24G# show version
```

## Software Management

### Best Practices for Major Software Updates

```
Image stamp:      /sw/code/build/mbm(t3a)
                  Jan  9 2008 12:29:32
                  T.12.52
                  2253
```

```
Boot Image:      Primary
```

```
ProCurve Switch 2900-24G# show fla
```

```
Image            Size(Bytes)   Date    Version
-----
Primary Image    : 6690472     04/17/08 T.13.09
Secondary Image  : 6241116     01/09/08 T.12.52
Boot Rom Version: K.12.12
Default Boot     : Primary
```

```
ProCurve Switch 2900-24G# show config files
```

```
Configuration files:
```

id	act	pri	sec	name
1	*	*		config1
2			*	configT1252
3				

#### 7. Reload the new switch image.

```
Switch1# boot
```

```
System will be rebooted from primary image. Do you want to continue
[y/n]? y
```

At the prompt, answer **y**, for yes, and the switch will boot with the new image.

---

### Note:

As an additional step, ProCurve advises saving the startup-config to a tftp server using the **copy tftp** command. For example:

```
Switch1# copy startup-config tftp 10.1.1.60 Switch1_config_T_13_09.cfg
```

---

## Rolling Back Switch Software

If you have followed the update procedures documented in the previous section, you should be able to revert to your previous configuration and software version using the steps below.

To roll back your switch from T.13.06 to T.12.57, for example, follow the steps below:

1. Verify that your images and configuration are set correctly using the **show version**, **show flash**, and **show config files** commands.

```
ProCurve Switch 2900-24G# show version
Image stamp:      /sw/code/build/mbm(t3a)
                  Apr 17 2008 09:46:38
                  T.13.09
                  344
Boot Image:       Primary
ProCurve Switch 2900-24G# show flash
Image             Size(Bytes)   Date    Version
-----
Primary Image    : 6690472      04/17/08 T.13.09
Secondary Image  : 6241116      01/09/08 T.12.52
Boot Rom Version: K.12.12
Default Boot     : Primary
```

```
ProCurve Switch 2900-24G# show config files
```

Configuration files:

id	act	pri	sec	name
1	*	*		config1
2			*	configT1252
3				

2. Boot the switch using the secondary image (with config2).

```
Switch1# boot system flash secondary
```

```
System will be rebooted from secondary image. Do you want to continue  
[y/n]? y
```

Answer **y**, for yes, and the switch will boot from the secondary image (T.12.52, in this example) with the corresponding configuration for that software version (configT1252).

## Viewing or Transferring Alternate Configuration Files

Viewing or copying an alternate configuration saved to the switch will always be accomplished through the software currently running on the switch. This may result in a misleading portrayal of the configuration. For example, if a configuration is created on T.12.52 and saved as configT1252, and if it is then viewed or transferred while the switch is running T.13.09, it will appear as though T.13.09 has converted the configuration. However, the alternate configuration file, configT1252, will still be intact on the switch and load properly when the switch is booted into the same software version from which the configuration file originated.

When an enhancement introduces a feature that did not previously exist in the switch, it may present several challenges to the user.

Backwards compatibility of the configuration created with a version of software that supports a new feature or parameter is not guaranteed. Software versions that did not recognize or support a particular command or parameter will not be able to interpret that line in the configuration. For this reason, it is strongly recommended that network administrators always save their configuration *while still running the switch with the original software version*, and with a notation indicating the software version on which the configuration was saved.

For example, a user might save a configuration for a switch running T.12.52 to a TFTP server with an IP address of 10.10.10.15 as follows:

```
ProCurve5406zl-onK1257# copy running-config tftp 10.10.10.15  
2900onT1252
```

If, for example, the user deems it necessary to revert to the use of T.12.52, she can boot into it and then restore the saved config from the TFTP server.

Viewing or copying an alternate configuration that is saved to the switch flash can be accomplished only with the software that is currently running on the switch.

Here, for example, a configuration is created on T.12.52 and then saved to flash:

```
ProCurve Switch 2900-24G# copy config config1 config configT1252 <cr>
```

And later, the configuration that was created on T.12.57 is viewed while the switch is running T.13.06:

```
ProCurve Switch 2900-24G# show config configT1252 <cr>
```

The command output will show how the T.12.57 config would be interpreted, if it were to be used by the T.13.06 software. Copying the T1257config to a TFTP server would similarly trigger an interpretation by the software performing the file transfer. Note, however, that this does not actually *change* the configuration. If the version is rolled back from T.13.06 to T.12.57 with a command like the following (given that T.12.57 is stored in secondary flash), the T.12.xx formatted config is still intact and valid.

```
ProCurve5406zl# boot system flash secondary config K1257config
```

This interpretation during a TFTP or **show** command execution is inherent in the architecture of the switch. When switch features change significantly (e.g. the move from IPv4 support to IPv6 support), there may be configuration parameters from the previous config that cannot be translated by the switch for viewing while it is running the new software. This necessitates storing configurations for each version of software to an external location, if the user would like to view the stored config prior to reloading it.

## HP 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, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G), Switch 8212zl and Switch 6600 Series (6600-24G, 6600-24G-4XG, 6600-24XG).
<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>R</b>	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
<b>T</b>	Switch 2900 Series (2900-24G and 2900-48G)
<b>U</b>	Switch 2510-48
<b>W</b>	Switch 2910al Series (2910al-24G, 2910al-24G-PoE+, 2910al-48G, and 2910al-48G-PoE+)
<b>VA/VB</b>	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
<b>WA</b>	ProCurve Access Point 530
<b>WS</b>	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
<b>WT</b>	ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module
<b>Y</b>	Switch 2510G Series (2510G-24 and 2510G-48)

Software Letter	ProCurve Networking Products
<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, SP2 and 7.0	Sun Java 2 Runtime Environment: – Version 1.5.0_11, Version 1.6.0
Windows Server SE 2003 SP2		
Windows Vista		

## Minimum Software Versions

### For ProCurve Series 2900 Switches and Hardware Features

ProCurve Device	Product Number	Minimum Supported Software Version
ProCurve 100-BX-D SFP-LC Transceiver	J9099B	T.13.45
ProCurve 100-BX-U SFP-LC Transceiver	J9100B	T.13.45
ProCurve 1000-BX-D SFP-LC Mini-GBIC	J9142B	T.13.45
ProCurve 1000-BX-U SFP-LC Mini-GBIC	J9143B	T.13.45
Procurve 10-GbE X2-SC LRM Optic	J9144A	T.13.18

## Support Notes

---

**Password Encryption.** The Password Manager portion of the Include Credentials feature is using SHA-0 Instead of SHA-1 for creation of the hash value. In order to accommodate customers that have worked around this issue, this fix will translate the configuration and correctly report the use of SHA-0 in the config after a software update containing this fix.

Example line from password encryption config prior to the fix:

```
password operator sha-1 "lsadjklkjfsd..."
```

Example of what that line might look like after the fix:

```
password operator sha0 "lsadjklkjfsd..."
```

No switch administrator intervention is required for the forward configuration translation to occur.

This fix has implications for rolling back the software. If password encryption is configured and a switch running software with the fix is rolled back to a software version prior to the fix using the same config file, the config loading will fail, and error messages for each line containing "sha0" or "sha1" will be displayed on the switch terminal. In the following example, sha1 was line 14 in the config, and sha0 was on line 15 of the config.

```
Line:14. Invalid input: *sha1*  
Line:15. Invalid input: *sha0*
```

To avoid configuration compatibility issues, please follow the instructions in the [“Best Practices for Major Software Updates” on page 6](#). If roll back to a pre-fix software version occurs without following the Best Practice suggestion (association of a compatible config file with a software version), the switch administrator should gain access to the switch by hitting <enter> at the password prompt, and must then reconfigure the password encryption with valid parameters (the pre-fix CLI syntax is **SHA-1**, versus the post-fix CLI use of **SHA0** or **SHA1**).

The default hash value for newly configured password encryption on a software version with this fix is **SHA1**.

**CAUTION - Updating to Version T.13.xx:** It is important that you update to T.13.xx from a configuration that has not been previously converted from a pre-T.13.xx format and subsequently rolled back to T.12.xx. If you have updated to T.13.xx and rolled back to T.12.xx to workaround an issue, you should load a saved T.12.xx configuration to the switch and boot to it prior to updating to T.13 again. Archive Pre-T.13.xx configuration files before updating! A configuration file saved under version T.13.xx software is not backwards-compatible with previous software versions.



# 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.

■ **MSTP mCheck**

Unlike other MSTP parameters, 'mCheck' is not a configurable option. It is a flag that tells MSTP to initiate transmission of RST/MST BPDUs for a MigrateTime (3 secs) period, to test whether all STP Bridges on the attached LAN have been removed and the Port can migrate to the native MSTP mode and use RST/MST BPDUs for transmission. The 'mCheck' is always cleared (set FALSE) prior to port initialization.

Some of the earlier ProCurve MSTP implementations allowed the 'mCheck' option to be a configurable parameter, which resulted in it being stored in the config. That was corrected beginning with version T.12.04.

■ **Menu Interface Configuration Limit**

The menu interface allows the user to perform VLAN port assignment for up to 32 VLANs. CLI or Web Management Interface should be used for VLAN port assignment beyond 32 VLANs.

■ **Virtual Stacking/Management VLANs:**

A ProCurve switch that is configured as a Stack Member can no longer be managed by the Stack Commander if it is also configured with a Management VLAN. This is by design. The Management VLAN is configured when the network administrator desires an isolated, non-routable VLAN for use in managing the network. Virtual Stacking is intended to conserve IP addresses on the network by allowing the management of up to 16 switches through the IP address of the Commander Switch. Due to the expectation that Stack Members will not have their own IP address, stacking traffic was not designed to traverse a Management VLAN. Virtual stacking and Management VLANs should therefore be considered mutually exclusive features.

## Known Issues

---

### Release T.13.63

The following problems are known issues as of release T.13.63.

- **SCP (PR\_0000016819/0000039942)** — Transferring a switch configuration of 4,201 bytes or larger to a switch's /cfg/startup-config directory via SCP will result in the switch coming up on factory defaults or with the new configuration only partly installed after reboot.
- **MAC-Authentication (PR\_0000039905)** — Problems authenticating multiple clients via MAC-authentication using an hp-nas-filter-rule.

### Release T.13.08

The following problems are known and open issues in release T.13.08.

- **Port Security (PR\_1000777162)** — When Port Security is configured for static MAC address learning, prolonged flooding of unicast traffic may occur under certain conditions.
- **Certificate (PR\_1000416167)** — The Web Management interface submission form limits CA-signed certificates to 1800 bytes.
- **CLI (PR\_1000760929)** — The CLI output from the command **show name int <x-x>** does not display the port number beyond the ninth port.
- **RADIUS/Jumbo (PR\_1000779048)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. When the RADIUS server replies with a large frame, the switch does not respond, causing the authentication process to halt.
- **SNMP Trap (PR\_1000772026)** — The switch does not send the proper OID value for a Redundant Power Supply (RPS) failure.
- **Web (PR\_1000761014)** — The web interface truncates 16 character passwords to 15 characters. Workaround: configure 16 character passwords via the CLI.
- **ICMP (PR\_1000764033)** — ICMP TTL expired messages are being sent with a source address of the interface the message leaves from rather than the interface that receives the expired packet.
- **Auto-TFTP/Config (PR\_0000001410)** — Auto-TFTP configuration is lost during the update from T.12.xx to T.13.03.

- **Web Authentication (PR\_0000000968)** — Web authentication to IAS over PEAP may trigger a software exception crash with a message similar to the following.

```
Software exception at exception.c:501 -- in 'mWebAuth', task ID =  
0x843c2b0 -> internal error
```

- **CLI (PR\_1000745509)** — There are multiple issues with respect to the output from the CLI command **show ipv6 neighbor vlan <x>**.
- **Module Selftest (PR\_0000001273)** — After reboot, ports 1-24 or ports 25-48 may become unresponsive followed by green and amber port LEDs remaining lit. Ports recover automatically. The log file will show the following messages.

```
chassis: Ports 1-24: Slave ROM Tombstone: 0x13000601  
chassis: Ports 1-24: Lost Communications detected - Heart Beat Lost(4A)  
chassis: Ports 1-24 Downloading  
chassis: Ports 1-24 Download Complete  
chassis: Ports 1-24 Ready
```

- **CLI (PR\_1000782972)** — The CLI command **show system power** provides incorrect output for those regions that use a 220 Volt standard.
- **CLI (PR\_1000430534)** — Output from the **show port-access mac-based** CLI command may omit some connected clients.
- **Config Transfer (PR\_1000781015)** — A config file transfer will fail with a corrupted configuration message, if the file specifies MDIX-mode for a dual-personality port.
- **Config Transfer (PR\_1000781004)** — The switch allows a config file transfer to set an invalid speed-duplex setting on a 100FX SFP.
- **Config Transfer (PR\_1000781031)** — When the valid port setting 'auto-1000' is configured for a 10/100/1000 interface and the configuration gets copied to the switch, the port setting gets altered to 'auto.'
- **Config Transfer (PR\_1000781011)** — A config file copied to the switch allows an entry to enable flow control on a half-duplex interface. However, the flow control on a half-duplex interface is disabled, as specified by IEEE 802.3 Annex 31B.
- **CLI (PR\_1000775644)** — When flow control is enabled, the output from a **show int brief** CLI command inaccurately indicates that flow control is off.

## Release T.13.03

The following problems are known and open issues in release T.13.03.

**Known Issues**  
Release T.13.03

**PCM+ USB Autorun (PR\_1000767612)** — Issuing the command **copy startup-config usb test** may crash the switch when executed in a PCM+ Autorun cmd file. The crash message is similar to:

```
PPC Data Storage (Bus Error) exception vector 0x300:
```

```
Stack Frame=0x07cbda70 HW Addr=0x70983298 IP=0x001bcf70 Task='tUsbAuto'  
Task ID0 fp: 0x7098328c s
```

# 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.13.02 Enhancements](#)” on page 51.

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 T.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.

- **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** 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 29](#).
- 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.

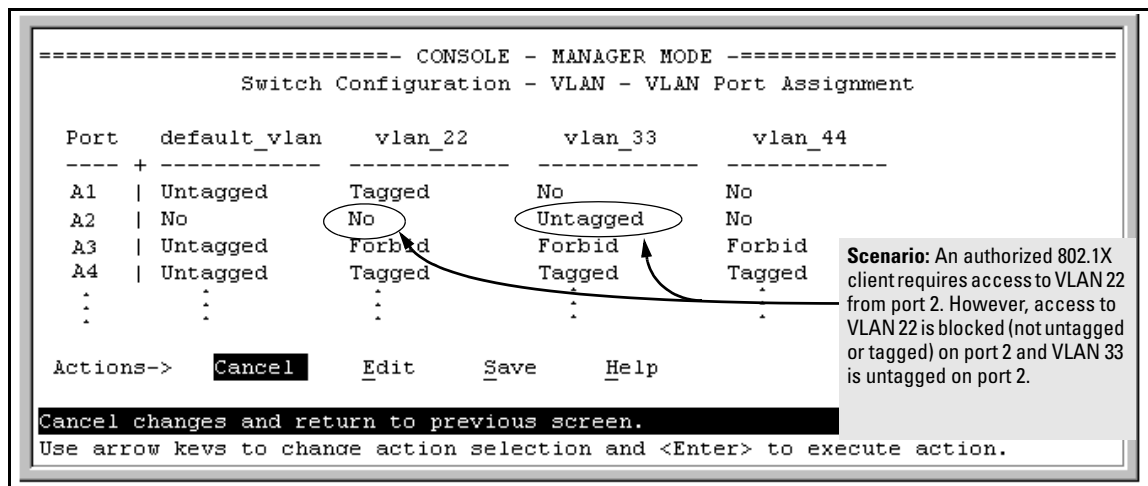
If this temporary VLAN assignment causes the switch to disable a different untagged static or dynamic VLAN configured on the port (as described in the preceding bullet and in [“Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session” on page 27](#)), the disabled VLAN assignment 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.

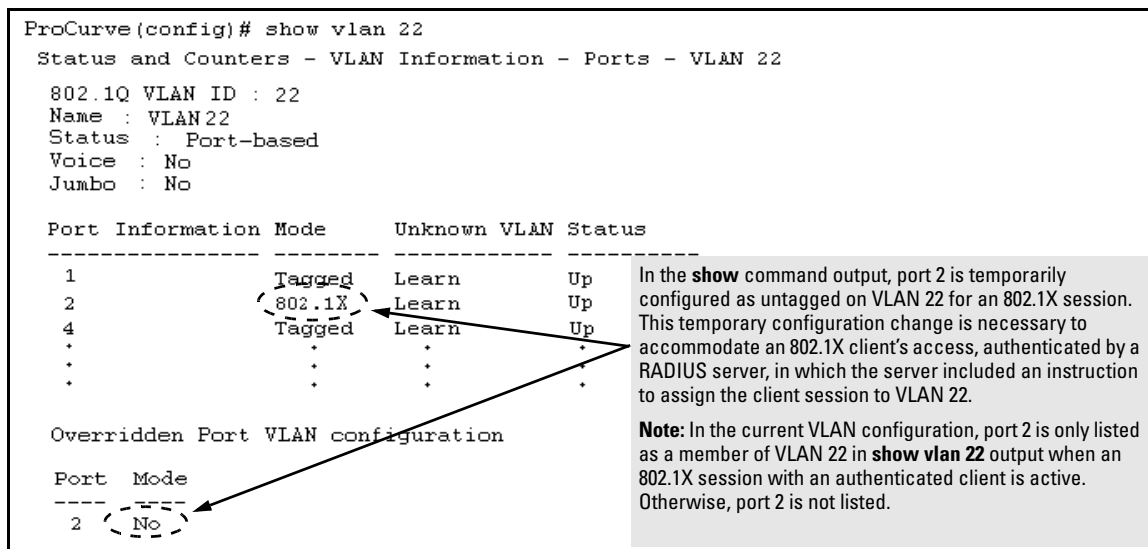


**Figure 1. Example of an Active VLAN Configuration in the Menu Interface View**

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).

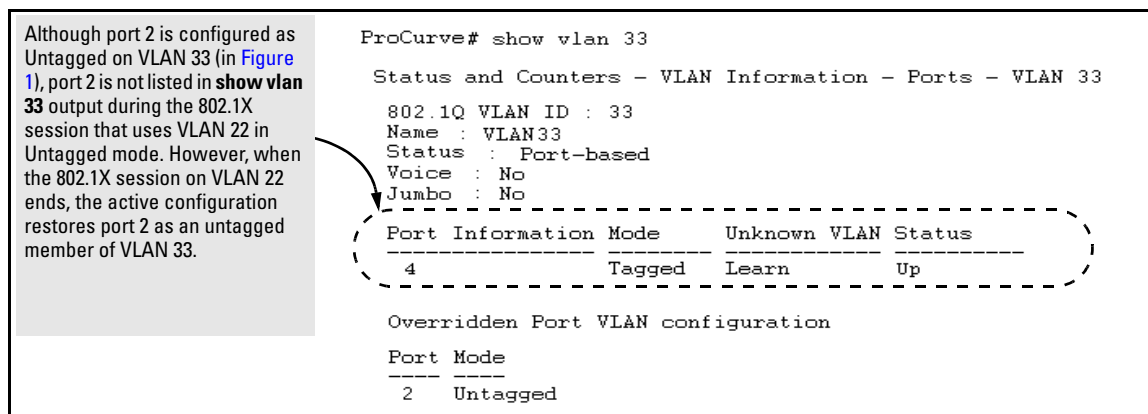
To view the temporary VLAN assignment as a change in the active configuration, use the **show vlan <vlan-id>** command as shown in Figure 2, where <vlan-id> is the (static or dynamic) VLAN used in the authenticated client session.



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

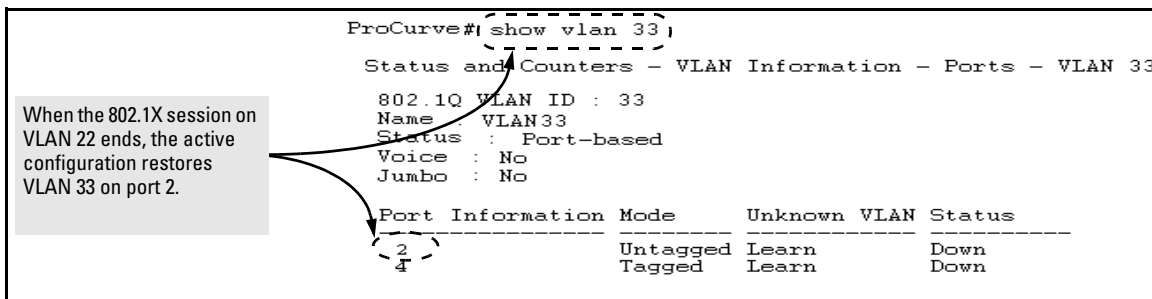
However, as shown in [Figure 1](#), VLAN 33 is configured as untagged on port 2 and because a port can be untagged on only one VLAN, port 2 loses access to VLAN 33 for the duration of the 802.1X session on VLAN 22.

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](#).



**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>]
```



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 35](#).

## 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 33](#).

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

- A keystore cannot contain both single and double quotes.
- A keystore 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 T.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|operator> [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 \
BhkXjtHhz6gD701otgizU0O6/Xzf4/J9XkJHkOCnbHIqtB1sbRYBTxj3NzA \
K1ymvIaU09X5TDAAAFQCPwKxnbwFfTPasXnxfvDuLSxaC7wAAAIASBwxUP \
pv2scqPPXQghgaTkdPwGGtdFW/+K4xRskAnIaxuG0qLbnekohi+ND4TkKZd \
EeidgDh7qHusBhOFXM2g73RpE2rNqQnSf/QV95kdNwWtbxuusBAzvfaJptd \
gca6cYR4xS4TuBcaKiorYj60kk144E1fkDWieQx8zABQAAAIEAu7/1kV0dS \
G0vE0eJD23TLXvu94plXhRKCUAyvv2UyK+piG+Q1el1w9zsMaxPA1XJzSY/ \
imEp4p6WXEMcl0lpXMRnkhnuMMPaPMAQUT8NJTNU6hqf/LdQ2kqZjUuIyV9 \
LWyLg5ybS1kFLeOt0oo2Jbpy+U2e4jh2Bb77sX3G5C0= spock@sfc.gov" \
ip ssh public-key manager "ssh-rsa \
AAAAB3NzaC1yc2EAAAADAQABAAQGDyO9RDD52JZP8k2F2YZXubgwRAN0R \
JRslEov6y1RK3XkmgVatzl+mspiEmPS4wNK7bX/IoXNdGrGkoE8tPklZOZ \
oqGCf5Zs50PlnkxXvAidFs55AWqOf4MhfCqvtQCelnt6LFh4ZMig+YewgQG \
M6H1geCSLUBXXScipdPHysakw== "TectiaClientKey [1024-bit rsa, \
nobody@testmachine, Mon Aug 15 2005 14:47:34]"
ip ssh public-key manager "ssh-rsa \
AAAAB3NzaC1yc2EAAAIBwAAAIEA1Kk9sVQ9LJOR6XO/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 31](#) 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 31](#) 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 31](#)) 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 33](#). (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 48](#).

[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. For more information, see the *ProCurve Access Security Guide*.
- **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. For more information see the ProCurve *Management and Configuration Guide*.
- **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. For more information about the MSTP VLANs, see the ProCurve *Advanced Traffic Management Guide*.

---

## Release T.12.51 Enhancements

*No new enhancements, software fixes only.*

---

## Release T.12.52 Enhancements

*No new enhancements, software fixes only.*

---

## Release T.13.02 Enhancements

The following enhancements are included in the T.13.02 release.

- **Enhancement:** Beginning with T.13.02, DHCP can now be enabled on a Management VLAN. Since, by definition, there is no routing to or from a VLAN configured as a management VLAN, DHCP relay is still prohibited so the DHCP server must be attached to the management VLAN for that VLAN to acquire an address. All DHCP options will be supported.

The following enhancements have been documented in the latest revisions to the manuals (January 2008). Refer to the indicated manuals for additional details.

Software Manual/ Enhancements	Description
<i>Management and Configuration Guide</i>	
<b>USB Secure Autorun:</b>	Helps ease the configuration of ProCurve switches by providing a way to auto-execute CLI commands from a USB flash drive. Note that the ability to create a valid AutoRun file also requires ProCurve Manager. For details, see the section on “USB Autorun” in the Appendix on “File Transfers”.
<b>SNMP Traps:</b>	Allow you to configure the switch to send network security and link-change notifications to configured trap receivers. More error conditions can be reported and logged to help resolve security threats and network issues.
<b>Show Command Changes:</b>	<p>The <b>show power-management</b> CLI command has been changed to <b>show power-over-ethernet</b>. You can use this command and the <b>show power slot &lt;slot-id&gt;</b> to display information about PoE power.</p> <p>The <b>show system-information</b> CLI command syntax has been changed to <b>show system</b> with additional options to display details of system components: <b>fans</b>, <b>information</b>, <b>power-supply</b>, and <b>temperature</b>.</p>
<i>Advanced Traffic Management Guide</i>	
<b>STP Diagnostics:</b>	Adds more diagnostic functions to resolve STP issues. See the section on “Troubleshooting an MSTP configuration” in the chapter on Multiple Instance Spanning-Tree Operation.
<i>Access and Security Guide</i>	
<b>Dynamic Configuration Arbiter:</b>	ProCurve provides different methods (for example, CLI, SNMP, or IDM/RADIUS) to configure network and security parameters and respond to threats. This feature allows you to determine the client-specific parameters that are assigned in an authentication session by applying or removing them as needed in a specified hierarchy of precedence.

Software Manual/ Enhancements	Description
<b>RADIUS Attributes:</b>	<p>Additional RADIUS attributes included with this release:</p> <ul style="list-style-type: none"> <li>• Change of authorization: allows changes to user service without re-authentication</li> <li>• Vendor-ID: allows Microsoft RADIUS servers to use vendor ID as part of the policy</li> <li>• Capability advertisement: allows the switch to advertise its capability to the RADIUS server</li> <li>• Session termination: allows the switch to report to the RADIUS server the reason a session is terminated</li> </ul> <p>For more information, see the section on “Additional RADIUS Attributes” in the chapter on “RADIUS Authentication and Accounting”.</p>
<b>RADIUS VLAN Support:</b>	<p>Supports RADIUS-assigned tagged and untagged VLAN configuration on an authenticated port. This allows you, for example, to use IDM to dynamically configure tagged and untagged VLANs as required for different client devices, such as PCs and IP phones, that share the same switch port. See the section on “VLAN Assignment in an Authentication Session” in the chapter on “RADIUS Authentication and Accounting”.</p>

---

## Release T.13.03 through T.13.04 Enhancements

*No new enhancements, software fixes only.*

## Release T.13.05 Enhancements

Release T.13.05 includes the following enhancement:

- **Enhancement (PR\_0000000420)** — This enhancement provides the **show-tech** option to **copy tftp** output for customizing output to the **show tech** command.

### Copy TFTP Command with Show Tech Option

Using the **copy tftp** command with the **show-tech** option provides the ability to copy a customized command file to the switch. When the **show tech custom** command is executed, the commands in the custom file are executed instead of the hard-coded list of commands. If no custom file is found, the current hard-coded list is executed. This list contains commands to display data such as the image stamp, running configuration, boot history, port settings, and so on.

**Syntax:** `copy tftp show-tech <ipv4 or ipv6 address> <filename>`

*Copy a customized command file to the switch.*

```
ProCurve(config)# copy tftp show-tech 10.10.10.3 commandfile1
```

**Figure 9. Example of Using the copy tftp show-tech Command to Upload a Customized Command File**

**Syntax:** show tech custom

*Executes the commands found in a custom file instead of the hard-coded list.*

**Note:** *Exit the global config mode (if needed) before executing **show tech** commands.*

You can include **show tech** commands in the custom file, with the exception of **show tech custom**. For example, you can include the command **show tech all**.

If no custom file is found, a message displays stating “No SHOW-TECH file found.”

```
ProCurve# show tech custom  
No SHOW-TECH file found.
```

No custom file was uploaded with the **copy tftp show-tech** command

**Figure 10. Example of the show tech custom Command**

## Release T.13.06 through T.13.14 Enhancements

*No new enhancements, software fixes only.*

## Release T.13.15 Enhancements

Release T.13.15 includes the following enhancement:

- **Enhancement (PR\_0000001641)** — This enhancement allows the user to set the console inactivity time out without reboot.

### Console/Telnet Inactivity Timer

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

**Syntax:** console inactivity-timer <minutes>

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

*Default: 0 (zero)*

For example:

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

- **Enhancement (PR\_1000780247)** — This enhancement provides hpicf Download MIB support for transferring configuration files both to and from a TFTP server. Prior to this enhancement, MIB support was limited to downloading and uploading software files.

## Release T.13.16 Enhancements

Release T.13.16 includes the following enhancement:

- **Enhancement (PR\_0000000088)** — This enhancement provides new features for use with SSH. The SSH enhancements are: AES encryption (included in the T.13.02 release). A new configuration option is added to allow the server to specify the set of ciphers available for client connection; A configurable key; Message Authentication Code (MAC) configuration. A new configuration option provides the ability to configure which MACs a client is permitted to use; Feedback information; and, SSH CLI show command information enhancements.

## Release T.13.17 Enhancements

Release T.13.17 includes the following enhancement:

- **Enhancement (PR\_1000406763)** — New commands were added to the CLI response to the **show-tech** command.

## Release T.13.18 Enhancements

Release T.13.18 includes the following enhancement:

- **Enhancement (PR\_0000004124)** — Support is added for the J9144A ProCurve 10-GbE X2-SC LRM Optic, an X2 form-factor transceiver that supports the 10-Gigabit LRM standard, providing 10-gigabit connectivity for up to 220 meters on legacy multimode fiber.

## Enhancements

Release T.13.19 through T.13.23 Enhancements

### Release T.13.19 through T.13.23 Enhancements

*No new enhancements, software fixes only.*

### Release T.13.24 through T.13.26 Enhancements

*No new enhancements, software fixes only.*

### Release T.13.27 through T.13.44 Enhancements

*No new enhancements; Release never built.*

### Release T.13.45 Enhancements

Release T.13.45 includes the following enhancement:

■ **Enhancement (PR\_0000010783)** — Support was added for the following products:

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

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

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

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

### Release T.13.46 through T.13.56 Enhancements

*No new enhancements; Release never built.*

### Release T.13.57 Enhancements

*No new enhancements, software fixes only.*

### Release T.13.58 through T.13.59 Enhancements

*No new enhancements; Release never built.*



## Release T.13.60 Enhancements

*No new enhancements, software fixes only.*

## Release T.13.61 through T.13.62 Enhancements

*No new enhancements; Never released.*

## Release T.13.63 Enhancements

*No new enhancements, software fixes only.*

## Release T.13.64 Enhancements

*No new enhancements, software fixes only (not a public release).*

## Release T.13.65 Enhancements

Release T.13.65 includes the following enhancements (not a public release).

- **Enhancement (PR\_0000016965)** — Debug logging enhancements have been made so that task name prefix, time stamp prefix, and other types of information are available to improve the troubleshooting processes.
- **Enhancement (PR\_0000017230)** — Crash data has been improved in order to help speed time to problem resolution.

## Release T.13.66 Enhancements

*No new enhancements, software fixes only (software never released).*

## Release T.13.67 Enhancements

*No new enhancements, software fixes only.*

## Release T.13.68 Enhancements

*No new enhancements, software fixes only.*

## Release T.13.69 Enhancements (Never released.)

Release T.13.69 includes the following enhancement (not a public release).

- **Enhancement (PR\_0000040638)** — Output from the CLI command **show config files** has been added to the CLI output for the **show tech** and **show tech all** commands.

## Release T.13.70 Enhancements (Never built.)

Release T.13.70 was never built.

## Release T.13.71 Enhancements

Release T.13.71 includes the following enhancements.

- **Enhancement (PR\_0000042147/0000042840)** — Port-Based Debug Logging Enhancement. This enhancement provides debug logging with the ability to filter debug messages related to a specific set of configured ports. When the port filter is enabled for a debug type, only the messages that have inherently refer to a specific port will be filtered. All other messages for that debug type will still be sent to debug logging. The CLI command for this enhancement is below.

```
Switch# debug <security> <port-access | port-security |  
user-profile-mib> <optional detailed debug type> include port  
[PORT-LIST]
```

The following is used to remove all ports:

```
Switch# [no] debug <security> <port-access | port-security |  
user-profile-mib> <optional detailed debug type> include port
```

- **Enhancement (PR\_0000016657)** — Access Control Debug Logging changes have been made.

### Access Control Debug Logging

Debug logging provides real-time messages on the status of processes running on the switch. The access control changes deal mainly with the client authentication process.

The debug options include a new security branch that contains all the security features. The existing options are moved under a parent option of “security”. The new options also reside under the parent security option.

Existing Security Debug Options	New Security Debug Options
SSH	Radius
Dynamic Arp	Web-Auth (has subnodes)

Existing Security Debug Options	New Security Debug Options
Dsnoop agent events packets	Port Access authenticator (802.1X) mac-based supplicant (802.1X) web-based
Dynamic IP Lockdown	TACACS  Port Security  User Profile MIB

For more information about debug events, see “Using the Event Log for Troubleshooting Switch Problems” in the *Troubleshooting* chapter of the *Management and Configuration Guide* for your switch.

**Syntax:** debug security [arp-protect | dhcp-snooping | dynamic-ip-lockdown | port-access | port-security | radius-server | ssh | tacacs-server | user-profile-mib]

*Displays debug messages for the selected option.*

*Default: Option is disabled.*

```
ProCurve(config)# debug security ssh info
ProCurve(config)# debug security dhcp-snooping agent
ProCurve(config)# debug security port-access mac-based

ProCurve(config)# show debug

Debug Logging

Source IP Selection: Outgoing Interface
Destination:      Session

Enabled debug types:
security ssh (info)
security dhcp-snooping agent
security port-access mac-based
```

**Figure 2. Example of Enabling Debug Messages for Selected Security Options**

## **Events Logged**

### **802.1X, Web/MAC, IDM, and DCA Authentication Debug Log Events**

- A client authentication request is sent to RADIUS for a specific client on a port.
- A client authentication response is received from RADIUS for a specific client on a port.
- Access denied on a port because of conflicts with RADIUS-assigned attributes (VLAN).
- Displays RADIUS-assigned switch attributes for each user authenticated on the switch. VLAN attributes include tagged or untagged.
- Provides information on authentication process for a client, for example, client A detected on port B.
- Provides information about credentials obtained from a client if the client is rejected by the RADIUS server and placed on the Guest VLAN.
- Reauth timer information for Web Authentication.
- For Web Authentication, provides information on the protocols that are spoofed by Web Authentication (DHCP, DNS, ARP, EWA, redirect).
- When a client moves from one port to another, when enabled.
- When a client is deauthenticated due to reauth period, logoff period, or forced reauth.

### **Port Security Debug Log Events**

- MAC addresses added through 802.1X or Web MAC authentication.
- MAC addresses that have been added, removed, learned, or aged on a port-security enabled port.

### **User Profile MIB Debug Log Events**

- All clients that are added or removed from the user profile MIB through SNMP.

### **RADIUS and TACACS+ Debug Log Events**

These debug log events cover management interface authentications (telnet, ssh, http, etc.) as well as access control authentication requests.

- Provides information about all RADIUS or TACACS+ request packets sent, for example, RADIUS request sent to server A for Client B on port 2.
- Provides information on all RADIUS or TACACS+ response packets received, for example, RADIUS response received on server A for Client B on port 2.
- All retries and timeouts for RADIUS or TACACS+ requests.
- All RADIUS drops due to bad attributes.

# Software Fixes in Release T.11.10 - T.13.71

---

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.13.09” on page 78](#).

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='mSnmpCtrl'
```
- **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.

- **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 skip-count 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**.
- **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.
- **sFlow (PR\_1000361604)** — Changed the maximum sFlow skip-count 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."
- **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** 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 **swlnitTask**. 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 45](#).
- **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).

- **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.
- **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 24](#).
- **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.
- **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 back-slash 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 ssp:

## 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.

## 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.
- **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.
- **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.
- **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.
- **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. For more information about the MSTP VLANs, see the ProCurve *Advanced Traffic Management Guide*.
- **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.
- **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.



- **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 30](#).

## Release T.13.02

The following problems were resolved in release T.13.02.

- **Enhancement:** Beginning with T.13.02, DHCP can now be enabled on a Management VLAN. Since, by definition, there is no routing to or from a VLAN configured as a management VLAN, DHCP relay is still prohibited so the DHCP server must be attached to the management VLAN for that VLAN to acquire an address. All DHCP options will be supported. For more information, see [“Release T.13.02 Enhancements” on page 51](#).
- **CLI (PR\_1000307590)** — Tab-help error in the spanning-tree instance *<instance number>* `vlan <vlan number>` command context.
- **CLI (PR\_1000330684)** — Help text in the spanning-tree `<port_id>` context was updated.
- **CLI (PR\_1000742426)** — The CLI command `copy usb pub-key-file` doesn't provide all the appropriate options.
- **Counters (PR\_1000758834)** — SFLOW counter-polling samples may be infrequent or stop until the switch is rebooted.
- **IGMP (PR\_1000739226)** — Some hosts or downstream devices may experience a disruption in multicast data due to loss of IGMPv3 reports.
- **DHCP Relay (PR\_1000751623)** — If the IP address on a VLAN interface is changed, any previously configured IP Helper address stops working.
- **SCP (PR\_1000760416)** — Software transferred through SCP upload becomes corrupted; the image is successfully copied via SCP, but when the switch processes the image to burn it to flash, the write never completes.

## Release T.13.03

The following problems were resolved in release T.13.03.

**RADIUS (PR\_1000767109)** — RADIUS authentication may fail due to what appears to the RADIUS server as a mis-configured password.

## Release T.13.04

Release T.13.04 was never built.

## Release T.13.05

The following problems were resolved in release T.13.05 (never released).

- **Port/Config (PR\_1000772652)** — A switch running software version T.12.52 or later only accepts the speed-duplex settings 'auto' or '1000-full' for the dual-personality ports when the configuration file is transferred to the switch via tftp, scp or sftp. Other port settings that should be valid cause the file transfer to abort with a "corrupted download file" error.
- **Port/Config (PR\_1000778004)** — The switch accepts, via file transfer, a config file with invalid speed/duplex settings on dual-personality ports. Additionally, the 100-FX port settings do not survive a reboot.
- **SNMPv3/Config (PR\_1000777656)** — The SNMPv3 configuration is removed from the switch's config file after an update from T.12.xx to T.13.03.
- **SSH/Config (PR\_1000777873)** — SSH becomes disabled (an 'ip ssh' entry in the config file becomes a 'no ip ssh' entry in the config file) after an update from T.12.xx to T.13.03.
- **TFTP/Config (PR\_0000000922)** — TFTP client configuration becomes disabled ('no tftp client') after an update from T.12.xx to T.13.03.
- **'show tech all/route'/Hang (PR\_1000779458)** — When the **show tech all** or **show tech route** commands are used within a remote management session, the switch may hang.
- **'show tech' (PR\_0000000635)** — The **show tech** CLI command will cause an "Invalid input: power" error message to be displayed.
- **CLI (PR\_0000000358)** — The output from the **show modules** CLI command shows the module serial number as being all zeros, or fails to show any output at all for that value.
- **Link/Config (PR\_1000771549)** — On a ProCurve 3500yl Series Switch, a link will not come up after configuring the port mode from MDI to AUTOMDIX (on one side of the link).

- **Static Route/Config (PR\_1000785177)** — The VLAN ID for the static route configuration is changed from its original value after updating from T.12.xx to T.13.03.

- **Crash (PR\_1000783817)** — The switch may crash with a message similar to:

```
NMI event SW:IP=0x0010770c MSR:0x00029210 LR:0x00107714  
Task='midmCtrl' Task ID=0x8417f00 cr: 0x24004084 sp:0x08417c08  
xer:0x00000000
```

- **SNMP/Config (PR\_1000780506)** — The TFTP transfer of a config file to the switch will fail if the config file contains the command **snmp-server trap-source** <xx.xx.xx.xx>.
- **SNMP/Config (PR\_1000786158)** — The TFTP transfer of a configuration file created on T.12.xx to a switch running T.13.03 will fail if the configuration file contains the command **snmp-server enable traps authentication**.
- **IPv6/Config (PR\_1000781026)** — When a configuration file is transferred to the switch and the file contains a VLAN with the **ipv6 mld** statement, the switch alters the **ipv6 mld** statement to **no ipv6 mld fastleave 1-A24,=1-Mesh,Trk1-Trk60,Dyn1-Dyn60**.
- **SNTP/Config (PR\_1000786156)** — The TFTP transfer of a configuration file created on T.12.xx to a switch running T.13.03 will fail if the configuration file contains the command **sntp server** <x.x.x.x>.
- **VLAN/Config (PR\_1000782308)** — Updating from T.12.xx to T.13.03 may result in an incorrect port VLAN assignment.
- **Telnet-Server/Config (PR\_0000000946)** — The TFTP transfer of a config file to the switch will fail if the config file contains the command **no telnet-server**.
- **Authorized-Manager/Config (PR\_1000789930)** — The update from T.12.xx to T.13.03 does not translate the IP authorized-manager configuration properly.
- **UDLD (PR\_0000001433)** — After the switch is rebooted, UDLD may continue to keep switch ports in a blocked state.
- **VLAN Mirroring/Config (PR\_0000001240)** — The VLAN Mirroring configuration is changed from its original value after updating from T.12.xx to T.13.03.
- **Bootup/Flash (PR\_1000785118)** — During the write-to-flash process, the OS file may become truncated if the switch is interrupted (by crash or power outage, for example). This fix minimizes that risk.
- **Bootup/Flash (PR\_1000785113)** — During the write-to-flash process, the configuration file may become truncated if the switch is interrupted (by crash or power outage, for example). This fix minimizes that risk.
- **Static Route/Config (PR\_0000001471)** — Rebooting a switch running T.13.03 may cause the static route configuration to become corrupted.

- **Enhancement (PR\_0000000420)** — This enhancement provides the **show tech** option for customizing **copy tftp** output. For more information, see [“Release T.13.05 Enhancements” on page 53](#).

## Release T.13.06

The following problems were resolved in release T.13.06 (never released).

- **UDLD (PR\_0000001616 and PR\_0000001638)** — After the switch is rebooted, UDLD may continue to keep ports in a blocked state, particularly if the port is in a static LACP trunk.
- **CLI (PR\_0000001643)** — The **ip authorized-managers** CLI command does not allow the 10.0.0.0 IP address to be used.

## Release T.13.07

The following problems were resolved in release T.13.07 (not a public release).

- **Loopback Interface (PR\_1000793862)** — A ping or telnet session to a loopback address may fail intermittently. A traceroute to the loopback address completes successfully. This may cause some protocol packets to fail to reach the loopback address.
- **Crash (PR\_0000001689)** — A switch running software version T.13.04 or higher may crash during configuration of a trunk group from either the CLI or menu interface. Event log messages may be similar to the following.

```
W 03/11/06 03:18:53 00374 chassis: Ports 25-48 Slave ROM Tombstone:
0x13000601
W03/11/06 03:18:53 00374 chassis: Ports 25-48 Slave ROM Tombstone: 0x13000601
W 03/11/06 03:18:53 00374 chassis: Ports 25-48: Lost Communications detected
- Heart Beat Lost
I 03/11/06 03:19:00 00375 chassis: Ports 25-48 Downloading
I 03/11/06 03:19:01 00376 chassis: Ports 25-48 Download Complete
I 03/11/06 03:19:15 00422 chassis: Ports 25-48 Ready
```

## Release T.13.08

The following problems were resolved in release T.13.08.

- **SNMP/Config (PR\_0000001672)** — The **snmp-server** configuration may change during the migration from T.12.xx to T.13.03.
- **Web/MAC Authentication (PR\_1000793226)** — Web or MAC authentication to the switch by a client that moves from one port to another may either fail or cause the switch to crash with a message similar to the following.

```
Program exception vector - Task='mWebAuth' Task ID=0x83bc390
```

## Release T.13.09

The following problems were resolved in release T.13.09.

- **Crash (PR\_0000001689a)** — A switch running software version T.13.05 or higher may crash during configuration of broadcast rate limiting. Event log messages may be similar to the following.

```
W 03/11/06 03:18:53 00374 chassis: Ports 25-48 Slave ROM Tombstone:
0x13000601
W 03/11/06 03:18:53 00374 chassis: Ports 25-48 Slave ROM Tombstone:
0x13000601W
03/11/06 03:18:53 00374 chassis: Ports 25-48: Lost Communications
detected - Heart Beat Lost
I 03/11/06 03:19:00 00375 chassis: Ports 25-48 Downloading
I 03/11/06 03:19:01 00376 chassis: Ports 25-48 Download Complete
I 03/11/06 03:19:15 00422 chassis: Ports 25-48 Ready
```

- **Web Authentication (PR\_0000002047)** — Use of Web authentication with MS-CHAP-v2 to Microsoft IAS may cause the switch to crash with a message similar to the following.

```
Software exception at exception.c:501 -- in 'mWebAuth', task ID =
0x8438440 Memory System error at 0x7f56610 - memPartFree
```

- **MAC Authentication (PR\_0000002075)** — A client that fails MAC authentication will be blocked by AAA rather than the port being moved, unblocked, into a configured Unauthenticated VLAN.

## Release T.13.10 through T.13.13 (Never built)

There were no problems resolved in release T.13.10 through T.13.13.

## Release T.13.14 (Never released)

The following problems were resolved in release T.13.14.

- **VLAN/Config (PR\_1000782308)** — Updating from T.12.xx to T.13.03 may result in an incorrect port VLAN assignment.
- **MAC Authentication (0000002318)** — Authenticated MAC Auth clients may intermittently get placed into the unauthenticated VLAN and never come on-line.
- **Port Security (PR\_1000777162)** — When Port Security is configured for static MAC address learning, prolonged flooding of unicast traffic may occur under certain conditions.
- **Static Routes/Config (0000001461)** — Static routes mapped to VLANs are incorrectly migrated during the update from T.12.xx to T.13.xx.
- **RADIUS/Jumbo (PR\_1000779048)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. When the RADIUS server replies with a large frame, the switch does not respond, causing the authentication process to halt.
- **RADIUS (0000001164)** — The switch drops RADIUS messages with EAP-packets larger than 1496 bytes.
- **Auto-TFTP/Config (PR\_0000001410)** — Auto-TFTP configuration is lost during the update from T.12.xx to T.13.03.
- **TACACS+ (PR\_1000764992)** — After authentication to the switch using TACACS+, the switch may crash with a message similar to the following.

```
PPC Data Storage (Bus Error) exception vector 0x300:.Stack
Frame=0x08632568 HW Addr=0x30313165 IP=0x008bba1c Task='mTacacsR'
Task ID=0x86329c0.fp: 0x08632750 sp:0x08632628 lr:0x008bba00
```

- **DHCP Snooping (PR\_1000469934)** — When DHCP Snooping is enabled and configured, and a client sends a “DHCPINFORM” after receiving address information, the DHCP server response is not forwarded to the client by the switch.
- **Static Route (0000002610)** — After an update/roll-back/update (T.12 to T.13 to T.12 to T.13), static route entries may become corrupted, causing the CLI to hang following execution of the show ip route command.
- **Crash (PR\_0000002347)** — When a VLAN is deleted, all the port banks may crash with a message similar to the following.

```
ipamSRtDescr.c Line:289 mIpAdmUpCt0x4484364c ->ASSERT: failed
```

- **Certificate (PR\_1000416167)** — The Web Management interface submission form limits CA signed certificates to 1800 bytes.
- **802.1X (PR\_0000002036)** — 802.1X with Funk Steel Belted RADIUS server causes the switch to fail to assign the VLAN that it was sent with the "Tunnel-Private-Group-Id" parameter.
- **Module Selftest (PR\_0000001273)** — After reboot, ports 1-24 or ports 25-48 may become unresponsive followed by green and amber port LEDs remaining lit. Ports recover automatically. The log file will show the following messages.

```
chassis: Ports 1-24: Slave ROM Tombstone: 0x13000601
```

- **SNMP Trap (PR\_1000772026)** — The switch does not send the proper OID value for a Redundant Power Supply (RPS) failure.
- **CLI (PR\_0000002177)** — Presence of a ProCurve switch yl 10-GbE transceiver in the switch may cause the prompt, "Do you want to save the config?," even when no changes to the config have been made.
- **CLI (PR\_1000745509)** — There are multiple issues with respect to the output from the CLI command `show ipv6 neighbor vlan <x>`.
- **ICMP (PR\_1000764033)** — ICMP TTL expired messages are being sent with a source address of the interface the message leaves from rather than the interface that receives the expired packet.
- **Web (PR\_1000761014)** — The web interface truncates 16 character passwords to 15 characters. Workaround: configure 16 character passwords via the CLI.
- **MIB (PR\_1000770084)** — Several OIDs in MIB violate RFC 2737 and RFC 4133. The affected OIDs are:

```
.iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhysicalEntry.entPhysicalHardwareRev
.iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhysicalEntry.entPhysicalFirmwareRev
.iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhysicalEntry.entPhysicalSerialNum
.iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhysicalEntry.entPhysicalModelName
```

- **802.1X (PR\_1000446227)** — Switch 802.1X authentication running over PAP does not work if the RADIUS message authenticator attribute is required. This fix added the message authenticator attribute to non-EAP RADIUS responses.



- **VLAN/MSTP (PR\_0000002103)** — The alteration of the VLAN/MSTP instance mapping in the pending configuration is not properly functioning. Any attempt to remove a single VLAN ID (VID) from one MSTP instance and then assign it to another MSTP instance fails, though specifying a VID range succeeds.
- **SSH (PR\_0000001296)** — Upon reboot, if no key is present, a 1024-bit dsa ssh host key is installed rather than the previous default host key type of a 2048-bit rsa key.
- **CLI (PR\_1000430534)** — Output from the show port-access mac-based CLI command may omit some connected clients.
- **Static Routes/Config (0000001461)** — Static routes mapped to VLANs are incorrectly migrated during the update from T.12.xx to T.13.xx. This is a further improvement to an earlier fix.
- **DHCP (PR\_0000002888)** — A client may not be able to get a DHCP address when the Management VLAN is configured on the switch.

## Release T.13.15 (Never released)

The following problems were resolved in release T.13.15.

- **Enhancement (PR\_0000001641)** — This enhancement allows the user to set the console inactivity time out without reboot. For more information, see [“Release T.13.15 Enhancements” on page 54](#).
- **Enhancement (PR\_1000780247)** — This enhancement provides hpicf Download MIB support for transferring configuration files both to and from a TFTP server. Prior to this enhancement, MIB support was limited to downloading and uploading software files. For more information, see [“Release T.13.15 Enhancements” on page 54](#).

## Release T.13.16 (Not a public release)

The following problems were resolved in release T.13.16.

- **Enhancement (PR\_0000000088)** — This enhancement provides new features for use with SSH. The SSH enhancements are: AES encryption (included in the T.13.02 release). A new configuration option is added to allow the server to specify the set of ciphers available for client connection; A configurable key; Message Authentication Code (MAC) configuration. A new configuration option provides the ability to configure which MACs a client is permitted to use; Feedback information; and, SSH CLI show command information enhancements. For more information, see [“Release T.13.16 Enhancements” on page 55](#).

## Release T.13.17 (Never released)

The following problems were resolved in release T.13.17.

- **RADIUS/Jumbo (PR\_1000779048)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. When the RADIUS server replies with a large frame, the switch does not respond, causing the authentication process to halt.
- **Protocol Starvation (PR\_0000003814)** — If the switch is configured for routing, certain packets may cause a packet buffer leak, resulting in TELNET, ping, and SNMP becoming unresponsive.
- **Authorized Managers (PR\_1000806039)** — ProCurve Manager may delete Authorized Managers that have been configured on the switch.
- **Crash (PR\_0000001756)** — Configuration of VLANs and VLAN port assignment using SNMP may cause the switch may crash with a message similar to the following.

```
Software exception at bcmHwVlans.c:149 -- in 'mAdMgrCtrl', task ID=
0x18636e8 -> ASIC call failed: Entry not found.
```

- **Crash (PR\_1000715077)** — When RADIUS Accounting is configured, the switch may crash with a message similar to the following.

```
NMI event SW:IP=0x002bd6c4 MSR:0x00029210 LR:0x002bc6a8
Task='mAcctCtrl' Task ID=0x85e9f10 cr: 0x48000084 sp:0x085e9e38
xer:0x20000000
```

- **SNMP (PR\_0000001807)** — Use of a correctly configured third party utility to connect to the switch via SNMPv3 may result in the following event log message.

```
SNMP Security access violation from <ip address>
```

- **UDLD (PR\_0000002473)** — UDLD protocol packets received on a (non-UDLD) trunk port are incorrectly forwarded out of same port they are received on, resulting in high CPU usage on the switch.
- **Enhancement (PR\_1000406763)** — New commands were added to the CLI response to the **show tech** command.

## Release T.13.18 (Never released)

The following problems were resolved in release T.13.18.

- **Mirror/CLI (PR\_0000003269)** — The CLI incorrectly configures the option "no-tag-added" across multiple mirror sessions, resulting in the wrong output saved to the config file.

- **Wake-On-LAN (PR\_0000004794)** — Wake-On-LAN does not always work successfully.
- **IP Phone (PR\_0000004803)** — A tandem IP phone may stop talking to the switch after a connected PC login failure and reboot.
- **Authentication (PR\_0000005582)** - Sometimes PC in the PC-phone tandem authentication does not get authorized on an untagged VLAN.
- **Enhancement (PR\_0000004124)** — Support was added for the J9144A ProCurve 10-GbE X2-SC LRM Optic. For more information, see [“Release T.13.18 Enhancements” on page 55](#).
- **CLI (PR\_0000001528)** — 10-GbE X2 transceivers do not report their part numbers in response to the CLI command show tech transceivers.
- **X2 Transceivers (PR\_0000004758)** — Some ProCurve SR and ER X2-10GbE (J8436A, J8437A) transceivers have a timing issue that prevents the transceivers from being correctly identified either when hot swapped or during a cold boot.
- **LEDs (PR\_0000005623)** — Upon insertion of a removable transceiver – either X2 or SFP - the link LED fails to light for the 2 second-long indication of insertion confirmation.
- **Event Log (PR\_0000005624)** — A failed "removable" transceiver results in two event log messages rather than just one.

## Release T.13.19 - T.13.21 (Never built)

Releases T.13.19 through T.13.21 were never built.

## Release T.13.22 (Never released)

The following problems were resolved in release T.13.22.

- **CLI (PR\_1000760929)** — Output from the CLI command show name int <port list> fails to display the port number for interfaces with numbers larger than 9.
- **Config (PR\_0000003638)** — Fastboot can be configured, but then it cannot be disabled.
- **Multicast Filter (PR\_0000002988)** — Multicast filters may become corrupted following their initial configuration, save and subsequent switch reload.
- **CLI (PR\_1000782972)** — An incorrect line voltage value may be displayed in the output of the show system power CLI command.
- **Config (PR\_1000781011)** — Copying a config onto a switch allows the appearance of an invalid flow control setting (enabled) on half duplex ports.

- **Config (PR\_1000781015)** — When the MDIX-mode is configured for dual-personality ports, copying a config onto a switch fails and produces a message about config file corruption.
- **Config (PR\_1000781031)** — When the valid port setting 'auto-1000' is configured for any 10/100/1000 interface in an external configuration file and the configuration file is copied to the switch, the system returns the port setting to the default value, changing 'auto-1000' to 'auto.'
- **Event Log (PR\_1000755803)** — ProCurve Manager is unable to display a link to the switch Web Interface in events generated by Fault Finder.

## Release T.13.23

The following problems were resolved in release T.13.23.

- **Crash (PR\_0000006624)** — When using the Web Management Interface on software version T.13.17 and higher, the switch may crash if the "Configuration" and then "IP Configuration" tabs are clicked. There may be other triggers for this crash. The switch will display a message similar to the following.  

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack
Frame=0x0815da48 HW Addr=0xa2d3e193 IP=0x00169178 Task='tHttpd' Task
ID=0x fp: 0x00a650c4 sp:
```
- **Authentication (PR\_0000007209)** — A PC behind a tandem IP phone is not able to authenticate.

## Release T.13.24

The following problems were resolved in release T.13.24 (Never released).

- **802.1X (PR\_0000007259)** — Configuring 802.1X without activating it does not function as expected, resulting in blocking of the port.
- **Crash (PR\_0000004023)** — Repeated PCM configuration scans may cause the switch to crash with a message similar to the following.  

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack
Frame=0x07af44c0
HW Addr=0x6520463a IP=0x00965a88 Task='tSsh0' Task ID=0x7af4810fp:
0x013d97cc sp:0
```
- **Management Module (PR\_0000005902)** — Management functions may become unresponsive, resulting in loss of TELNET, Web Management, and console access functionality of the switch.

- **802.1X Authentication (PR\_0000002695)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. This allows the RADIUS server to reply with a large fragment which the switch does not process, causing the authentication to fail. This is an additional fix for the issue described in T.13.17 via PR\_1000779048.

- **SSH (PR\_0000002934)** — Copying the client's public SSH keys from the switch fails with the following error.

```
Couldn't read from remote file "/ssh/mgr_keys/authorized_keys
```

- **GVRP/RADIUS (PR\_0000006051)** — RADIUS assigned VLANs are not propagated correctly in GVRP. Please see [“Note: This fix is associated with some new switch behavior:”](#) for a description of the behavior change with this fix.

Note: This fix is associated with some new switch behavior:

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

- **Assert (PR\_0000005208)** — Entering **no ipv6 enable** at the CLI may result in a crash with a message similar to the following.

```
Software exception at ConfigRecIndex.cc:421 -- in 'mSess1', task ID  
= 0x58c1c38-> ASSERT:  failed.
```

- **Config (PR\_0000002620)** — A MAC-lockdown command that includes VLAN information may fail when it is copied to the default configuration.
- **AAA (PR\_0000008409)** — The CLI commands **aaa authentication** and **aaa accounting** return a resource unavailable error.
- **PCM (PR\_0000008113)** — Repeated ProCurve Manager Config Scans may trigger subsequent Config Scan failure.
- **Config (PR\_0000007953)** — The config line **spanning-tree instance <n> vlan <vid>** is truncated in some cases, causing loss of configuration after reload of the config file.
- **CLI (PR\_0000000912)** — The CLI command **copy tftp show-tech** fails, resulting in failure to create a custom show-tech file on the switch.
- **TFTP (PR\_0000008559)** — The switch administrator is unable to download a new image file after executing the CLI command **erase primary flash**; a corrupted download file error is reported.
- **ARP (PR\_0000008011)** — When port-security is configured, the switch sends ARP requests twice for an unknown DA, making the switch appear to be slow.

- **SFTP/SCP (PR\_0000008270)** — SFTP/SCP will not close the "client" session after the file transfer. The client session will need to be manually closed.
- **RADIUS (PR\_0000007278)** — MAC-based authentication doesn't work with a secondary RADIUS server unless the primary and secondary RADIUS server keys are identically configured.
- **Crash (PR\_0000006476)** — Some configuration commands entered at the CLI (e.g. **web**, or **no web**) may cause the switch to crash with a message similar to the following:  

```
PPC Data Storage (Bus Error) exception vector 0x300:Stack
Frame=0x088befef8HW Addr=0x00cff108 IP=0x0096ca4c Task='mSnmpCtrl '
Task ID=0x88bf320 fp: 0x0845a7e0
```
- **Crash (PR\_0000005940)** — An attempt at tab completion for some configuration tasks may cause the switch to crash with a message similar to the following:  

```
Software exception at parser.c:6291 -- in 'mSess1', task ID =
0x82ab3b0
```
- **CLI (PR\_0000004042)** — The CLI command **snmp-server response-source dst-ip-of-request** does not work as expected when the destination IP address of the *SNMP Request* is the Loopback IP. The source IP address of the *SNMP Response* should be the destination IP of the *SNMP Request*, but instead the switch uses the IP address of the active interface from which the *SNMP Response* was sent.
- **CLI (PR\_0000007686)** — The switch does not allow IP authorized-manager configuration of 10.0.0.0.
- **TACACS+ (PR\_0000003839)** — The TACACS server configuration parameter accepts an address from an invalid/reserved IP range: 0.0.0.1 to 0.255.255.255.
- **Boot Log (PR\_0000009434)** — The switch doesn't create an event log message after deleting an invalid TACACS server host config entry upon bootup following an update from T.12.xx to T.13.xx

## Release T.13.25

The following problems were resolved in release T.13.25 (Not a public release).

- **SNMP (PR\_0000001926)** — An SNMP query for the MIB **ifInUnknownProts** returns incorrect and varying results.

## Release T.13.26

The following problems were resolved in release T.13.26 (Never released).

- **ICMP Redirects (PR\_0000004534)** — When the next hop router in the same VLAN as the host machine, the switch does not generate ICMP redirects.
- **CLI (PR\_1000803731)** — If the "|" character exists in the banner text of a configuration file downloaded via TFTP transfer, the banner text may become corrupted, or the TFTP transfer may fail with a corrupted download file error message.
- **Hang (PR\_0000007806)** — Using the CLI command **no arp** on ARP entries that do not exist may cause the switch to hang.
- **CLI (PR\_0000008617)** — The **copy** command for USB options has incorrect optional parameters for plain text files.
- **RADIUS Accounting (PR\_0000004139)** — Procurve switches do not send the accounting-request to RADIUS server upon execution of the **reload** CLI command.
- **RADIUS Accounting (PR\_0000004145)** — An incomplete "Calling-Station-ID" field is sent in the accounting-request to the RADIUS server upon execution of the **boot system** CLI command.
- **RADIUS Accounting (PR\_0000004141)** — The "Acct-Status-Type" attribute is missing in the accounting-request to the RADIUS server upon execution of the **boot system** CLI command.
- **Terminal Display (PR\_0000008238)** — The default boot message is incorrectly displayed with the wrong formatting if the terminal width is changed.
- **CLI (PR\_0000008236)** — The **enable** command is listed in the enable-mode help.
- **UDLD (PR\_0000009505)** — UDLD misconfiguration (where UDLD is enabled on one side and disabled on the other) could lead to unicast packet storm which results in MSTP running with multiple roots.
- **CLI (PR\_0000008217)** — The **copy flash** CLI command does not allow user to specify source OS location (primary/secondary).
- **CLI (PR\_0000010762)** — The **show interfaces** command results in empty display list.
- **STP (PR\_0000010815)** — When a switch configured with BPDU protection is added to a network, if the MSTP configuration of the uplink port is changed from **auto-edge** to **no auto-edge** there is a topology change event that takes place as the switch asserts itself as a new root.

## Release T.13.27 - T.13.44 (Never built)

Releases T.13.27 through T.13.44 were never built.

T.13.27 - T.13.44 were never built

## Release T.13.45

The following problems were resolved in release T.13.45.

- **Enhancement (PR\_0000010783)** — Support was added for the following products:

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

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

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

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

For more information, see [“Release T.13.45 Enhancements” on page 56](#).

- **Transceivers (PR\_0000010525)** — Intermittent self test failure may occur if transceivers are hot-swapped in and out of the switch in too short a time frame. Note that even with this fix, transceivers should always be allowed to initialize fully prior to removal and subsequent re-insertion.

*Best Practice Tip:* Upon hot insertion of a transceiver, the Mode LED will come on for two seconds while the transceiver is initialized. Once the Mode LED has extinguished, it is safe to remove the transceiver.

- **Selftest Failure (PR\_0000010937)** — Rarely, the switch may experience self test failure of all the port-banks. Messages like the following will be visible in the event log.

```
W <date/time stamp> 00374 chassis: Slot # Failed to  
boot-timeout- (SELFTTEST)
```

## Release T.13.46 - T.13.56 (Never built)

Releases T.13.46 through T.13.56 were never built.

## Release T.13.57

The following problems were resolved in release T.13.57.



- **sFlow (PR\_0000003723)** — The switch uses the loopback as the sFlow agent address, even after explicit configuration of the VLAN IP address and the collector receiving the sFlow packets.
- **SCP/SFTP (PR\_0000009174)** — Failure to upload a configuration via SFTP/SCP may occur. As a result, it is possible that the switch may become unresponsive or crash with a message similar to the following.

```
Software exception at cfg_edit.cc:313 - in 'swinitTask',  
task ID =0xa9bbcc0
```

- **SCP (PR\_0000011488)** — The switch does not return the scp/sftp session after new software is uploaded.
- **CLI (PR\_0000009997)** — The CLI response to the boot set-default flash <primary | secondary> configuration setting is inconsistent between the various platforms that support this feature, potentially causing issues for customers running scripts.
- **Password Encryption (PR\_0000011828)** — The Password Manager portion of the Include Credentials feature is using SHA-0 Instead of SHA-1 for creation of the hash value. In order to accommodate customers that have worked around this issue, this fix will translate the configuration and correctly report the use of SHA-0 in the config after a software update containing this fix.

Example line from password encryption config prior to the fix:

```
password operator sha-1 "lsadkjlkjfsd..."
```

Example of what that line might look like after the fix:

```
password operator sha0 "lsadkjlkjfsd..."
```

No switch administrator intervention is required for the forward configuration translation to occur.

For more information, see [“Support Notes” on page 16](#).

- **Crash (PR\_0000011049)** — Copying a configuration with mirroring enabled from USB to switch may trigger a software exception with a message similar to the following.
- ```
Software exception at cli_mirror.c:9953 -- in 'mftTask', task ID =  
0xa932bc0
```
- **DHCP Relay (PR\_0000011726)** — DHCP Discover packets may be relayed with a corrupted IP address for the Relay Agent. This causes the server to look up a client address range for an invalid network segment, and ultimately fail to communicate with the DHCP Server.
  - **PC/Phone Authentication (PR\_0000010104)** — When using an IP phone in tandem with a PC, sometimes the post-authentication VLAN assignment of the PC is delayed.

- **DHCP Relay (PR\_0000013661/000008196)** — After adding a second IP Address to a VLAN with IP Helper configured, the switch Relay Agent IP Address gets corrupted such that the DHCP server does not recognize the request as part of a configured scope, and drops the request. Workaround: Save the configuration and reload the switch after configuration of an IP Helper address and DHCP Relay.
- **Auto-TFTP (PR\_0000014646/0000013552)** — Certain software file names may trigger auto-tftp to reload the same software file repeatedly.
- **Config (PR\_0000014381)** — Switches running K.13.18 or newer software may be unable to upload a valid config file to the switch, if it is set with the parameter, speed-duplex 1000-full, and on a dual personality port with a mini-GBIC inserted. The switch will display a message similar to the following. (The example below contained the speed-duplex value in line 8 of the config, and the value was applied to port 47.)

```
line: 8. Value 1000-full is not applicable to port 47.  
Corrupted download file.
```
- **Config (PR\_0000014818)** — Although the switch CLI provides an appropriate error message when the user tries to add more MAC addresses than a port is configured to allow, it seems to save the excess MAC addresses and display them in the configuration.
- **CLI (PR\_0000009868)** — Execution of a **show** command in one Telnet or console session prevents successful execution of a **show** command in a concurrent management (CLI) session.
- **TELNET (PR\_0000008234)** — When a user Telnets from one switch's CLI to a second switch's CLI, and then logs out from the session on the second switch, the CLI message, "telnet connection reset by peer," is inappropriately displayed.
- **Syslog (PR\_0000008241)** — Event log messages with a severity of "E" (error) are not always supported by default on syslog servers. This fix updates the show logging help text to clarify the dependency. In order to modify the syslog configuration file on a Linux server in order to receive error messages, complete the following steps.
  - 1) # vim /etc/syslog.conf
  - 2) Add the following line in the syslog.conf file:

```
*. * /var/log/messages
```
  - 3) # /etc/init.d/syslog restart
- **Syslog (PR\_0000012167)** — Syslog messages longer than 119 characters get truncated.
- **Console (PR\_0000008235)** — The CLI command **console local-terminal** should affect only the session in which the command is issued, but instead it is persistent for any subsequent connections that use the same session number.

- **Crash (PR\_0000010915)** — Deletion of a VLAN or creation of a trunk group from the CLI during a Telnet session from another switch may cause an unexpected reboot with a message similar to one of the following.

```
PPC Data Storage (Bus Error) exception vector 0x300:  
Stack Frame=0x088bf120 HW Addr=0xc3d2e1f0 IP=0x008631c0  
Task='mSnmpCtrl' Task ID =0x88bf6a0 fp: 0xc3d2e1f0  
Software exception at iputil_integrity.c:3054  
-- in 'mIpCtrl', task ID = 0x1a4a0640
```

- **Crash Messaging (PR\_0000015799)** — Important data may be truncated from the crash message.
- **Crash (PR\_0000015804)** — When there is a heavy volume of routing table changes, the switch may unexpectedly reboot and report a message similar to the following.

```
Software exception at alloc_free.c:435 -- in 'mIpPktRecv',  
task ID = 0x85624f0 -> No msg buffer
```

- **Crash (PR\_0000016373)** — Switches with heavy routing and ARP activity may experience an unexpected reboot and report the following event log message and one of the following or a similar crash messages.

**Event Log:**

W 02/08/08 17:23:18 00436 NETINET: 1 route entry creation(s) failed.

**Crash Messages Possible:**

```
PPC Data Storage (Bus Error) exception vector 0x300:  
Stack Frame=0x08564480 HW Addr=0x4b5a6978 IP=0x0095ce28 Task='mIpPktRecv'  
Task ID=0x8564940 fp: 0xc0206921 sp:0x08564540 lr:0x0095cd90
```

```
PPC Data Storage (Bus Error) exception vector 0x300:  
Stack Frame=0x080b4da8 HW Addr=0x2f830000 IP=0x00867238 Task='mLinkTest'  
Task ID=0x0925aef0
```

```
PPC Data Storage (Bus Error) exception vector 0x300:  
Stack Frame=0x088b2b88 HW Addr=0x4b5a6978 IP=0x0095c170 Task='mSnmpCtrl'  
Task ID=0x88b3190 fp: 0xc0206921
```

```
PPC Program exception vector 0x700:  
Stack Frame=0x088b2960 HW Addr=0x0badbad0 IP=0x00000080 Task='mSnmpCtrl'  
Task ID =0x88b3190 fp: 0x008ecf3c sp:0x088b2a20 lr:
```

```
PPC Program exception vector 0x700:  
Stack Frame=0x0856af90 HW Addr=0x0badbad0 IP=0x09529d14 Task='mIpCtrl'  
Task ID=0 fp: 0x00000001 sp:0x0856b050 lr:0x
```

## Software Fixes in Release T.11.10 - T.13.71

### Release T.13.58 - T.13.59 (Never built)

SubSystem 0 went down: 02/08/08 22:11:41

Software exception at alloc\_free.c:435 -- in 'mIpPktRecv',  
task ID = 0x8564910 -> No msg buffer

- **Crash (PR\_0000015804)** — When there is a heavy volume of routing table changes, the switch may unexpectedly reboot and report a message similar to the following.

Software exception at alloc\_free.c:435 -- in 'mIpPktRecv',  
task ID = 0x85624f0 -> No msg buffer

- **Port Communication (PR\_0000004568)** — An Intel NIC using the 82566DM chipset may send fragments to the switch which results in the loss of communication on that or another port, regardless of a continuous connection. Symptoms may include one or more of the following behaviors.

- Rx Bytes counter does not increment
- CRC/alignment errors
- Duplex mismatch
- Collisions, runts
- Giants
- Other physical layer errors

Symptoms improve or resolve with updated NIC firmware and/or drivers, when they are available from the device manufacturer.

- **IGMP (PR\_0000009415)** — The switch may intermittently fail to forward a multicast stream.
- **IGMP (PR\_0000014293)** — When forced fast leave (FFL) is in use, a GMP leave sometimes terminates the stream before the appropriate timeout. Additionally, the FFL timeout value configured is not honored.

## Release T.13.58 - T.13.59 (Never built)

Releases T.13.58 through T.13.59 were never built.

## Release T.13.60

The following problems were resolved in release T.13.60.

- **CLI (PR\_0000018670)** — Execution of the CLI command **show tech all** on a switch running software version T.13.57 may trigger the switch to become unresponsive and require a power-cycle to recover.

- **DHCP-Snooping (PR\_0000015171)** — Client DHCP-snooping leases don't get renewed after uploading the DHCP-snooping binding file to the switch from a TFTP server. The client connectivity problems on the switch are compounded if ARP-protect is also enabled.
- **Debug (PR\_0000013983)** — Some of the DHCP-snooping debug messages reference the wrong port number.
- **802.1X (PR\_0000012568)** — There is a problem with a login error message.
- **Config (PR\_0000005260)** — If a VLAN has been previously configured as an **auth-vid** or **unauth-vid** VLAN for aaa port-access authentication, that VLAN cannot be deleted, even after removal of the port-access configuration using the CLI command **no aaa port-access authenticator <port>**. Attempts to remove the VLAN yield the following CLI message.

Can't remove, VID <VLAN ID> is auth-vid or unauth-vid

- **Appletalk ARP (PR\_0000015652)** — Appletalk ARP (AARP) packets are not traversing the Protocol VLAN making file sharing and print services unavailable.
- **CLI (PR\_0000010101)** — The last portion of the switch response to the CLI command **show port-access mac-based <port list> clients detailed** is garbled.
- **Authentication (PR\_0000011138)** — If the Radius server becomes unavailable, the **eap-radius authorized** option allows the switch to authenticate devices. If the response time of the RADIUS subsystem is greater than the server-timeout value on the switch or the device supplicant then switch will not be able to authenticate devices, and no warning of this failure will be displayed. This fix triggers the display of the following CLI message.

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

- **DHCP (PR\_0000010341)** — The DHCP retransmission delay time is not RFC compliant. The RFC described an exponential back-off algorithm but the switch sent a DHCP Request packet every 4 seconds.
- **Crash (PR\_0000007580)** — The switch may reboot unexpectedly when an attempt is made to add a route that overlaps with the next hop gateway. The crash message will be similar to the following.

```
PPC Data Storage (Bus Error) exception vector 0x300:
Stack Frame=0x0850abb0 HW Addr=0x00cf5194 IP=0x008110f8 Task='mIpAd-
MCtrl' Task 0 fp: 0x0850aca8
```

- **Authentication (PR\_0000012553)** — The switch sends EAP supplicant packets with the identity field truncated to 24 bytes after a reload.
- **Crash (PR\_0000017435)** — Configuring a switch using the CLI command **include-credentials** may cause an unexpected reboot if the switch has never had the feature previously enabled. The task in the crash message varies.

- **Authentication (PR\_0000011917)** — The switch does not recognize the "session-timeout" attribute from a RADIUS server following MAC authentication.
- **Authentication (PR\_0000016211)** — If no RADIUS server is accessible during a re-authentication attempt, the clients will remain connected to an auth-vid even if an unauth-vid was defined.
- **Crash (PR\_0000012405)** — If a port is added to an existing trunk group on a switch with jumbo frames configured, the port banks may reset, logging messages similar to the following in the event logs.

```
chassis: Slave ROM Tombstone: 0x13000601
ports: trunk Trk2 is now inactive
chassis: Msg loss detected - no ack for seq # 37230
```

- **Switch Hang (PR\_0000014307)** — A switch with 802.1X configured may stop passing AAA requests and routed traffic. Over time this issue manifests itself in the form of lost TELNET and SSH access, and eventually even console access to its management is lost. Clients that attempt to authenticate will get a "domain not available" message. The switch must be reloaded to recover from this state.
- **Crash (PR\_0000009411)** — A switch with 802.1X and RADIUS accounting configured may experience an unexpected reboot with a message similar to the following.

```
Software exception at aaa8021x_proto.c:255.
```

- **802.1X (PR\_0000009344)** — The switch sends an EAP-notification out to the client as a result of the Radius server sending a Reply-Message in the Access-Accept packet after EAP-Success. This fix follows the suggestion in RFC 3579, section 2.6.5 and silently discards attributes sent out after the authentication is complete.
- **CLI (PR\_0000007572)** — The CLI command **password port-access username <username> plaintext <password-string>** is inappropriately available without the prerequisite include-credentials configuration.
- **SNMP (PR\_0000004133)** — SNMP *informs* are not sent by the switch when they should be sent.
- **Virtual Stacking (PR\_0000007320)** — Virtual stacking passwords do not propagate from Commander to Members as required by the feature.
- **802.1X (PR\_0000010850)** — If an unauth-vid is configured, and the client limit is reached on a switch port, a properly credentialed re-authentication following an improperly credentialed authentication attempt (for example, incorrect password) will leave the 802.1x client in the unauthorized VLAN instead of applying the appropriate authorized VLAN.
- **802.1X (PR\_0000005372)** — Some combinations of source and destination MAC addresses may cause 802.1X to stop functioning on a port; only a reboot will recover functionality.

- **MAC Authentication (PR\_0000011949)** — Mac authentication may fail to occur unless the switch port status is toggled.

- **Crash (PR\_0000010809)** — Changing the **aaa port-access mac-based reauth-period** on the switch may trigger an unexpected reboot with a message similar to the following.

```
Software exception at wma_bauth_sm.c:1089 -- in 'mWebAuth' task ID  
= 0xa93e880
```

- **Web Authentication (PR\_0000010189)** — When Web-Authentication is configured and there is no RADIUS server available, the authentication attempt times out prior to the amount of time expected when the configured server-timeout and max-requests are considered.
- **Web Authentication (PR\_0000016178)** — When a client connecting to the switch through Web Authentication enters the wrong credentials, the switch places the client in the unauth-vid and does not prompt for authentication retry. Once the port is in the unauthenticated state, only a reload of the switch allows for reauthentication.
- **Web Authentication (PR\_0000017374)** — Following successful Web Authentication by a client, the browser redirect (to either the configured redirect URL or the client's home page) does not work.
- **Web Authentication (PR\_0000017431)** — During Web Authentication login, the login progress pages are cached and the user is subjected to these cached pages when trying to navigate to other sites after successful authentication.
- **Crash (PR\_0000017707)** — Following configuration of Web Authentication, connection of a PC into a switch port followed by an attempt to browse the Web may trigger a switch running T.13.57 software to reboot unexpectedly with a software exception.
- **Web Authentication (PR\_0000018047)** — A Web Authentication request may return a blank page.
- **802.1X/WMA (PR\_0000017371)** — Unknown 802.1X/WMA clients take too long connect, causing very slow DHCP addressing.
- **RADIUS Accounting (PR\_0000012487)** — The switch doesn't send an accounting-stop when a switch **reload** closes the session.
- **ARP (PR\_0000037632)** — When the **ip ARP-age** is set to a low value, the re-ARP behavior is excessive.
- **CLI (PR\_0000018594)** — Attempts to utilize the CLI interface configuration command **mdix-mode mdix** yields an error setting value mdix for port <port number> on software version T.13.57.
- **10-GbE (PR\_0000038110/0000038298)** — 10-GbE X2 transceivers may fail to initialize entirely or initialize only after a long delay.

## Release T.13.61

The following problems were resolved in release T.13.61. (Never released.)

- **Port Communication (PR\_0000018161)** — On some driver/firmware revisions, the Intel 82566DM and 82566DM-2 gigabit NIC chipsets may send an excessive number of corrupt packets. This traffic may affect communication on the port attached to the problem NIC, or on another port on the same module or port-bank. This fix helps to ensure continued communication by downgrading the port setting to auto-10/100, and logging an FFI message in the event log. The event log message will be similar to the following, and will indicate the port that is receiving the problem traffic. Please check with your PC vendor to see if there is an updated firmware version available for the affected NIC.

02671 FFI: Port <number> has been downgraded to 10/100. See  
[www.procurve.com/device\\_help/nic\\_update](http://www.procurve.com/device_help/nic_update) for details.

- **Config (PR\_0000018667)** — A config file upload to the switch fails if **dhcp-snooping trust** is configured on Trk1. The switch CLI will report an error referencing the configuration line, as shown below.

Port Trk1 is invalid.  
Corrupted download file.

- **Config (PR\_0000000914)** — The configuration parameter **unknown-vlans <learn | block | disable>** cannot be pre-configured on a transceiver not currently inserted; the switch will report Error setting value block for port <number>.
- **CLI (PR\_0000016116)** — When the **include** parameter is used with a **show** command, and the switch finds a matching regular expression, the console output contains all-zero byte.
- **Counters (PR\_0000018242)** — The **clear statistics <portlist>** command is clearing the statistics across all sessions, rather than for the current management session only. In order to clear statistics on all ports and across all sessions, the **clear stats global** command should be used.
- **GVRP (PR\_0000014896)** — GVRP-learned VLANs are not being propagated out 10-GbE ports.
- **CLI Help (PR\_0000010484)** — The CLI tab completion for the command parameter **[ethernet] PORT-LIST** should list the **all** option, but it does not.

## Release T.13.62

The following problems were resolved in release T.13.62. (Never released.)

- **Web Authentication (PR\_0000018869)** — After redirection to the login page, and successful login using Web Authentication, the initial URL cannot be reached.



- **MSTP (PR\_0000011865)** — The spanning-tree port priority reported by the CLI command **show span instance <x>** incorrectly reports 0 for the priority instead of 128 (the default/mean value). If a valid port priority value is manually configured, the switch properly reports the assigned value.
- **Web-Authentication (PR\_0000037681)** — When **peap-mschapv2** is configured within the **aaa authentication** CLI command, usernames that include a backslash "\" character delimiter fail Web-authentication.
- **Port Communication (PR\_0000017032/0000037992)** — Invalid/corrupt packets sent to the switch by a NIC operating at gigabit speed may trigger a loss of communication on a different port that shares the same ASIC. In that case, the port will retain its link and the Rx bytes, ifInDiscards, and the Discard Rx counters increment. Prior to this fix, communication on the port could only be reliably recovered by switch reload. This problem may also be associated with the following event log messages.

```
00374 chassis: Slot <x> Slave ROM Tombstone: 0x13000601
00374 chassis: Slot <x>: Lost Communications detected - Heart Beat
Lost
```

## Release T.13.63

The following problems were resolved in release T.13.63.

- **FFI/Config (PR\_0000039989)**

**FFI** — If an FFI event is triggered, and then the link is brought down and back up again, the same FFI event will be triggered again in about 20 seconds even if the trigger condition isn't met.

**Config** — Configuration changes made for PR\_0000018161, page 96, are not visible to the user; it appears that a port configured at both the NIC and the switch for auto-gig is operating at 100FDx for no reason (particularly if the associated event log message has scrolled out of the switch log). This fix makes the downgrade of the port to auto-10/100 visible in the running configuration. Note that this may trigger the switch to ask "Do you want to save current configuration?" upon logout or switch reload.

- **802.1X (PR\_0000012724)** — When multiple clients are authenticated through MAC-authentication, if the users have different nas-filter-rules, the second (or subsequent) users will not get authenticated.
- **Web/FFI (PR\_0000040095)** — The Web Management Interface Alert Log message does not match the FFI log message for PR\_0000018161 on page 96.

## Release T.13.64

The following problems were resolved in release T.13.64 (not a public release).

- **GVRP (PR\_0000012224)** — Changing the GVRP **unknown-vlan** state from 'block' to 'learn' and vice versa stops all GVRP advertisements from that interface until the interface is disabled and then re-enabled.
- **IGMP (PR\_0000018494)** — IGMP joins may cause multicast streams to flood, briefly, across the VLAN.
- **Crash (PR\_0000007631)** — The switch or port bank may reboot unexpectedly with a software exception due to a failure to release message buffers. The crash message may be similar to the following.

```
Software exception at bttfLPR.c:7  
2 -- in 'mAdMUpCtrl', task ID = 0xe47038
```

- **LLDP (PR\_0000038230)** — The length of a CDP packet may prevent the switch from accepting the packet.

## Release T.13.65

The following problems were resolved in release T.13.65 (not a public release).

- **Enhancement (PR\_0000016965)** — Debug logging enhancements have been made so that task name prefix, time stamp prefix, and other types of information are available to improve the troubleshooting processes.
- **Enhancement (PR\_0000017230)** — Crash data has been improved in order to help speed time to problem resolution.
- **Port Communication (PR\_0000040651)** — Switches running T.13.57 and newer software may see an increased likelihood of port toggling (repeated online/offline/online) on gigabit ports.
- **Crash (PR\_0000015145)** — The switch may reboot unexpectedly due to memory depletion. The crash message may be similar to the following.

```
NMI event SW:IP=0x008ff314 MSR:0x00029210 LR:0x008ff2fc  
Task='mSnmpCtrl' Task ID=0x8809d30
```

- **Crash (PR\_0000018505)** — The switch may reboot unexpectedly due to memory depletion, logging a crash message similar to the following,

```
NMI event SW:IP=0x009009c8 MSR:0x00029210 LR:0x009009b0 Task='mIpPk-  
tRecv' Task ID=0x84baba0
```

- **Web Authentication (PR\_0000037786)** — Login progress pages provided during Web Authentication give the end-users an "Access Granted" page prior to completion of the network transition. Better dialogue with clearer instructions to end-users is implemented with this fix.
- **Crash (PR\_0000039315)** — The switch may reboot unexpectedly due to memory depletion when the CLI configuration command `lldp enable-notification <port-list>` is configured to send the output via an SNMP trap.
- **Crash (PR\_0000016958)** — The switch may reboot unexpectedly when a second SSH session is established with the switch management while the switch is transferring a `show tech custom` file to a TFTP server. The crash message will be similar to the following.  

```
Software exception at exception.c:501 -- in 'mSess3', task ID =  
0x8280a60-> Memory system error at 0x60 - memPartFree
```
- **Crash (PR\_0000041168)** — Running or copying the output from the CLI command `show tech` causes a memory leak that will eventually result in memory depletion and switch reboot. The crash messages vary widely, and may include PPC errors, NMI errors, and "Out of resources: no token found" errors.

## Release T.13.66

The following problems were resolved in release T.13.66 (never released).

- **SSH (PR\_0000003030)** — The default behavior when the CLI command `clear crypto client-public-key` is executed is to delete the operator level key only. The additional CLI argument of `<operator | manager>` is not explicitly required for operator level deletion. If only a manager key is configured, it might appear to the user as if the client-public-key is not getting removed appropriately. This fix introduces an additional verification that indicates the level of key being deleted, as illustrated in the example below.  

```
ProCurve Switch(config)# clear crypto client-public-key  
All Operator level public keys will be deleted, do you want to  
continue [y/n]
```
- **Counters (PR\_0000016513)** — Beginning with software version T.13.45, the menu and Web management interfaces display the port number in the 'Giants Rx' and 'Total Rx Error' counters. Use of the CLI command `clear statistics global` or selection of 'reset' from the menu interface on the port does not clear these two anomalous values. Workaround: View the port counters using the CLI command `show interface <port number>`.
- **CLI (PR\_0000015982)** — Using the port-security feature, attempts to enter more than the configured MAC address limit on a port result in an ambiguous error message: `Inconsistent value`. This fix triggers a more appropriate error message: `Warning: Number of configured addresses on port 3 exceeds address-limit`.

- **Authentication (PR\_0000003486)** — Failure to authenticate to the switch management creates an event log entry as it should, however, the information being logged is missing where the failure was seen, (e.g. CONSOLE or TELNET).
- **CLI (PR\_0000015197)** — The CLI response to **show int eth <port number>** displays only the second half of the first byte of the MAC address. The switch response to **show mac** and other commands that list the MAC address accurately display the proper format of MAC addresses.
- **Config (PR\_0000000913)** — The switch does not allow the user to configure a VLAN to be monitored if mirror port is a transceiver or mini-GBIC that is not yet inserted. When the attempt is made, the switch reports an error: `Invalid value`.
- **Config (PR\_0000000915)** — The switch does not allow the user to configure monitoring of a port if that port is a transceiver or mini-GBIC not yet installed in the switch. When the attempt is made, the switch reports an error: `Invalid value`.
- **Crash (PR\_0000002449/0000002511)** — The switch may reboot unexpectedly with a software exception when MSTP is configured.
- **CLI Help (PR\_0000000845)** — The `<cr>` option is accepted (but should not be) in the tab completion help for the CLI command **task-monitor**.
- **MAC Authentication (PR\_0000015520)** — Traffic from unauthenticated clients may be allowed during the process of authenticating clients under heavy loads.
- **Config (PR\_0000002749/1000799983)** — The positions of SNTP and SNMP servers in the config file is changed in T.13 compared to previous major revisions.
- **CLI (PR\_0000010378)** — Session time (sec.) remains at zero in response to the CLI command **show port-access authenticator <port> session-counters**; it should increment.
- **sFlow (PR\_0000015656)** — Outbound sampling using sFlow is not functioning.
- **sFlow (PR\_0000012123)** — The switch does not allow sFlow to be configured on a mirror port.
- **Switch Hang (PR\_0000005332)** — If the switch is reloaded during a configuration save, there is a very small chance that the switch may become unresponsive and require the switch to be reset or power cycled.
- **Config (PR\_0000008649)** — A configuration migrated from an earlier major revision of software may allow the import of an invalid IP address - loading that same configuration from TFTP would provide an appropriate error.
- **SNMP (PR\_0000014902)** — SNMP traps contain the wrong instance number for the event Description (the eventDescription is one instance number too low).

- **Config (PR\_0000005084)** — If an attempt is made to remove a configured IP address from the switch configuration using a command that does not match the IP address' configured subnet mask, the switch is erroneously removing the IP address instead of providing an appropriate error.
- **Stacking (PR\_0000013054)** — In switches configured for virtual stacking, TELNET from the Commander to the stack members does not work from the CLI.
- **Crash (PR\_0000002589)** — Ping of an invalid IP address multiple times may trigger an unexpected reboot.
- **Crash (PR\_0000009930)** — The switch may reboot unexpectedly when being configured with a VLAN IP address at starts with 46 (46.x.x.x.x). The crash message may be similar to the following.

```
Software exception at ConfigRecIndex.cc:424 -- in 'mSnmpCtrl', task ID  
= 0xa92fec0
```

- **MLD (PR\_0000002665/1000756980)** — The forced fast leave timeout portion of the CLI display for the command **show ipv6 mld config** does not state the unit of measure.
- **Crash (PR\_0000002841/1000761185)** — Switches configured for virtual stacking may reboot unexpectedly with a crash message similar to the following.  

```
Software exception at bttdDma.c:784 -- in tDevPollTx',
```
- **CLI (PR\_0000002852/1000795603)** — When an attempt is made to configure the switch with an IP address after the maximum number of addresses has been reached, an inaccurate error message is displayed: `This is a subnet-router anycast address.`
- **CLI (PR\_0000002849/1000764523)** — The switch provides a generic error, `Unable to create vlan <id> ipv6 mld <port-list> records` when it should indicate that the VLAN in question cannot have mld configured without having pre-requisite port membership.
- **IGMP (PR\_0000007402)** — IGMP port participation is not expiring after the time-out period.
- **Port Authentication (PR\_0000010737)** — Configuration of 802.1X after MAC-Authentication will override the MAC-Auth logoff-period value. With this fix, the switch accurately reflects the fact that all logoff timers on a port (802.1X, MacAuth, WebAuth) are functionally identical; i.e. writing a value to one will automatically write them all.
- **802.1X (PR\_0000041041)** — The switch may reach a point at which it will no longer be able to authenticate 802.1X clients until it is reloaded. The speed at which this occurs is dependent on the rate of 802.1X connection attempts.

- **Port Authentication (PR\_0000016949)** — Port (MAC or Web) Authentication is randomly 'Blocked by AAA' as reported in the event log. Output from the CLI command **show port-access < mac-based | web-based >** shows neither an authenticated nor an unauthenticated client when this occurs. The correct behavior is to move unauthenticated clients to the unauth VLAN.
- **Port Connectivity (PR\_0000038601)** — The time between a port coming up and that port being online and passing traffic varies, and at times, may be extended to over a minute.
- **CLI (PR\_0000041272)** — CLI output from the commands **show port-access web clients** or **show port-access web clients detailed** only displays the client information the first port that is active (i.e. has authenticated or unauthenticated clients). All other ports will not show any clients, even if the port has several authenticated or unauthenticated clients.
- **Crash (PR\_0000041815)** — When the CLI configuration parameter **logging priority-descr** is modified, the switch may (eventually) reboot unexpectedly due to memory depletion.
- **STP (PR\_0000017189)** — When the switch is running in RSTP-mode (through the use of the CLI configuration command **spanning-tree force-version rstp-operation**) and MSTI settings are still present in the switch, a TCN is triggered when the MSTI settings are modified or removed.
- **Config (PR\_0000041014)** — When the CLI command **no module** is used to remove a module's configuration, the switch does not clear corresponding aaa configuration as it should.
- **Crash (PR\_0000041445)** — When Web Authentication is in use, the switch may experience conditions that cause it to reboot unexpectedly with a crash message similar to the following.  
  

```
Software exception at buffers.c:2231 -- in 'tHttpd', task ID = 0x80d25b0
```

## Release T.13.67

The following problems were resolved in release T.13.67.

- **DHCP-Snooping (PR\_0000039481)** - When DHCP-snooping is enabled, the switch changes the DHCP-Request Packets (removing the "option end" flag (0xff) at the end of the options field) as they travel from server to client. Workaround: Disable DHCP-relay option 82.
- **Crash (PR\_0000042176/0000041586)** - On switch software version T.13.65, entry or upload of multi-line CLI config commands may cause the switch to reboot unexpectedly with a message similar to the following.

```
PPC Data Storage (Bus Error) exception 0x300: esf=0x082e6058  
addr=0x942201fc ip=0x001c7910 Task='mSess1' tid=0x82e6b20
```

## Release T.13.68

The following problems were resolved in release T.13.68.

- **QoS (PR\_0000042343)** — QoS on Ports may not behave correctly when trunks are involved, e.g., if QoS is configured on a port that is a member of a trunk, the CLI command **no qos** does not disable the feature as it should.
- **QoS (PR\_0000039751)** — Strict outbound queuing is being enforced on trunk ports; when traffic is egressing (sent out of) a trunk port on multiple queues, the higher priority queues will starve out lower priority queues when oversubscribed.
- **IP Communication (PR\_0000042790)** — A very busy switch may cease all IP communication when the CLI command **show tech route** is executed. Messages similar to the following may be seen in the event log when this occurs.

```
W <date> <time> 00436 NETINET: 1 route entry creation(s) failed.  
W <date> <time> 00075 system: Out of pkt buffers; miss count: 0
```

- **Port Communication (PR\_0000043048)** — On software version T.13.66 or higher, the switch will not allow a port to link if the MDIX-MODE is set to MDI or MDIX (only the autoMDIX setting will allow link).
- **10-GbE (PR\_0000043292)** — Some J8438A HP ProCurve 10-GbE X2-SC ER Optics (a subset of those with serial number containing the letters DM in the middle) do not turn on the laser after the switch reboots. Workarounds: Hotswap the optic, update to a software version with the fix, or request a replacement.

## Release T.13.69

The following problems were resolved in release T.13.69. (Never released.)

- **SNMP/IPv6 (PR\_0000039353)** — An SNMP walk of the ipAddressType at the switch CLI (**walkmib 1.3.6.1.2.1.4.34.1.4**) erroneously shows all IPv6 address types as 'anycast'.
- **Crash (PR\_0000038431)** — When the Web Management Interface is used for port security configuration of 44 or more ports concurrently (Security > Port Security > Select 44 ports > click on 'Set Security Policy for the Selected Ports') the switch will reboot unexpectedly with a message similar to the following.

```
PPC Bus Error exception vector 0x300:  
Stack-frame=0x033ace80 HW Addr=0x37392c38 IP=0x0047ade0 Task='tHttpd'  
Task ID=0x33ad408 fp: 0x0000001c sp:0x033acf40 lr:0x
```

- **CLI (PR\_0000038055)** — When **startup-default** settings are configured for flash location or configuration, these settings are ignored when the CLI command **reload** is executed. Both the **reload at** and **reload after** CLI commands honor the **startup-default** settings as they should.

- **Crash (PR\_0000041031)** — Rarely, an attempt to enter the CLI configuration parameter **ip-recv-mac-address** on a VLAN may cause an unexpected reload. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary. The crash message may be similar to the following.

Software exception at hwBp.c:156 -- in 'eDevIdle', task ID = 0xabc3240

- **Crash (PR\_0000041493)** — Rarely, an attempt to configure an SNMPv3 user may cause a switch running to reboot unexpectedly with the following message. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at hwBp.c:156 -- in 'eDevIdle', task ID = 0xabeb240

- **Crash (PR\_0000039688)** — Rarely, an attempt to configure an IP address for a timep server will trigger an unexpected reload with a crash message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at hwBp.c:156 -- in 'eDevIdle', task ID = 0xabc3240

- **Crash (PR\_0000038735)** — Rarely, an attempt to configure an **ip dns server-address** will result in an unexpected reload, with a crash message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at hwBp.c:156 -- in 'mIpPktRecv', task ID = 0x853b2e

- **Crash (PR\_0000012124)** — Rarely, at switch startup, a switch configured for meshing will reboot unexpectedly with a crash message similar to the following.

Software exception at ldbal\_util.c:2525 -- in 'mLdBalCtrl', task ID = 0xa971300

- **DHCP Snooping (PR\_0000040580)** — Configuration of trust status for DHCP-snooping on ports participating in a dynamic trunk yields undesirable results when the ports of the trunk are removed. This configuration should not be allowed on dynamic trunks (e.g. **dhcp-snooping trust Dyn1**) and this fix enforces that limitation at the CLI with an error message.
- **SFTP (PR\_0000015791)** — SFTP returns to a prompt immediately after initiation of switch image upload; the image is written in the background. However, if a subsequent upload attempt is made while the first is still in progress, the switch gets into a state in which it will no longer attempt to upload any image. This fix triggers the switch to reject a file upload request if there is already a flash write in progress.
- **RADIUS Accounting (PR\_0000017924)** — When AAA Accounting is used for commands (i.e. **aaa accounting commands <start-stop | stop-only> radius**), the Calling-Station-ID value sent is incorrect.



- **DHCP (PR\_0000002817/1000462986)** — When the switch is acting as a DHCP relay agent, it uses UDP port 68 as the source for sending messages to the server. This fix changes the UDP source port for such communication to port 67.
- **Crash (PR\_0000041029)** — Rarely, and attempt to configure **ip rip** within the VLAN context will cause the switch to reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at hwBp.c:156 -- in 'eDevIdle'

- **CLI (PR\_0000007920)** — When the IP default gateway has been manually configured, the CLI command **no ip default-gateway** does not remove it if the IP address on the VLAN is configured for DHCP.
- **Crash (PR\_0000041028)** — Rarely, an attempt to use the CLI command **no vlan 2 ipv6 address dhcp full** will trigger an unexpected reboot with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at hwBp.c:156 -- in 'mIpCtrl', task ID = 0x8540760

- **RADIUS Accounting (PR\_0000017732)** — RADIUS accounting is incrementing the wrong counter in response to a dropped (invalid) packet from the RADIUS server.
- **Crash (PR\_0000041509)** — Removing a module that contains a mirror destination port may trigger one or more modules to reset.
- **Unauthenticated VLAN (PR\_0000010533)** — The switch allows an inherent configuration conflict; an unauthenticated VLAN (**unauth-vid**) can be configured concurrently for both 802.1X and Web/MAC authentication. This fix will not allow concurrent configuration of an **unauth-vid** for the **aaa port-access authenticator** and **aaa port-access web-based** or **aaa port-access mac-based** functions. Software versions that contain this fix will not allow this configuration conflict at the CLI. *Existing configurations will be altered by this fix*, and an error will be reported at the switch CLI and event log.

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

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

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

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

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

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

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

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

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

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

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

Message 3:

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

Event log message when the configuration is changed:

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

- **Crash (PR\_0000017415)**—Rarely, execution of the CLI command **show modules** will cause an unexpected reboot with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at hwBp.c:156 -- in 'eDevIdle', task ID = 0x89a1a70

- **Crash (PR\_0000037410)** — Rarely, various CLI configuration commands will trigger an unexpected reload with a crash message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at hwBp.c:156 -- in 'eDevIdle'

- **SNMP (PR\_0000016931)** — Link up/down traps may not be sent from switch when it transitions a link from blocking to forwarding.
- **Config (PR\_0000041561)** — Some preconfigured speed-duplex settings are removed after physical insertion or hotswap of transceivers.
- **TACACS (PR\_0000008881)** — The switch will accept invalid IP addresses and symbols in the CLI configuration of **tacacs server host <IP>**.
- **Enhancement (PR\_0000040638)** — Output from the CLI command **show config files** has been added to the CLI output for the **show tech** and **show tech all** commands.
- **Web Authentication (PR\_0000043209)** — Following successful Web Authentication, the browser redirect does not work correctly; it omits the hostname from the redirect URL.
- **Management (PR\_0000016049)** — If a console or telnet session to the switch is used to execute a CLI command (e.g. execution of the **show tech** command) and then the management session is abandoned before the task is completed (e.g. the window is closed), that session becomes unresponsive. If, at that point, another management session is established and the CLI command **kill** is executed to end the initial, now unresponsive session, the new management session will become unresponsive as well, until all sessions are in use and unresponsive.

## Release T.13.70 (Never built)

Release T.13.70 was never built.

## Release T.13.71

The following problems were resolved in release T.13.71.

- **CLI (PR\_0000044888)** — The "show system temperature" CLI command was incorrectly displaying temperature values for the Switch 2900. The Switch 2900 does not support temperature sensors. With this fix, the output from the "show system temperature" CLI command now correctly displays "No system temperature sensors are available".
- **Mini-GBIC (PR\_0000044130)** — The HP ProCurve Gigabit-SX-LC Mini-GBIC (J4858C) does not transmit after a switch reboot or hot-swap when it is used in a dual-personality port.

- **IP Communication (PR\_0000044004)** — Switches running software versions T.13.65 - T.13.68 may experience a resource leak in ICMP that eventually causes loss of IP communication with the following symptoms.
  - The switch will stop routing traffic for hosts for which it provides gateway services.
  - In-band network management stops functioning. The switch will become inaccessible via Telnet, SSH, WEB, and TFTP.
  - Console management may become very sluggish and may appear to be non-responsive.
  - Output from the CLI command **show ip route** will be corrupted.
  - A reboot is required to clear up the symptoms.
- **Web Authentication (PR\_0000044856)** — The Web-Authentication login page is not functional if a port-range has been set and a logoff period has been configured.
- **Port Authentication (PR\_0000042402)** — Configuration of 802.1X after MAC-Authentication will override the MAC-Auth logoff-period value. A previous fix (PR\_0000010737) allowed the network administrator to see that all logoff timers on a port (802.1X, MacAuth, WebAuth) are functionally identical; i.e. writing a value to one will automatically write them all. This fix allows different timers to be used for different authentication methods.
- **Enhancement (PR\_0000042147/0000042840)** — Port-Based Debug Logging Enhancement. This enhancement provides debug logging with the ability to filter debug messages related to a specific set of configured ports. When the port filter is enabled for a debug type, only the messages that have inherently refer to a specific port will be filtered. All other messages for that debug type will still be sent to debug logging. The CLI command for this enhancement is below.  
  

```
Switch# debug <security> <port-access | port-security |  
user-profile-mib> <optional detailed debug type> include port  
[PORT-LIST]
```

The following is used to remove all ports:

```
Switch# [no] debug <security> <port-access | port-security |  
user-profile-mib> <optional detailed debug type> include port
```
- **Enhancement (PR\_0000016657)** — Access Control Debug Logging changes have been made. For more information, see [“Access Control Debug Logging” on page 58](#).
- **CLI (PR\_0000012407)** — Output from the CLI command **show port-access authenticator <port number> client details** shows the Frames In and Frames Out for each client to be exactly the same and it does not increment as it should. Workaround: Output from the CLI command **show port-access authenticator <port> session-counters** shows the Frames In and Frames Out incrementing correctly.

- **802.1X (PR\_0000037816)** — 802.1X does not allow for authentication of new clients when the client-limit is reached; unauthenticated clients contribute to the client-limit. This fix gives authenticated users precedence over unauthenticated users. In addition, the relevant 'show' commands are updated to display clients in the unauthenticated state so the administrators will have the ability to see unintended users on a port.

- **802.1X (PR\_0000044041)** — When a large number of 802.1X supplicants logs off single port simultaneously, the switch may reboot unexpectedly, logging a crash message similar to the following.

```
Software exception at aaa8021x_util.c:2265 -- in 'm8021xCtrl', task ID  
= 0x84c1a10
```

- **Port Access (PR\_0000043432)** — CLI output from the command **show port-access authenticator** does not update the authenticated client list for local authentication clients.
- **Crash (PR\_0000043538)** — When multiple 802.1X users try to authenticate simultaneously, the module or port bank may reset unexpectedly with a messages similar to the following.

```
chassis: Slot B: Msg loss detected - no ack for seq #  
chassis: Slot B: Lost Communications detected - Source Message  
System(50)  
chassis: Slot B Slave ROM Tombstone: 0x13000601
```

```
Software exception at interrupts_bts.c:294 -- in 'tMsgCount', task  
ID = 0x4489bb1c
```

- **Crash (PR\_0000043740)** — When switch ports are configured for both 802.1X authenticator and MAC-authentication, with different authenticated VLAN ID's for each, the switch may reboot unexpectedly with a software exception as they try to authenticate a client using both methods simultaneously. One of the following messages may be recorded by the switch crash log.

```
Software exception at portsecMaster_util.c:1088 -- in m8021xCtrl'  
or
```

```
Software exception at portsecMaster_util.c:1093 -- in m8021xCtrl'
```

- **Port Access (PR\_0000017541)** — The switch allows an inherent configuration conflict; port-based 802.1X should not be allowed concurrently with Web and MAC authentication.
- **Crash (PR\_0000043765)** — Switches performing port-access authentication may experience an unexpected reboot with crash message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at radius_request.c:1472 -- in 'mRadius006', task  
ID = 0x8320
```

- **Crash (PR\_0000044225)** — When multiple MAC-authentication clients attempt to log in to the switch with a RADIUS-assigned VLAN unknown to the switch, the switch may reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at radius\_util.c:463 -- in 'mRadius006', task ID = 0x8306d60

- **Crash (PR\_0000044219)** — When the switch is configured for web-auth with client moves enabled using the CLI command 'aaa port-access web-based <port-list> client-moves', if a client is authenticated on one port and moves to another port (also configured for web-auth), the switch may reboot unexpectedly with a crash message similar to the following. Note that this problem was found and fixed on an internal software development build; symptoms in released software may vary.

Software exception at wma\_client\_sm.c:387 -- in 'mWebAuth', task ID = 0x8379a70

- **Web-Authentication (PR\_0000042390)** — The Web-authentication login page is no longer functional after there has been a configuration change in the DHCP range the switch uses for Web-auth.
- **Crash (PR\_0000043188)** — Rarely, downloading a config file from a TFTP server to the switch may cause the switch to reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at hwBp.c:156 -- in 'tDcacheUpd', task ID = 0xa9835c0

- **RADIUS Accounting (PR\_0000043555)** — When the switch is configured for RADIUS accounting of commands (**aaa accounting commands stop-only radius**), and a user has logged on to the switch via telnet, the switch sends the incorrect calling-station-id AVP in the radius-accounting-request packet. The calling-station-id AVP is supposed to list the IP address of the host from which the user has connected to the switch.
- **Crash (PR\_0000043802)** — When GVRP is configured and the switch is learning GVRP VLANs through a trunk, if GVRP is disabled on the neighboring switch, or if the neighbor switch is reloaded, the switch will reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at vls\_dyn\_reconfig.c:2487 -- in 'mGarpCtrl', task ID = 0x83b9670

- **CLI (PR\_0000043334)** — When the CLI config command **aaa port-access authenticator** is issued for a port that is part of a trunk, the error message is generic and does not let the user know the problem. This fix introduces a more specific error message.



© 2006-2009

Hewlett-Packard Development Company, LP.

The information contained herein is subject to  
change without notice.

October 2009

Manual Part Number

5991-4790