



# Release Notes:

## Version R.11.12 Software

*for the ProCurve Series 2610 Switches*

---

### **Release R.11.12 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.11.12 ([page 15](#))
- A listing of software fixes included in releases R.11.07 through R.11.12 ([page 23](#))

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

## Publication Number

Part Number 5991-2127  
May 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](http://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

## Enhancements

Release R.11.04 Enhancements .....	15
Release R.11.07 Enhancements .....	15

Release R.11.08 through R.11.10 Enhancements .....	15
Release R.11.11 Enhancements .....	15
Release R.11.12 Enhancements .....	15
Dynamic ARP Protection .....	16

**Software Fixes in Release R.11.04 - R.11.12**

Release R.11.04 .....	23
Release R.11.07 .....	23
Release R.11.08 through R.11.10 .....	24
Release R.11.11 .....	24
Release R.11.12 .....	24

# 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.

## Downloading Software to the Switch

ProCurve Switch, Routing Switch, and Router Software Keys

# ProCurve Switch, Routing Switch, and Router Software Keys

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

## OS/Web/Java Compatibility Table

The switch web agent supports the following combinations of OS browsers and Java Virtual Machines:

Operating System	Internet Explorer	Java
Windows NT 4.0 SP6a	5.00, 5.01 5.01, SP1 6.0, SP1	Sun Java 2 Runtime Environment: – Version 1.3.1.12 – Version 1.4.2.05
Windows 2000 Pro SP4	5.05, SP2 6.0, SP1	
Windows XP Pro SP2	6.0, 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.

# 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 K.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.11.10 Enhancements

*No enhancements.*

- Versions R.11.08 through R.11.10 were never built.

## Release R.11.11 Enhancements

*No enhancements, software fixes only.*

- Version R.11.11 was never released.

## Release R.11.12 Enhancements

Release K.11.12 includes the following enhancements:

- **Enhancement (PR\_1000366744)** — DHCP Protection (Snooping) enhancement is added.
- **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 16](#).

## 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. For more information about the ARP cache, refer to “ARP Cache Table” in the *Multicast and Routing Guide*.

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

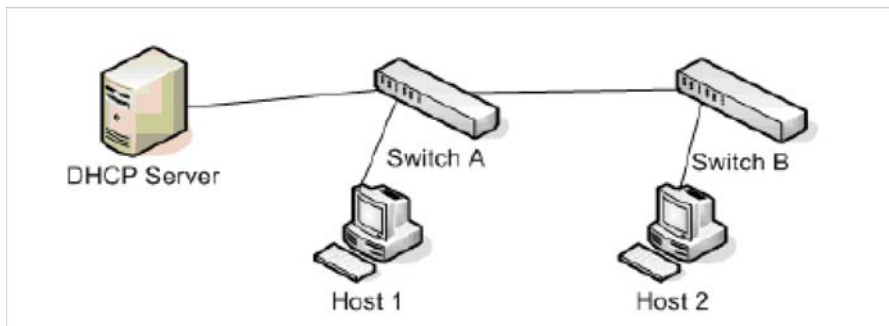
In a similar way to DHCP snooping, dynamic ARP protection allows you to configure VLAN interfaces in two categories: trusted and untrusted ports. ARP packets received on trusted ports are forwarded without validation.

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**

# Software Fixes in Release R.11.04 - R.11.12

---

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

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

Release 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

### Problems 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)** — Broadcast limiting algorithm improvements have been made.
- **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.

## Software Fixes in Release R.11.04 - R.11.12

Release R.11.08 through R.11.10

- **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 through R.11.10

Software never built.

## Release R.11.11

Software never released.

- **Crash (PR\_1000795039)** — The switch may crash during uploading of 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 enhancements were added in release R.11.012.

- **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 15](#).
- **Enhancement (PR\_1000366744)** — DHCP Protection (Snooping) enhancement is added. For more information, see [“Release R.11.12 Enhancements” on page 15](#).
- **System (PR\_1000754636)** — CPU optimization.
- **Trunks (PR\_1000772303)** — Load balancing is improved accross trunks for broadcast and multicast traffic.



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

Part Number 5991-2127  
May 2008