



Release Notes:

Version R.11.16 Software

for the ProCurve Series 2610 Switches

Release R.11.16 supports these switches:

- ProCurve Switch 2610-24 (J9085A)
- ProCurve Switch 2610-24/12PWR (J9086A)
- ProCurve Switch 2610-24-PWR (J9087A)
- ProCurve Switch 2610-48 (J9088A)
- ProCurve Switch 2610-48-PWR (J9089A)

These release notes include information on the following:

- Downloading Switch Documentation and Software from the Web ([page 1](#))
- Clarification of operating details for certain software features ([page 14](#))
- Software enhancements available in releases R.11.07 through R.11.16 ([page 17](#))
- A listing of software fixes included in releases R.11.07 through R.11.16 ([page 41](#))

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

Publication Number

Part Number 5991-2127
October 2008

Applicable Product

ProCurve Switch 2610-24	(J9085A)
ProCurve Switch 2610-24/12PWR	(J9086A)
ProCurve Switch 2610-24-PWR	(J9087A)
ProCurve Switch 2610-48	(J9088A)
ProCurve Switch 2610-48-PWR	(J9089A)

Trademark Credits

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. Java™ is a US trademark of Sun Microsystems, Inc.

Software Credits

SSH on ProCurve Switches is based on the OpenSSH software toolkit. This product includes software developed by the OpenSSH Project for use in the OpenSSH Toolkit. For more information on OpenSSH, visit

[http:// www.openssh.com](http://www.openssh.com).

SSL on ProCurve Switches is based on the OpenSSL software toolkit. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information on OpenSSL, visit

<http://www.openssl.org>.

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

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
www.procurve.com

Contents

Software Management

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

Downloading Software to the Switch

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

Enforcing Switch Security

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

Clarifications

General Switch Traffic Security Guideline	14
The Management VLAN IP Address	14
Management and Configuration Guide	14
Access Security Guide	15

Known Issues

Release R.11.12	16
-----------------------	----

Enhancements

Release R.11.04 Enhancements	17
Release R.11.07 Enhancements	17
Release R.11.08 through R.11.11 Enhancements	17
Release R.11.12 Enhancements	17
DHCP Snooping	17
Dynamic ARP Protection	27
Release R.11.13 Enhancements (Never released)	34
Release R.11.14 Enhancements	34
DHCP Option 66 Automatic Configuration Update	34
SSH Enhancements	36
Displaying the SSH Information	39
Logging Messages	39
Release R.11.15 Enhancements (Not a public release)	40
Release R.11.16 Enhancements	40

Software Fixes in Release R.11.04 - R.11.16

Release R.11.04	41
Release R.11.07	41
Release R.11.08	42
Release R.11.09	42
Release R.11.10	43
Release R.11.11	43
Release R.11.12	43
Release R.11.13	43
Release R.11.14 (Not a Public Release)	44
Release R.11.15	44
Release R.11.16	45

Software Management

Software Updates

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


Downloading Switch Documentation and Software from the Web

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

To Download a Software Version:

1. Go to the ProCurve Networking Web site at: <http://www.procurve.com/software>.
2. Click on **Switches**.

To Download Product Documentation: You will need the Adobe® Acrobat® Reader to view, print, and/or copy the product documentation.

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

Downloading Software to the Switch

Caution

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

HP periodically provides switch software updates through the ProCurve Networking Web site <http://www.procurve.com/software>. After you acquire the new software file, you can use one of the following methods for downloading it to the switch:

- For a TFTP transfer from a server, do either of the following:
 - Click on **Download OS** in the Main Menu of the switch's menu interface and use the (default) **TFTP** option.
 - Use the **copy tftp** command in the switch's CLI (see below).
- For an Xmodem transfer from a PC or Unix workstation, do either of the following:
 - Click on **Download OS** in the Main Menu of the switch's menu interface and select the **Xmodem** option.
 - Use the `copy xmodem` command in the switch's CLI (page 4).
- Use the download utility in ProCurve Manager Plus.
- A switch-to-switch file transfer

Note

Downloading new software does not change the current switch configuration. The switch configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another switch of the same model.

This section describes how to use the CLI to download software to the switch. You can also use the menu interface for software downloads.

TFTP Download from a Server

Syntax: `copy tftp flash <ip-address> <remote-os-file> [< primary | secondary >]`

Note that if you do not specify the flash destination, the TFTP download defaults to the primary flash.

For example, to download a software file named R_11_04.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

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

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

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

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

3. Reboot the switch.

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

Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port on a PC operating as a terminal. (Refer to the Installation Guide you received with the switch for information on connecting a PC as a terminal and running the switch console interface.)
- The switch software is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the Microsoft Windows NT® terminal emulator, you would use the **Send File** option in the **Transfer** drop-down menu.)

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

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

1. To reduce the download time, you may want to increase the baud rate in your terminal emulator and in the switch to a value such as 57600 bits per second. (The baud rate must be the same in both devices.) For example, to change the baud rate in the switch to 57600, execute this command:

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

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

2. Execute the following command in the CLI:

```
ProCurve # copy xmodem flash primary
The primary OS image will be deleted. continue [y/n]? Y
Press 'enter' and start XMODEM on your host . . .
```

3. Execute the terminal emulator commands to begin the Xmodem transfer. The download can take several minutes, depending on the baud rate used in the transfer.
4. Reboot the switch.

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

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

```
ProCurve> show system
```

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

6. If you increased the baud rate on the switch ([step 1](#)), use the same command to return it to its previous setting. (HP recommends a baud rate of 9600 bits per second for most applications.) Remember to return your terminal emulator to the same baud rate as the switch.

Saving Configurations While Using the CLI

The switch operates with two configuration files:

- **Running-Config File:** Exists in volatile memory and controls switch operation. Rebooting the switch erases the current running-config file and replaces it with an exact copy of the current startup-config file. To save a configuration change, you must save the running configuration to the startup-config file.
- **Startup-Config File:** Exists in flash (non-volatile) memory and preserves the most recently-saved configuration as the “permanent” configuration. When the switch reboots for any reason, an exact copy of the current startup-config file becomes the new running-config file in volatile memory.

When you use the CLI to make a configuration change, the switch places the change in the running-config file. If you want to preserve the change across reboots, you must save the change to the startup-config file. Otherwise, the next time the switch reboots, the change will be lost. There are two ways to save configuration changes while using the CLI:

- Execute **write memory** from the Manager, Global, or Context configuration level.
- When exiting from the CLI to the Main Menu, press **[Y]** (for Yes) when you see the “Do you want to save current configuration [y/n]?” prompt.

ProCurve Switch, Routing Switch, and Router Software Keys

Software Letter	ProCurve Networking Products
C	1600M, 2400M, 2424M, 4000M, and 8000M
CY	Switch 8100fl Series (8108fl and 8116fl)
E	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
F	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
G	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
H	Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. Switch 6108: H.07.xx and earlier
I	Switch 2800 Series (2824 and 2848)
J	Secure Router 7000dl Series (7102dl and 7203dl)
K	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, and 5400zl Series (5406zl, 5406zl-48G, 5412zl, and 5412zl-96G) and Switch 8212zl.
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 through M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 through M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
R	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
T	Switch 2900 Series (2900-24G, and 2900-48G)
U	Switch 2510-48
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
WA	ProCurve Access Point 530
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
WT	ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module
Y	Switch 2510G Series (2510G-24 and 2510G-48)
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

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		

Enforcing Switch Security

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

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

Caution:

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

Switch Management Access Security

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

Default Settings Affecting Security

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

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

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

Local Manager Password

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

Inbound Telnet Access and Web Browser Access

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

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

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

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

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

Secure File Transfers

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

SNMP Access (Simple Network Management Protocol)

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

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

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

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

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

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

snmp-server mib hpswitchauthmib excluded

Note on SNMP Access to Local Authentication MIB Objects

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

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

Front-Panel Access and Physical Security

Physical access to the switch allows the following:

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

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

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

Other Provisions for Management Access Security

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

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

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

Network Security Features

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

Web and MAC Authentication

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

Secure Shell (SSH)

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

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

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

Secure Socket Layer (SSLv3/TLSv1)

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

Clarifications

General Switch Traffic Security Guideline

Where the switch is running multiple security options, it implements network traffic security based on the OSI (Open Systems Interconnection model) precedence of the individual options, from the lowest to the highest. The following list shows the order in which the switch implements configured security features on traffic moving through a given port.

1. Disabled/Enabled physical port
2. MAC lockout (Applies to all ports on the switch.)
3. MAC Lockdown
4. Port security
5. Authorized IP Managers
6. Application features at higher levels in the OSI model, such as SSH.

(The above list does not address the mutually exclusive relationship that exists among some security features.)

The Management VLAN IP Address

The optional Management VLAN, if used, must be configured with a manual IP address. It does not operate with DHCP/Bootp configured for the IP address.

Management and Configuration Guide

- The manual for the Switch 2610 Series contains an error. The *Management and Configuration Guide*, dated December 2007, page 13-25, states:

For switches covered in this guide, 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. CLI-configured sFlow instances may be saved to the startup configuration to persist across a switch reboot.

The 2610 only supports a single sFlow collector and can only be configured via SNMP. By design, when sFlow is configured via SNMP, the sFlow-MIB OIDs that have been set do not survive a reboot.

- The *Management and Configuration Guide*, dated December 2007, in pages 10-25, 10-26, and 10-27 incorrectly indicates that the QoS Passthrough Mode is disabled by default. The factory default for QoS Passthrough Mode is **enabled**.

Access Security Guide

- The *Access Security Guide*, dated December 2007, contain incorrect references to the **password port-access** command. References are made to the **password port-access** command on pages 11-4, 11-14, 11-15, 11-16, and 11-24. The **password port-access** command is NOT supported on the HP Procurve Switch 2610 for configuring 802.1X authentication credentials.

The local operator password configured with the **password** command for management access to the switch continues to be accepted as an 802.1X authenticator credential.

Known Issues

Release R.11.12

The following problems are known issues in release R.11.12.

SSH (PR_0000003592) — Repeatedly performing crypto key generation tasks, and then connecting to the switch via SSH and executing a **show ip ssh** command may trigger a switch crash with a message similar to the following.

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

SSH (PR_0000004562) — If an SSH client disconnects and reconnects SSH sessions in rapid succession, this may trigger a switch crash that produces a message like the following.

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

Workaround: Increase to at least a five-second interval between connections.

Enhancements

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

Release R.11.04 Enhancements

No new enhancements. Initial Release.

Release R.11.07 Enhancements

Release R.11.07 includes the following enhancement:

- **Enhancement (PR_1000462847)** — Mini-GBIC slots can be configured before one is inserted.

Release R.11.08 through R.11.11 Enhancements

No enhancements, software fixes only.

Release R.11.12 Enhancements

Release K.11.12 includes the following enhancements:

- **Enhancement (PR_1000366744)** — DHCP Snooping enhancement is added. For more information, see [“DHCP Snooping” on page 17](#).

DHCP Snooping

Overview

You can use DHCP snooping to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP snooping accomplishes this by allowing you to distinguish between trusted ports connected to a DHCP server or switch and untrusted ports connected to end-

users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded. Packets from untrusted sources are dropped. Conditions for dropping packets are shown below.

Condition for Dropping a Packet	Packet Types
A packet from a DHCP server received on an untrusted port	DHCPOFFER, DHCPACK, DHCPNACK
If the switch is configured with a list of authorized DHCP server addresses and a packet is received from a DHCP server on a trusted port with a source IP address that is not in the list of authorized DHCP server addresses.	DHCPOFFER, DHCPACK, DHCPNACK
Unless configured to not perform this check, a DHCP packet received on an untrusted port where the DHCP client hardware address field does not match the source MAC address in the packet	N/A
Unless configured to not perform this check, a DHCP packet containing DHCP relay information (option 82) received from an untrusted port	N/A
A broadcast packet that has a MAC address in the DHCP binding database, but the port in the DHCP binding database is different from the port on which the packet is received	DHCPRELEASE, DHCPDECLINE

Enabling DHCP Snooping

DHCP snooping is enabled globally by entering this command:

```
ProCurve(config)# dhcp-snooping
```

Use the **no** form of the command to disable DHCP snooping.

Syntax: [no] dhcp-snooping [authorized-server | database | option | trust | verify | vlan]

authorized server: *Enter the IP address of a trusted DHCP server. If no authorized servers are configured, all DHCP server addresses are considered valid. Maximum: 20 authorized servers*

database: *To configure a location for the lease database, enter a URL in the format **ftp://ip-addr/ascii-string**. The maximum number of characters for the URL is 63.*

option: *Add relay information option (Option 82) to DHCP client packets that are being forwarded out trusted ports. The default is **yes**, add relay information.*

trust: *Configure trusted ports. Only server packets received on trusted ports are forwarded. Default: **untrusted**.*

verify: *Enables DHCP packet validation. The DHCP client hardware address field and the source MAC address must be the same for packets received on untrusted ports or the packet is dropped. Default: **Yes***

vlan: *Enable DHCP snooping on a vlan. DHCP snooping must be enabled already. Default: **No***

To display the DHCP snooping configuration, enter this command:

```
ProCurve(config)# show dhcp-snooping
```

An example of the output is shown below.

```
ProCurve(config)# show dhcp-snooping
DHCP Snooping Information
  DHCP Snooping           : Yes
  Enabled Vlans           :
  Verify MAC              : Yes
  Option 82 untrusted policy : drop
  Option 82 Insertion     : Yes
  Option 82 remote-id     : mac
  Store lease database    : Not configured
  Port Trust
  -----
  B1      No
  B2      No
```

To display statistics about the DHCP snooping process, enter this command:

```
ProCurve(config)# show dhcp-snooping stats
```

An example of the output is shown below.

```
ProCurve(config)# show dhcp-snooping stats
```

Packet type	Action	Reason	Count
server	forward	from trusted port	8
client	forward	to trusted port	8
server	drop	received on untrusted port	2

server	drop	unauthorized server	0
client	drop	destination on untrusted port	0
client	drop	untrusted option 82 field	0
client	drop	bad DHCP release request	0
client	drop	failed verify MAC check	0

Enabling DHCP Snooping on VLANs

DHCP snooping on VLANs is disabled by default. To enable DHCP snooping on a VLAN or range of VLANs enter this command:

```
ProCurve(config)# dhcp-snooping vlan <vlan-id-range>
```

You can also use this command in the vlan context, in which case you cannot enter a range of VLANs for snooping.

Below is an example of DHCP snooping enabled on VLAN 4.

```
ProCurve(config)# dhcp-snooping vlan 4
ProCurve(config)# show dhcp-snooping
```

DHCP Snooping Information

```
DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC              : Yes
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : mac
```

Configuring DHCP Snooping Trusted Ports

By default, all ports are untrusted. To configure a port or range of ports as trusted, enter this command:

```
ProCurve(config)# dhcp-snooping trust <port-list>
```

You can also use this command in the interface context, in which case you are not able to enter a list of ports.

Enhancements

Release R.11.12 Enhancements

DHCP server packets are forwarded only if received on a trusted port; DHCP server packets received on an untrusted port are dropped.

```
ProCurve(config)# dhcp-snooping trust B1-B2
ProCurve(config)# show dhcp-snooping
```

DHCP Snooping Information

```
DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC              : Yes
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : mac
```

```
Store lease database : Not configured
```

```
Port  Trust
-----
B1    Yes
B2    Yes
B3    No
```

Use the **no** form of the command to remove the trusted configuration from a port.

Configuring Authorized Server Addresses

If authorized server addresses are configured, a packet from a DHCP server must be received on a trusted port AND have a source address in the authorized server list in order to be considered valid. If no authorized servers are configured, all servers are considered valid. You can configure a maximum of 20 authorized servers.

To configure a DHCP authorized server address, enter this command in the global configuration context:

```
ProCurve(config)# dhcp-snooping authorized-server
                  <ip-address>
```

```
ProCurve(config)# show dhcp-snooping
```

DHCP Snooping Information

```
DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC              : No
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : subnet-ip
```

Authorized Servers

111.222.3.4

Using DHCP Snooping with Option 82

DHCP adds Option 82 (relay information option) to DHCP request packets received on untrusted ports by default. (See the preceding section *Configuring DHCP Relay* for more information on Option 82.)

When DHCP is enabled globally and also enabled on a VLAN, and the switch is acting as a DHCP relay, the settings for the DHCP relay Option 82 command are ignored when snooping is controlling Option 82 insertion. Option 82 inserted in this manner allows the association of the client's lease with the correct port, even when another device is acting as a DHCP relay or when the server is on the same subnet as the client.

Note

DHCP snooping only overrides the Option 82 settings on a VLAN that has snooping enabled, not on VLANS without snooping enabled.

If DHCP snooping is enabled on a switch where an edge switch is also using DHCP snooping, it is desirable to have the packets forwarded so the DHCP bindings are learned. To configure the policy for DHCP packets from untrusted ports that already have Option 82 present, enter this command in the global configuration context.

Syntax: [no] dhcp-snooping option 82 [remote-id <mac | subnet-ip | mgmt-ip>]
[untrusted-policy <drop | keep | replace>]

Enables DHCP Option 82 insertion in the packet.

remote-id *Set the value used for the **remote-id** field of the relay information option.*

mac: *The switch mac address is used for the remote-id. This is the default.*

**untrusted-
policy**

subnet-ip: *The IP address of the VLAN the packet was received on is used for the remote-id. If **subnet-ip** is specified but the value is not set, the MAC address is used.*

mgmt-ip: *The management VLAN IP address is used as the remote-id. If **mgmt-ip** is specified but the value is not set, the MAC address is used.*

*Configures DHCP snooping behavior when forwarding a DHCP packet from an untrusted port that already contains DHCP relay information (Option 82). The default is **drop**.*

drop: *The packet is dropped.*

keep: *The packet is forwarded without replacing the option information.*

replace: *The existing option is replaced with a new Option 82 generated by the switch.*

Note

The default **drop** policy should remain in effect if there are any untrusted nodes, such as clients, directly connected to this switch.

Changing the Remote-id from a MAC to an IP Address

By default, DHCP snooping uses the MAC address of the switch as the remote-id in Option 82 additions. The IP address of the VLAN the packet was received on or the IP address of the management VLAN can be used instead by entering this command with the associated parameter:

```
ProCurve(config)# dhcp-snooping option 82 remote-id  
                  <mac|subnet-ip|mgmt-ip>
```

```
ProCurve(config)# dhcp-snooping option 82 remote-id subnet-ip  
ProCurve(config)# show dhcp-snooping
```

DHCP Snooping Information

```
DHCP Snooping           : Yes  
Enabled Vlans           : 4  
Verify MAC              : Yes  
Option 82 untrusted policy : drop  
Option 82 Insertion     : Yes
```

```
Option 82 remote-id      : subnet-ip
```

Disabling the MAC Address Check

DHCP snooping drops DHCP packets received on untrusted ports when the check address (chaddr) field in the DHCP header does not match the source MAC address of the packet (default behavior). To disable this checking, use the **no** form of this command.

```
ProCurve(config)# dhcp-snooping verify mac
```

```
ProCurve(config)# dhcp-snooping verify mac
```

```
ProCurve(config)# show dhcp-snooping
```

DHCP Snooping Information

```
DHCP Snooping          : Yes
Enabled Vlans          : 4
Verify MAC             : yes
Option 82 untrusted policy : drop
Option 82 Insertion    : Yes
Option 82 remote-id    : subnet-ip
```

The DHCP Binding Database

DHCP snooping maintains a database of up to 8192 DHCP bindings on untrusted ports. Each binding consists of:

- Client MAC address
- Port number
- VLAN identifier
- Leased IP address
- Lease time

The switch can be configured to store the bindings at a specific URL so they will not be lost if the switch is rebooted. If the switch is rebooted, it will read its binding database from the specified location. To configure this location use this command.

Syntax: [no] dhcp-snooping database [file<tftp://<ip-address>/<ascii-string>>]
[delay<15-86400>][timeout<0-86400>]

file	<i>Must be in Uniform Resource Locator (URL) format — “tftp://ip-address/ascii-string”. The maximum filename length is 63 characters.</i>
delay	<i>Number of seconds to wait before writing to the database. Default = 300 seconds.</i>
timeout	<i>Number of seconds to wait for the database file transfer to finish before returning an error. A value of zero (0) means retry indefinitely. Default = 300 seconds.</i>

A message is logged in the system event log if the DHCP binding database fails to update.

To display the contents of the DHCP snooping binding database, enter this command.

Syntax: show dhcp-snooping binding

Note

If a lease database is configured, the switch drops all DHCP packets until the lease database is read. This only occurs when the switch reboots and is completed quickly. If the switch is unable to read the lease database from the tftp server, it waits until that operation times out and then begins forwarding DHCP packets.

Enabling Debug Logging

To enable debug logging for DHCP snooping, use this command.

Syntax: [no] debug dhcp-snooping [agent | event | packet]

agent	<i>Displays DHCP snooping agent messages.</i>
event	<i>Displays DHCP snooping event messages.</i>
packet	<i>Displays DHCP snooping packet messages.</i>

Operational Notes

- DHCP is not configurable from the web management interface or menu interface.
- If packets are received at too high a rate, some may be dropped and need to be re-transmitted.
- ProCurve recommends running a time synchronization protocol such as SNTP in order to track lease times accurately.

- A remote server must be used to save lease information or there may be a loss of connectivity after a switch reboot.

Log Messages

Server <ip-address> packet received on untrusted port <port-number> dropped. Indicates a DHCP server on an untrusted port is attempting to transmit a packet. This event is recognized by the reception of a DHCP server packet on a port that is configured as untrusted.

Ceasing untrusted server logs for %s. More than one packet was received from a DHCP server on an untrusted port. To avoid filling the log file with repeated attempts, untrusted server drop packet events will not be logged for the specified <duration>.

Client packet destined to untrusted port <port-number> dropped. Indicates that the destination of a DHCP client unicast packet is on an untrusted port. This event is recognized when a client unicast packet is dropped because the destination address is out a port configured as untrusted.

Ceasing untrusted port destination logs for %s. More than one client unicast packet with an untrusted port destination was dropped. To avoid filling the log file with repeated attempts, untrusted port destination attempts will not be logged for the specified <duration>.

Unauthorized server <ip-address> detected on port <port-number>. Indicates that an unauthorized DHCP server is attempting to send packets. This event is recognized when a server packet is dropped because there are configured authorized servers and a server packet is received from a server that is not configured as an authorized server.

Ceasing unauthorized server logs for <duration>. More than one unauthorized server packet was dropped. To avoid filling the log file with repeated attempts, unauthorized server transmit attempts will not be logged for the specified <duration>.

Received untrusted relay information from client <mac-address> on port <port-number>.

Indicates the reception on an untrusted port of a client packet containing a relay information option field. This event is recognized when a client packet containing a relay information option field is dropped because it was received on a port configured as untrusted.

Ceasing untrusted relay information logs for <duration>. More than one DHCP client packet received on an untrusted port with a relay information field was dropped. To avoid filling the log file with repeated attempts, untrusted relay information packets will not be logged for the specified <duration>.

Client address <mac-address> not equal to source MAC <mac-address> detected on port <port-number>. Indicates that a client packet source MAC address does not match the “chaddr” field. This event is recognized when the dhcp-snooping agent is enabled to filter DHCP client packets that do not have a matching “chaddr” field and source MAC address.

Ceasing MAC mismatch logs for <duration>. More than one DHCP client packet with a mismatched source MAC and chaddr field was dropped. To avoid filling the log file with repeated attempts, client address mismatch events will not be logged for the specified <duration>.

Attempt to release address <ip-address> leased to port <port-number> detected on port <port-number> dropped. Indicates an attempt by a client to release an address when a DHCPRELEASE or DHCPDECLINE packet is received on a port different from the port the address was leased to.

Ceasing bad release logs for %s. More than one bad DHCP client release packet was dropped. To avoid filling the log file with repeated bad release dropped packets, bad releases will not be logged for <duration>.

Lease table is full, DHCP lease was not added. The lease table is full and this lease will not be added to it.

Write database to remote file failed errno (error-num). An error occurred while writing the temporary file and sending it using tftp to the remote server.

DHCP packets being rate-limited. Too many DHCP packets are flowing through the switch and some are being dropped.

Snooping table is full. The DHCP binding table is full and subsequent bindings are being dropped.

- **Enhancement (PR_1000451356)** — Dynamic ARP Protection (DARPP) protects your network from ARP cache poisoning by dropping packets, with an invalid IP-to-MAC address binding, that are received on untrusted ports. For more information, see [“Dynamic ARP Protection” on page 27](#).

Dynamic ARP Protection

Introduction

On the VLAN interfaces of a routing switch, dynamic ARP protection ensures that only valid ARP requests and responses are relayed or used to update the local ARP cache. ARP packets with invalid IP-to-MAC address bindings advertised in the source protocol address and source physical address fields are discarded.

ARP requests are ordinarily broadcast and received by all devices in a broadcast domain. Most ARP devices update their IP-to-MAC address entries each time they receive an ARP packet even if they did not request the information. This behavior makes an ARP cache vulnerable to attacks.

Because ARP allows a node to update its cache entries on other systems by broadcasting or unicasting a gratuitous ARP reply, an attacker can send his own IP-to-MAC address binding in the reply that causes all traffic destined for a VLAN node to be sent to the attacker's MAC address. As a result, the attacker can intercept traffic for other hosts in a classic "man-in-the-middle" attack. The attacker gains access to any traffic sent to the poisoned address and can capture passwords, e-mail, and VoIP calls or even modify traffic before resending it.

Another way in which the ARP cache of known IP addresses and associated MAC addresses can be poisoned is through unsolicited ARP responses. For example, an attacker can associate the IP address of the network gateway with the MAC address of a network node. In this way, all outgoing traffic is prevented from leaving the network because the node does not have access to outside networks. As a result, the node is overwhelmed by outgoing traffic destined to another network.

Dynamic ARP protection is designed to protect your network against ARP poisoning attacks in the following ways:

- Allows you to differentiate between trusted and untrusted ports.
- Intercepts all ARP requests and responses on untrusted ports before forwarding them.
- Verifies IP-to-MAC address bindings on untrusted ports with the information stored in the lease database maintained by DHCP snooping and user-configured static bindings (in non-DHCP environments):
 - If a binding is valid, the switch updates its local ARP cache and forwards the packet.
 - If a binding is invalid, the switch drops the packet, preventing other network devices from receiving the invalid IP-to-MAC information.

DHCP snooping intercepts and examines DHCP packets received on switch ports before forwarding the packets. DHCP packets are checked against a database of DHCP binding information. Each binding consists of a client MAC address, port number, VLAN identifier, leased IP address, and lease time. The DHCP binding database is used to validate packets by other security features on the switch.

If you have already enabled DHCP snooping on a switch, you may also want to add static IP-to-MAC address bindings to the DHCP snooping database so that ARP packets from devices that have been assigned static IP addresses are also verified.

- Supports additional checks to verify source MAC address, destination MAC address, and IP address.

ARP packets that contain invalid IP addresses or MAC addresses in their body that do not match the addresses in the Ethernet header are dropped.

When dynamic ARP protection is enabled, only ARP request and reply packets with valid IP-to-MAC address bindings in their packet header are relayed and used to update the ARP cache.

Dynamic ARP protection is implemented in the following ways on a switch:

- You can configure dynamic ARP protection only from the CLI; you cannot configure this feature from the web or menu interfaces.
- Line rate—Dynamic ARP protection copies ARP packets to the switch CPU, evaluates the packets, and then re-forwards them through the switch software. During this process, if ARP packets are received at too high a line rate, some ARP packets may be dropped and will need to be retransmitted.
- The SNMP MIB, HP-ICF-ARP-PROTECT-MIB, is created to configure dynamic ARP protection and to report ARP packet-forwarding status and counters.

Enabling Dynamic ARP Protection

To enable dynamic ARP protection for VLAN traffic on a routing switch, enter the **arp protect vlan** command at the global configuration level.

Syntax: [no] arp protect vlan [*vlan-range*]

vlan-range *Specifies a VLAN ID or a range of VLAN IDs from one to 4094; for example, 1–200.*

An example of the **arp protect vlan** command is shown here:

```
ProCurve(config)# arp protect vlan 1-101
```

Configuring Trusted Ports

In a similar way to DHCP snooping, dynamic ARP protection allows you to configure VLAN interfaces in two categories: trusted and untrusted ports. ARP packets received on trusted ports are forwarded without validation.

By default, all ports on a switch are untrusted. If a VLAN interface is untrusted:

- The switch intercepts all ARP requests and responses on the port.
- Each intercepted packet is checked to see if its IP-to-MAC binding is valid. If a binding is invalid, the switch drops the packet.

You must configure trusted ports carefully. For example, in the topology in Figure 1, Switch B may not see the leased IP address that Host 1 receives from the DHCP server. If the port on Switch B that is connected to Switch A is untrusted and if Switch B has dynamic ARP protection enabled, it will see ARP packets from Host 1 as invalid, resulting in a loss of connectivity.

On the other hand, if Switch A does not support dynamic ARP protection and you configure the port on Switch B connected to Switch A as trusted, Switch B opens itself to possible ARP poisoning from hosts attached to Switch A.

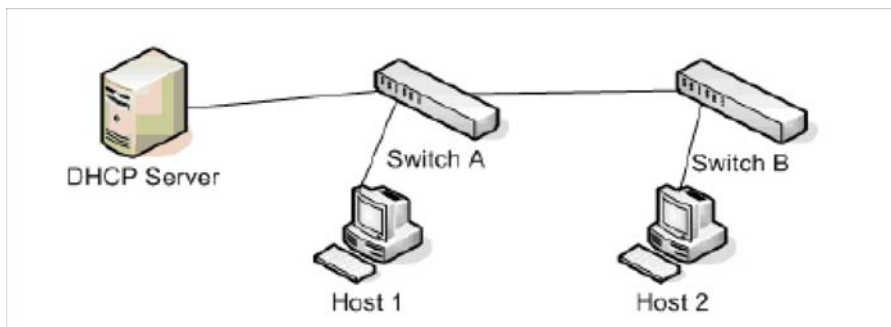


Figure 1. Configuring Trusted Ports for Dynamic ARP Protection

Take into account the following configuration guidelines when you use dynamic ARP protection in your network:

- You should configure ports connected to other switches in the network as trusted ports. In this way, all network switches can exchange ARP packets and update their ARP caches with valid information.
- Switches that do not support dynamic ARP protection should be separated by a router in their own Layer 2 domain. Because ARP packets do not cross Layer 2 domains, the unprotected switches cannot unknowingly accept ARP packets from an attacker and forward them to protected switches through trusted ports.

To configure one or more Ethernet interfaces that handle VLAN traffic as trusted ports, enter the **arp protect trust** command at the global configuration level. The switch does not check ARP requests and responses received on a trusted port.

Syntax: [no] arp protect trust <port-list>

port-list *Specifies a port number or a range of port numbers. Separate individual port numbers or ranges of port numbers with a comma; for example: c1-c3, c6.*

An example of the **arp protect trust** command is shown here:

```
ProCurve(config)# arp protect trust b1-b4, d1
```

Adding an IP-to-MAC Binding to the DHCP Database

A routing switch maintains a DHCP binding database, which is used for DHCP and ARP packet validation. Both the DHCP snooping and DHCP Option 82 insertion features maintain the lease database by learning the IP-to-MAC bindings on untrusted ports. Each binding consists of the client MAC address, port number, VLAN identifier, leased IP address, and lease time.

If your network does not use DHCP or if some network devices have fixed, user-configured IP addresses, you can enter static IP-to-MAC address bindings in the DHCP binding database. The switch uses manually configured static bindings for DHCP snooping and dynamic ARP protection.

To add the static configuration of an IP-to-MAC binding for a port to the database, enter the **ip source binding** command at the global configuration level.

Syntax: [no] ip source binding <mac-address> vlan <vlan-id> <ip-address>
interface <port-number>

mac-address Specifies a MAC address to bind with a VLAN and IP address on the specified port in the DHCP binding database.

vlan <vlan-id> Specifies a VLAN ID number to bind with the specified MAC and IP addresses on the specified port in the DHCP binding database.

ip-address Specifies an IP address to bind with a VLAN and MAC address on the specified port in the DHCP binding database.

interface <port-number> Specifies the port number on which the IP-to-MAC address and VLAN binding is configured in the DHCP binding database.

An example of the **ip source binding** command is shown here:

```
ProCurve(config)# ip source binding 0030c1-7f49c0  
interface vlan 100 10.10.20.1 interface A4
```

Note

Note that the **ip source binding** command is the same command used by the Dynamic IP Lockdown feature to configure static bindings. The Dynamic ARP Protection and Dynamic IP Lockdown features share a common list of source IP-to-MAC bindings.

Configuring Additional Validation Checks on ARP Packets

Dynamic ARP protection can be configured to perform additional validation checks on ARP packets. By default, no additional checks are performed. To configure additional validation checks, enter the **arp protect validate** command at the global configuration level.

Syntax: [no] arp protect validate [<src-mac> | <dst-mac> | <ip>]

src-mac (Optional) Drops any ARP request or response packet in which the source MAC address in the Ethernet header does not match the sender MAC address in the body of the ARP packet.

- dst-mac** *(Optional) Drops any unicast ARP response packet in which the destination MAC address in the Ethernet header does not match the target MAC address in the body of the ARP packet.*
- ip** *(Optional) Drops any ARP packet in which the sender IP address is invalid. Drops any ARP response packet in which the target IP address is invalid. Invalid IP addresses include: 0.0.0.0, 255.255.255.255, all IP multicast addresses, and all Class E IP addresses.*

You can configure one or more of the validation checks. The following example of the **arp protect validate** command shows how to configure the validation checks for source MAC address and destination MAC address:

```
ProCurve(config)# arp protect validate src-mac dst-mac
```

Verifying the Configuration of Dynamic ARP Protection

To display the current configuration of dynamic ARP protection, including the additional validation checks and the trusted ports that are configured, enter the **show arp protect** command:

```
ProCurve(config)# show arp protect

ARP Protection Information

Enabled Vlans   : 1-4094
Validate       : dst-mac, src-mac

Port   Trust
-----
B1     Yes
B2     Yes
B3     No
B4     No
B5     No
```

Figure 2. The show arp protect Command

Displaying ARP Packet Statistics

To display statistics about forwarded ARP packets, dropped ARP packets, MAC validation failure, and IP validation failures, enter the **show arp protect statistics** command:

```
ProCurve(config)# show arp protect statistics

Status and Counters - ARP Protection Counters for VLAN 1

Forwarded pkts   : 10      Bad source mac    : 2
Bad bindings     : 1       Bad destination mac: 1
Malformed pkts  : 0       Bad IP address    : 0

Status and Counters - ARP Protection Counters for VLAN 2

Forwarded pkts   : 1       Bad source mac    : 1
Bad bindings     : 1       Bad destination mac: 1
Malformed pkts  : 1       Bad IP address    : 1
```

Figure 3. Show arp protect statistics Command

Monitoring Dynamic ARP Protection

When dynamic ARP protection is enabled, you can monitor and troubleshoot the validation of ARP packets with the **debug arp protect** command. Use this command when you want to debug the following conditions:

- The switch is dropping valid ARP packets that should be allowed.
- The switch is allowing invalid ARP packets that should be dropped.

```
ProCurve(config)# debug arp protect

1. ARP request is valid
"DARPP: Allow ARP request 000000-000001,10.0.0.1 for 10.0.0.2 port A1,
vlan "

2. ARP request detected with an invalid binding
"DARPP: Deny ARP request 000000-000003,10.0.0.1 port A1, vlan 1"

3. ARP response with a valid binding
"DARPP: Allow ARP reply 000000-000002,10.0.0.2 port A2, vlan 1"

4. ARP response detected with an invalid binding
"DARPP: Deny ARP reply 000000-000003,10.0.0.2 port A2, vlan 1"
```

Figure 4. Example of debug arp protect Command

Release R.11.13 Enhancements (Never released)

No enhancements, software fixes only.

Release R.11.14 Enhancements

Enhancement (PR_000000084) — DHCP Option 66 enhancement added. For more information, see [“DHCP Option 66 Automatic Configuration Update” on page 34](#).

DHCP Option 66 Automatic Configuration Update

Overview

ProCurve switches are initially booted up with the factory-shipped configuration file. This enhancement provides a way to automatically download a different configuration file from a TFTP server using DHCP Option 66. The prerequisites for this to function correctly are:

- One or more DHCP servers with Option 66 are enabled
- One or more TFTP servers has the desired configuration file.

Caution

This feature must use configuration files generated on the switch to function correctly. If you use configuration files that were not generated on the switch, and then enable this feature, the switch may reboot continuously.

CLI Command

The command to enable the configuration update using Option 66 is:

Syntax: [no] dhcp config-file-update

Enables configuration file update using Option 66.

Default: Enabled

```
ProCurve(config)# dhcp config-file-update
```

Figure 1. Example of Enabling Configuration File Update Using Option 66

Possible Scenarios for Updating the Configuration File

The following table shows various network configurations and how Option 66 is handled.

Scenario	Behavior
Single Server serving Multiple VLANs	<ul style="list-style-type: none">• Each DHCP-enabled VLAN interface initiates DHCPDISCOVER message, receives DHCPOFFER from the server, and send DHCPREQUEST to obtain the offered parameters.• If multiple interfaces send DHCPREQUESTs, it's possible that more than one DHCPACK is returned with a valid Option 66.• Evaluating and updating the configuration file occurs only on the primary VLAN.• Option 66 is ignored by any interfaces not belonging to the primary VLAN.
Multiple Servers serving a Single VLAN	<ul style="list-style-type: none">• Each DHCP-enabled VLAN interface initiates one DHCPDISCOVER and receives one or more DHCPOFFER messages.• Each interface accepts the best offer.• Option 66 is processed only for the interface belonging to the primary VLAN.
Multiple Servers serving Multiple VLANs	<ul style="list-style-type: none">• Each DHCP-enabled VLAN interface initiates DHCPDISCOVER and receives one or more DHCPOFFER messages.• Each interface accepts the best offer.• Option 66 is processed only for the interface belonging to the primary VLAN.
Multi-homed Server serving Multiple VLANs	<ul style="list-style-type: none">• The switch perceives the multi-homed server as multiple separate servers.• Each DHCP-enabled VLAN interface initiates DHCPDISCOVER and receives one DHCPOFFER message.• Each interface accepts the offer.• Option 66 is processed only for the interface belonging to the primary VLAN.

Operating Notes

Replacing the Existing Configuration File: After the DHCP client downloads the configuration file, the switch compares the contents of that file with the existing configuration file. If the content is different, the new configuration file replaces the existing file and the switch reboots.

Option 67 and the Configuration File Name: Option 67 includes the name of the configuration file. If the DHCPACK contains this option, it overrides the default name for the configuration file (switch.cfg)

Global DHCP Parameters: Global parameters are processed only if received on the primary VLAN.

Best Offer: The “Best Offer” is the best DHCP or BootP offer sent by the DHCP server in response to the DHCPREQUEST sent by the switch. The criteria for selecting the “Best Offer” are:

- DHCP is preferred over BootP
- If two BootP offers are received, the first one is selected
- For two DHCP offers:
 - The offer from an authoritative server is selected
 - If there is no authoritative server, the offer with the longest lease is selected

Log Messages

The file transfer is implemented by the existing TFTP module. The system logs the following message if an incorrect IP address is received for Option 66:

```
Invalid IP address <ip-address> received for DHCP Option 66
```

Enhancement (PR_0000004180) — SSH enhancements added. For more information, see [“SSH Enhancements” on page 36](#).

SSH Enhancements

Overview

The SSH enhancements are:

- AES encryption (included in the K.13.02 release). A new configuration option is added to allow the server to specify the set of ciphers available for client connection.
- 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
- SSH CLI **show** command information enhancements

Specifying the Set of Ciphers

The following command allows you to specify which ciphers are available for a client to use for connection. All ciphers are available by default; use the **no** form of the command to disable specific ciphers.

Syntax: [no] ip ssh [cipher <cipher-type>]

Cipher types that can be used for connection by clients. Valid types are:

- *aes128-cbc*
- *3des-cbc*
- *aes192-cbc*
- *aes256-cbc*
- *rijndael-cbc@lysator.liu.se*
- *aes128-ctr*
- *aes192-ctr*
- *aes256-ctr*

Default: All cipher types are available.

*Use the **no** form of the command to disable a cipher type.*

```
ProCurve(config)# no ip ssh cipher 3des-cbc
```

Figure 2. Example of Disabling a Specific Cipher

Configuring Key Lengths and DSA/RSA Support

This enhancement allows you to specify the type and length of the generated host key. The command is:

Syntax: crypto key generate ssh [dsa | rsa [bits <num-bits>]]

Specify the type and length of the host key that is generated.

You can also generate and use a DSA key as the host key. The size of the host key is platform-dependent as different switches have different amounts of processing power. The size is represented by the <num-bits> key word and has the values shown in Table 5. The default value is used if **num-bits** is not specified.

Table 5. RSA/DSA Values for Various ProCurve Switches

Platform	Maximum RSA Key Size (in bits)	DSA Key Size (in bits)
5400/3500/6200/8200/2900	1024, 2048, 3072 Default: 2048	1024

Table 5. RSA/DSA Values for Various ProCurve Switches

Platform	Maximum RSA Key Size (in bits)	DSA Key Size (in bits)
2610	1024, 2048 Default: 1024	1024

Message Authentication Code (MAC) Support

This enhancement allows configuration of the set of MACs that are available for selection.

Syntax: [no] ip ssh [mac <MAC-type>]

Allows configuration of the set of MACs that can be selected. Valid types are:

- *hmac-md5*
- *hmac-sha1*
- *hmac-sha1-96*
- *hmac-md5-96*

Default: All MAC types are available.

*Use the **no** form of the command to disable a MAC type.*

Displaying the SSH Information

The **show ip ssh** command has been enhanced to display information about ciphers, MACs, and key types and sizes.

```
ProCurve(config)# show ip ssh

SSH Enabled      : No                Secure Copy Enabled : No
TCP Port Number : 22                Timeout (sec)       : 120
IP Version       : IPv4orIPv6
Host Key Type    : RSA                Host Key Size       : 1024

Ciphers : aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc,
         rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
MACs     : hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96

Ses Type      | Source IP                                     Port
-----+-----
1  console    |
2  inactive   |
3  inactive   |
4  inactive   |
5  inactive   |
6  inactive   |
```

Figure 3. Example of show ip ssh Command Showing Ciphers, MACs and Key Information

Logging Messages

There are new event log messages when a new key is generated and zeroized for the server:

```
ssh: New <num-bits> -bit [rsa | dsa] SSH host key installed
ssh: SSH host key zeroized
```

There are also new messages that indicates when a client public key is installed or removed:

```
ssh: <num-bits>-bit [rsa | dsa] client public key [installed | removed] ([manager| operator] access)
(key_comment)
```

Note: Only up to 39 characters of the key comment are included in the event log message.

Debug Logging

To add ssh messages to the debug log output, enter this command:

```
ProCurve# debug ssh LOGLEVEL
```

where LOGLEVEL is one of the following (in order of increasing verbosity):

- fatal
- error

- info
- verbose
- debug
- debug2
- debug3

Release R.11.15 Enhancements (Not a public release)

No enhancements, software fixes only.

Release R.11.16 Enhancements

No enhancements, software fixes only.

Software Fixes in Release R.11.04 - R.11.16

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

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

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

Release R.11.04

No problems resolved in release R.11.04. (Initial Release.)

Release R.11.07

The following problems were resolved in release R.11.07.

- **mini-GBIC (PR_1000754015)** — Hot Swap/Insertion of a 1000Base-T mini-GBIC requires switch to be rebooted.
 - **Broadcast Limiting (PR_1000754032)** — The broadcast limiting algorithm was not consistently applied to configured ports; the rates of throttle cycled from too high to too low (averaging to the configured value), which can present problems for latency-sensitive applications. This fix improved the consistency with which the broadcast limiting algorithm is applied to continuous traffic.
 - **MSTP (PR_1000756881)** — Some VLANs are removed from spanning-tree configuration after reboot.
 - **TFTP (PR_1000757101)** — The configuration containing **ip arp-age** cannot be copied to the switch using TFTP.
 - **VLAN (PR_1000768231)** — The switch may crash when removing a VLAN.
 - **System (PR_1000751322)** — The switch may be allowed to reboot before a new software image is fully written to flash.
 - **SCP (PR_1000428142)** — A secure **copy file** transfer will not properly close the session.
 - **ACL (PR_1000761850)** — The switch cannot support two IDM ACLs per user, per port.
 - **Counters (PR_1000759767)** — TX Drops (ifoutdiscards) are incorrectly incrementing on MSTP-blocked ports.
 - **SNMP (PR_1000763386)** — Some SNMPv3 configuration may be lost in the startup configuration after reboot.
-

- **Enhancement (PR_1000462847)** — Mini-GBIC slots can be configured before one is inserted.
- **DHCP (PR_1000753483)** — When issuing the **no dhcp-relay op 82 validate** command, the option 82 policy incorrectly changes to append.
- **Crash (PR_1000756775)** — The switch hangs after updating software and issuing a SNMP reset.

Release R.11.08

The following problems were resolved in release R.11.09. (Not a public release.)

- **Web GUI (PR_1000760153)** — A Java Error occurs when viewing the “Stack Closeup” page, causing a blank page to be displayed.
- **Authentication (PR_1000454714)** — Concurrent 802.1X and MAC-authentication does not give the 802.1X value precedence. This fix gives 802.1X VLAN assignment precedence over MAC-authentication RADIUS VLAN assignment.
- **CLI (PR_1000779621)** — If **show flash** is executed while the flash is being written, the file size is displayed. This corrects the behavior so that **show flash** shows a "0" until the writing has completed in order to avoid providing an indication that the download process has completed when it has not.

Release R.11.09

The following problems were resolved in release R.11.09. (Not a public release.)

- **CLI (PR_1000430534)** — CLI output from the show port-access mac-based command does not show the correct clients connected; some are omitted.
- **System Up-time (1000772402)** — The system up-time rolls back to zero after 49 days.
- **POE (1000750924)** — The last PoE port gets powered with limited power, even though there is sufficient power available.
- **Config (1000790501)** — When any supported transceiver is present in a mini-GBIC port, the configuration (including port-VLAN assignment) is not maintained across a reboot.
- **Radius Authentication (PR_1000779048)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. This allows the RADIUS server to reply with a large fragment which the switch does not process, causing the authentication process to fail. Workaround: set the Framed-MTU on the RADIUS server.

Release R.11.10

No problems resolved in release R.11.10. (Never Released.)

Release R.11.11

The following problems were resolved in release R.11.11. (Never Released.)

- **Crash (PR_1000795039)** — The switch may crash while uploading the configuration file, if there are extra space(s) in the configuration file header. The message is similar to:

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

Release R.11.12

The following problems were resolved in release R.11.12.

- **Enhancement (PR_1000451356)** — Dynamic ARP Protection (DARPP) protects your network from ARP cache poisoning by dropping packets, with an invalid IP-to-MAC address binding, that are received on untrusted ports. For more information, see [“Release R.11.12 Enhancements” on page 17](#).
- **Enhancement (PR_1000366744)** — DHCP Snooping enhancement is added. For more information, see [“Release R.11.12 Enhancements” on page 17](#).
- **System (PR_1000754636)** — CPU optimization.

Release R.11.13

The following problems were resolved in release R.11.13. (Never Released.)

- **VLAN (PR_000002103)** — The alteration of the VLAN/MSTP instance mapping in the pending configuration is not functioning properly. The attempt to remove any single VLAN ID (VID) from one MSTP instance and assign it to another MSTP instance fails, though specifying a VID range succeeds.
- **Crash (PR_000002579)** — Attempting to manage the switch with the browser web management interface, may cause the switch to crash with a message similar to:

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

- **Configuration (PR_1000786770)** — The switch may not reload as it should following an update of the configuration file via SCP. Sometimes, portions of the copied config are written to the running config. Event logs may show messages similar to the following.

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

Release R.11.14 (Not a Public Release)

The following problems were resolved in release R.11.14. (Not a public release.)

- **Enhancement (PR_0000000084)** — DHCP Option 66 enhancement added. For more information, see [“Release R.11.14 Enhancements” on page 34](#).
- **Enhancement (PR_0000004180)** — SSH enhancements added. For more information, see [“Release R.11.14 Enhancements” on page 34](#).
- **SSH (PR_0000003592)** — Repeatedly performing crypto key generation tasks, and then connecting to the switch via SSH and executing a **show ip ssh** command may trigger a switch crash with a message similar to the following.

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

Release R.11.15

The following problems were resolved in release R.11.15. (Not a public release.)

- **Crash (PR_0000003933)** — When the user attempts RADIUS authentication to the Web Management Interface, the switch may crash with a message similar to the following.

```
TLB Miss: Virtual Addr=0x0024c904 IP=0x0024c904 Task='tHttpd'  
Task ID=0x81e46eb0 fp:0x00000000 sp:0x81e46d70 ra:0x0024c904  
sr:0x1000fc01
```
- **DHCP (PR_0000004092)** — A ProCurve Switch 2610-48 running software version R.11.12 or greater drops DHCP packets across port banks when VLAN ID's 1024-1279 are used. Port banks are as follows: Bank 1: Ports 1-24; Bank 2: Ports 25-50. Workaround: Avoid use of VLAN IDs 1024-1279.
- **Dropped Packets (PR_0000004884)** — A ProCurve Switch 2610-48 running software version R.11.12 or greater may drop 802.1Q tagged packets with priority 4-7 between port banks. Port banks are as follows: Bank 1: Ports 1-24; Bank 2: Ports 25-50. Workaround: Disable the QoS passthrough feature using the procedure that follows.

Software Fixes in Release R.11.04 - R.11.16
Release R.11.16

```
Switch2610-48(config)# no-qos-pass-through  
Switch2610-48(config)# reload
```

Release R.11.16

The following problems were resolved in release R.11.16.

- **PoE (PR_0000005028)** — Removal of PoE controller "power management" firmware update to version 2.4.6 which was included in PR_1000750924, included in R.11.09 – R.11.15. The PoE controller firmware will remain as version 2.4.5.



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

Part Number 5991-2127
October 2008