



Release Notes:

Version WS.02.27 Software

for the ProCurve Wireless Edge Services xl Module (J9001A) and the ProCurve Redundant Wireless Services xl Module (J9003A)

These release notes include information on the following:

- Downloading switch software and documentation from the Web ([page 1](#))
- Important Support Notes for each release ([page 5](#))
- Key software enhancements for each release ([page 17](#))
- A listing of software fixes included in each release ([page 22](#))
- Known software issues and limitations ([page 31](#))

Changes to Dynamic Frequency Selection (DFS) in the 5 GHz Band

Depending on your country/region settings on this product, the available channels in the 5 GHz band may have changed.

Customers in the U.S.

Effective July 20, 2007, new FCC regulations on the use of the 5GHz band, the band used by radios supporting the IEEE 802.11a standard, prohibit the sale of radios not meeting the new specifications. To comply with these new requirements, several channels in the ProCurve Radio Ports 220 (J9005A), and 230 (J9006A) are disabled when using this product.

This product disables channels 52, 56, 60, 64 (5.25-5.35 GHz) in the U.S. These channels remain available for use in other countries except as noted below.

Customers in the European Union and Selected Countries/Regions*

In the European Union and selected countries/regions*, ProCurve Wireless Edge Services Modules, Access Points and Radio Ports purchased after April 1, 2008, are subject to new radar interference requirements that limit the available channels in the 5 GHz band. To comply with these new requirements, the operating channels impacted by this change have been removed.

As of April 1, 2008, the factory-installed software version that ships with your product limits the available 5 GHz channels to 36, 40, 44 and 48 (5.150 – 5.250 GHz).

* Other countries/regions that apply include South Africa, Turkey, Morocco, Croatia.

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

Publication Number

Part Number 5991-3775
July 2008

Applicable Product

ProCurve Wireless Edge Services xl Module (J9001A)
ProCurve Redundant Wireless Services xl Module(J9003A)

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.

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
<http://www.procurve.com>

Contents

Software Management

| | |
|--|---|
| Software Updates | 1 |
| Downloading Software and Documentation from the Web | 1 |
| Downloading Software to the Module | 2 |
| Saving Configurations | 2 |
| Saving the Current Configuration as the Start-Up Configuration | 3 |
| ProCurve Switch, Routing Switch, and Router Software Keys | 4 |

Support Notes

| | |
|--|----|
| Release WS.02.07 | 5 |
| Reconfigure Management Passwords After a Software Update from Version WS.01.xx to Version WS.02.xx | 5 |
| Accessing the Web Browser Interface After a Software Update from Version WS.01.xx to Version WS.02.xx | 6 |
| Clear the Internet Explorer (IE) Browser Cache | 6 |
| Clear the Java Cache | 8 |
| Restart the Browser | 12 |
| Configuring Authentication for Web-Users | 14 |
| Special Characters for the ACL ID Field | 15 |
| Correction: SNMP v3 Default Password | 15 |
| Correction: Stations per Radio | 15 |
| Correction: Stations per Module in a Layer 3 Mobility Domain | 16 |
| Correction: Disabling TKIP Countermeasures | 16 |
| Clarification: Setting Intrusion Detection with TKIP Countermeasures | 16 |

Enhancements

| | |
|---|----|
| Release WS.01.11 Enhancements | 17 |
| Release WS.02.07 Enhancements | 19 |
| New and Enhanced Features | 19 |
| New Features | 19 |
| Enhancements | 20 |
| Release WS.02.26 Enhancements | 21 |
| Support for Client Location Confidence in ProCurve Mobility Manager | 21 |

Software Fixes

| | |
|------------------------------------|----|
| Release WS.01.05 | 22 |
| Release WS.01.11 | 23 |
| Releases WS.02.01 — WS.02.06 | 23 |
| Release WS.02.07 | 23 |
| Releases WS.02.08 — WS.02.10 | 24 |
| Release WS.02.11 | 24 |
| Release WS.02.12 | 28 |
| Release WS.02.14 | 28 |
| Release WS.02.21 | 29 |
| Release WS.02.26 | 29 |
| Release WS.02.27 | 30 |

Known Software Issues and Limitations

| | |
|------------------------|----|
| Release WS.01.05 | 31 |
| Release WS.01.11 | 31 |
| Release WS.02.07 | 31 |
| Release WS.02.11 | 34 |
| Release WS.02.12 | 34 |

Software Management

Software Updates

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

Downloading Software and Documentation from the Web

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

To Download a Software Version:

To obtain software updates, go to the HP ProCurve Networking Web site at:

www.procurve.com/software

and click on **Wireless services modules**. Then select the desired software version for your product.

To Download Product Documentation:

You will need the Adobe® Acrobat® Reader to view, print, or copy the product documentation.

To view or download the latest available documentation, go to the HP ProCurve Networking Web site at:

www.procurve.com/manuals

and select the desired product. On the **Manuals** page for that product, select the desired document.

Note

Documentation for this product may be found on the **Manuals** pages for the following selections:

- ProCurve Switch 5300xl series
- J9001A ProCurve Wireless Edge Services xl Module
- J9003A ProCurve Redundant Wireless Services xl Module

On the resulting Web page, double-click on a document you want. 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 Module

Caution

The startup-config file generated by the latest software release is compatible with the same file generated by earlier software releases. HP recommends that you backup your current configuration before performing any software update. See the *Management and Configuration Guide* (5013-5912) for instructions and more information.

ProCurve Networking periodically provides software updates through the ProCurve Networking Web site (<http://www.procurve.com/software>). After you acquire the new software file, use TFTP or FTP from the Web browser interface or the CLI to update the module software. See the *Management and Configuration Guide* (5013-5912) for instructions and more information.

Note

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

Saving Configurations

The module operates with two configuration files:

- **Running-Config File:** Exists in volatile memory and controls module operation. Rebooting the module 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 current configuration in the running-config file 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 module reboots for any reason, an exact copy of the current startup-config file becomes the new running-config file in volatile memory.

In the **wireless-services** context of the CLI, you may use the **write memory** command to save changes made to the running-config file to the startup-up config file. Also, the system prompts you to save any unsaved changes when you leave the **wireless-services** context.

Saving the Current Configuration as the Start-Up Configuration

When you use the CLI to make a configuration change, the module 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 module reboots, the change will be lost.

To save configuration changes while using the CLI:

1. From the **wireless-services** context:

```
ProCurve Switch 5304XL(wireless-services-B)#write memory
[OK]
ProCurve Switch 5304XL(wireless-services-B)#
```

2. Verify that the **[OK]** message displays, indicating that the configuration was saved successfully. The current configuration is now saved as the startup configuration file, and the module will execute the file at each power-up.

See the *Management and Configuration Guide* (5013-5912) for more information on managing module configuration files.

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, Switch 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 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater. |
| N | Switch 2810 Series (2810-24G and 2810-48G) |
| PA/PB | Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx) |
| Q | Switch 2510-24 |
| R | Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR) |
| T | Switch 2900 Series (2900-24, and 2900-48G) |
| U | Switch 2510-48 |
| Y | Switch 2510G Series (2510G-24 and 2510G-48) |
| VA/VB | Switch 1700 Series (Switch 1700-8 - VA.xx, Switch 1700-24 - VB.xx) |
| WA | ProCurve Wireless Access Point 530 |
| WM | ProCurve Wireless Access Point 10ag |
| WS | ProCurve Wireless Edge Services xl Module and Redundant Wireless Services xl Module |
| WT | ProCurve Wireless Edge Services zl Module and Redundant Wireless Services zl Module |
| 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.) |

Support Notes

Support Notes are listed in chronological order by software release, oldest to newest.

Release WS.02.07

The *Management and Configuration Guide* (5013-5912, May 2007) has been updated with information on enhancements and new features in software release WS.02.07. To download this guide, see [“Downloading Software and Documentation from the Web” on page 1.](#)

This section contains the following Support Notes for this release:

- [“Reconfigure Management Passwords After a Software Update from Version WS.01.xx to Version WS.02.xx”](#)
- [“Accessing the Web Browser Interface After a Software Update from Version WS.01.xx to Version WS.02.xx”](#)
- [“Configuring Authentication for Web-Users”](#)
- [“Special Characters for the ACL ID Field”](#)
- [“Correction: SNMP v3 Default Password”](#)
- [“Correction: Stations per Radio”](#)
- [“Correction: Stations per Module in a Layer 3 Mobility Domain”](#)
- [“Correction: Disabling TKIP Countermeasures”](#)
- [“Clarification: Setting Intrusion Detection with TKIP Countermeasures”](#)

Reconfigure Management Passwords After a Software Update from Version WS.01.xx to Version WS.02.xx

Module management passwords which were configured using WS.01.XX software will NOT carry forward to the module running WS.02.07 (or later) software. Manager and operator passwords will return to their default values. After an update, ProCurve strongly recommends that the module's management password be immediately reconfigured.

Accessing the Web Browser Interface After a Software Update from Version WS.01.xx to Version WS.02.xx

The Java applet in the version WS.02.XX software has been updated. To access the Wireless Edge Services xl Module's Web browser interface after an update from version WS.01.XX to WS.02.XX software, you must complete these steps:

1. Clear your browser's cache.
2. Clear the Java cache.
3. Close the browser and re-open it.

Note

This procedure also applies if you downgrade from version WS.02.XX to WS.01.XX software.

The following instructions explain how to complete the first two steps. It is assumed that you have already updated the module's software and reset the module.

Clear the Internet Explorer (IE) Browser Cache

The following steps detail the process of clearing the cache in IE version 6. If you are using a different version, your steps might vary slightly.

Follow these steps to clear the cache:

1. Open IE.

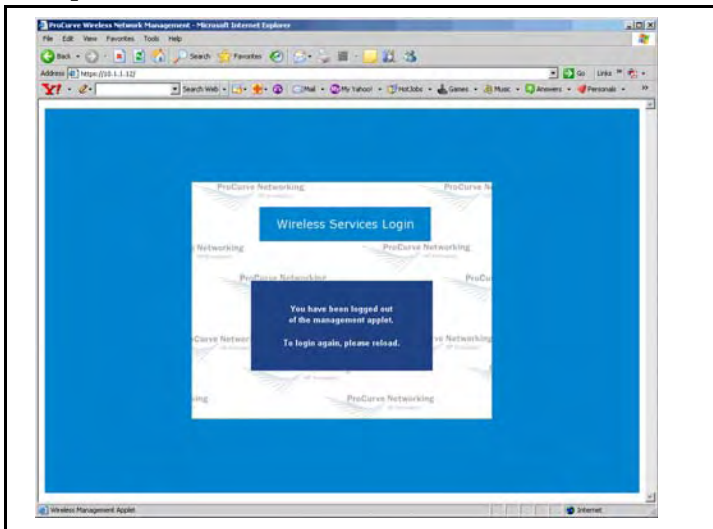


Figure 1. IE Browser

2. Select **Tools > Internet Options**. The **Internet Options** window is displayed.

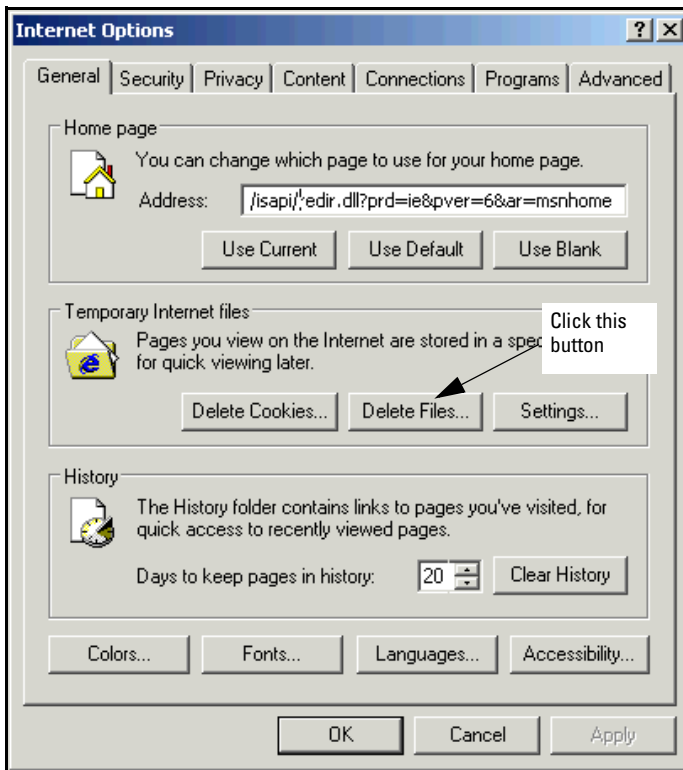


Figure 2. Tools > Internet Options

3. Make sure that you are in the **General** tab.
4. In the **Temporary Internet files** section, click **Delete Files**. The **Delete Files** window is displayed.

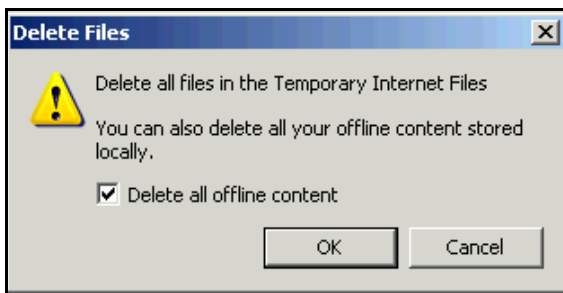


Figure 3. Delete Files

5. Check the **Delete all offline content** box.
6. Click the **OK** button.
7. In the **Internet Options** window, click the **OK** button.

Clear the Java Cache

The following steps explain how to delete the cache for Sun Java version 1.5 or higher on a Windows XP machine. The steps vary depending on whether your Java version is above or below. See either:

- [“Clear the Cache for Sun Java Versions 1.5 and Higher”](#) on page 8
- [“Clear the Cache for Sun Java Versions Prior to 1.5”](#) on page 11

Clear the Cache for Sun Java Versions 1.5 and Higher. Follow these steps to delete the Java cache:

1. Select **Start > Settings > Control Panel**.

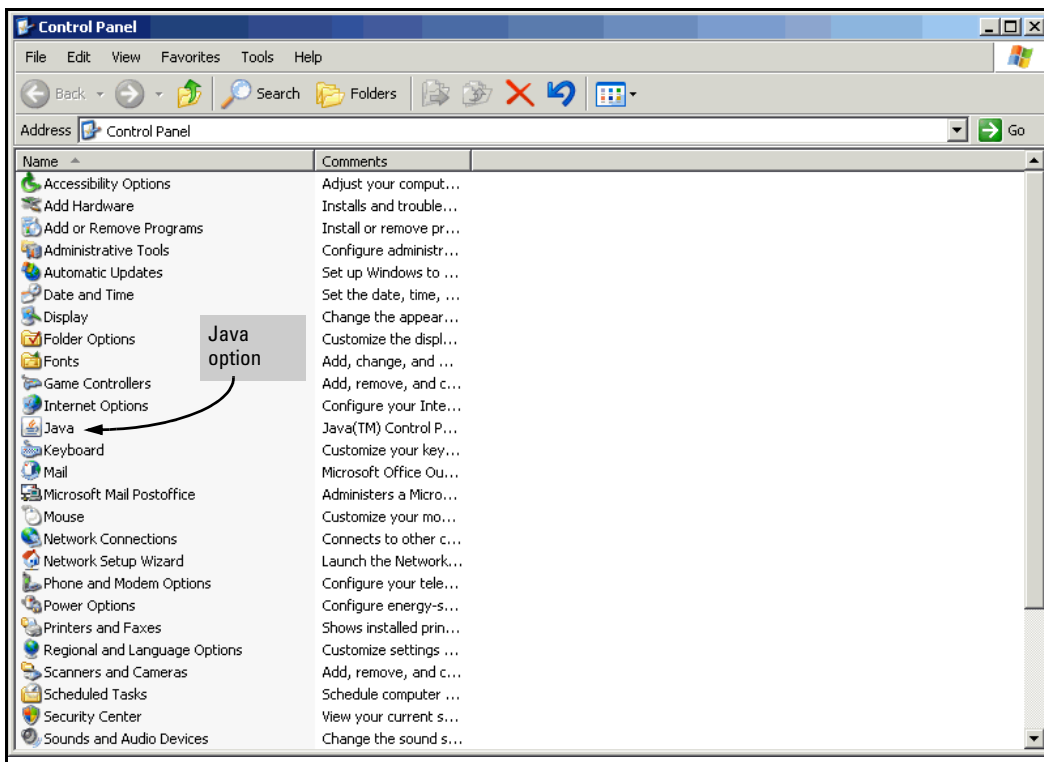


Figure 4. Control Panel

2. Select **Java**. The **Java Control Panel** window is displayed.

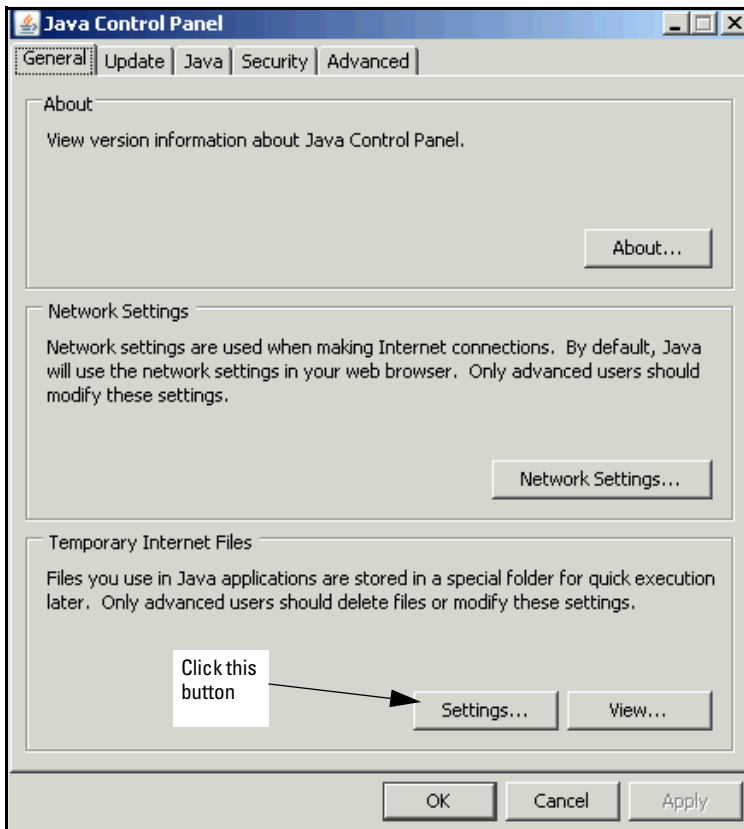


Figure 5. Java Control Panel

3. In the **Temporary Internet Files** section, click the **Settings** button. The **Temporary Files Settings** window is displayed.

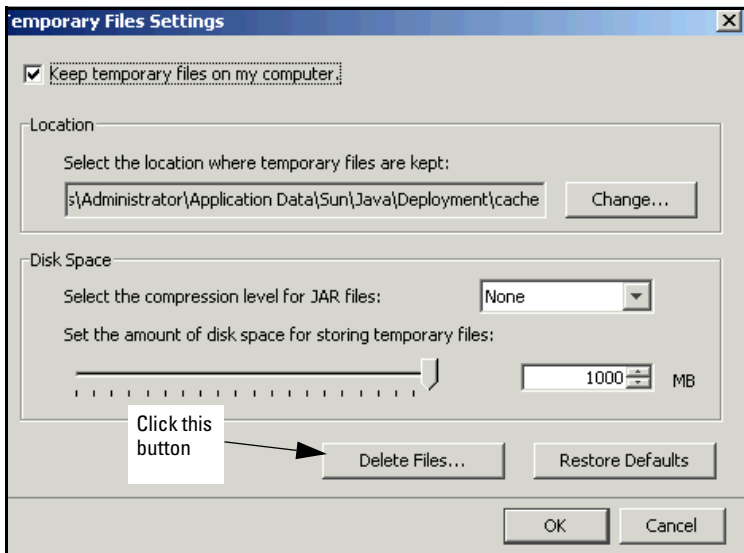


Figure 6. Temporary Files Settings (Java Control Panel)

4. Click the **Delete Files** button. The **Delete Temporary Files** window is displayed.

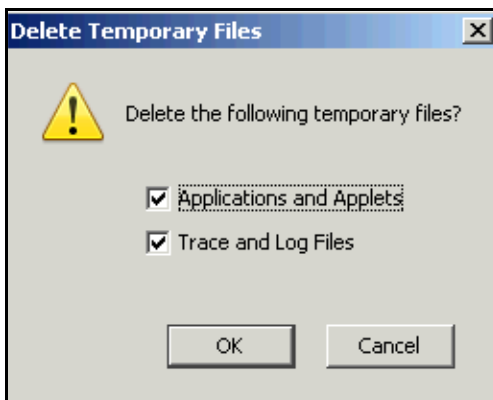


Figure 7. Delete Temporary Files (Java Control Panel)

5. Make sure that the **Applications and Applets** box is checked.
6. Click the **OK** button.
7. In the **Temporary Files Settings** window, click the **OK** button.
8. In the **Java Control Panel** window, click the **OK** button.

Clear the Cache for Sun Java Versions Prior to 1.5. Follow these steps to delete the Java cache:

1. Select **Start > Settings > Control Panel**.

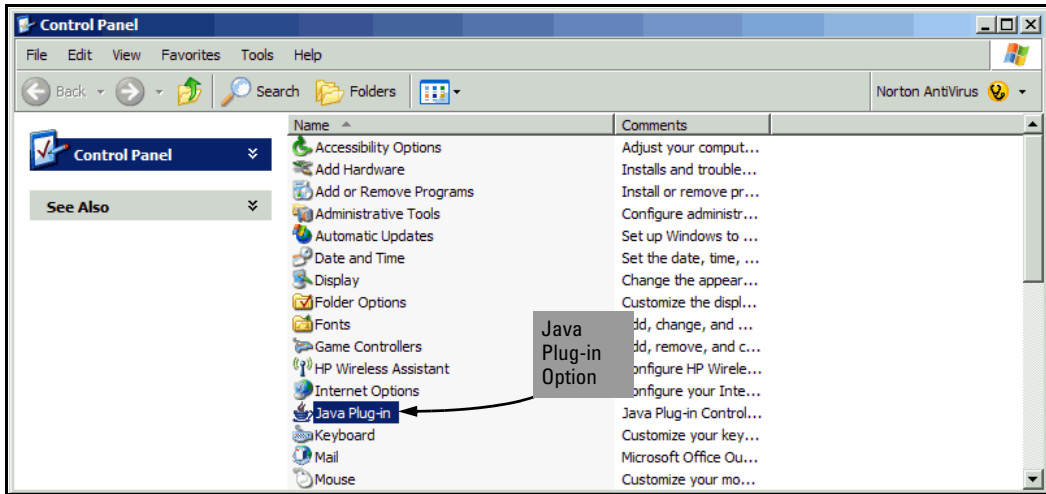


Figure 8. Control Panel

2. Select **Java Plug-in**. The **Java Plug-in Control Panel** window is displayed.

Note

If your workstation has more than one Java applet, the Control Panel will display multiple Java Plug-in options. Complete the following steps for each to ensure that the correct cache is cleared.

3. Select the **Cache** tab.

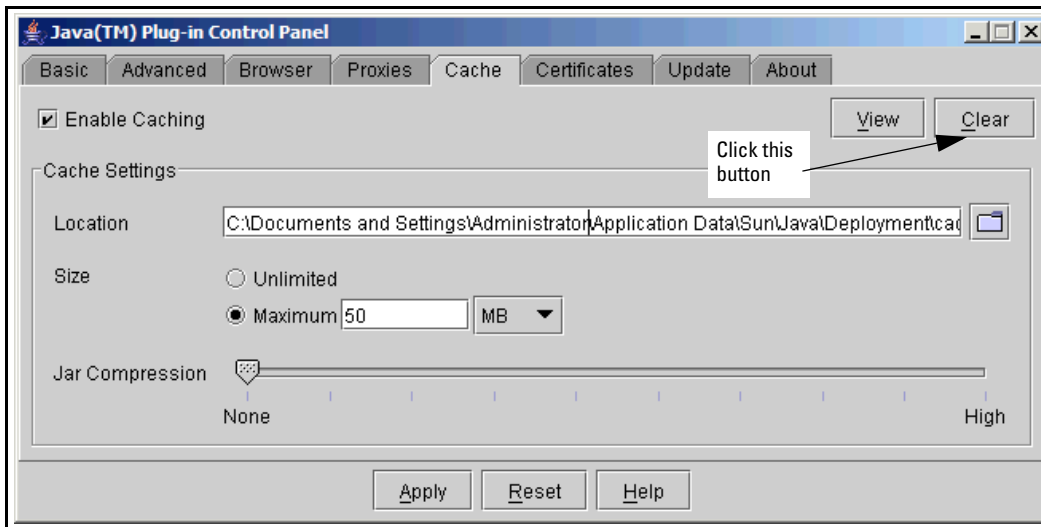


Figure 9. Java Plug-in Control Panel

4. You are prompted to confirm clearing the cache. Click the **Yes** button.

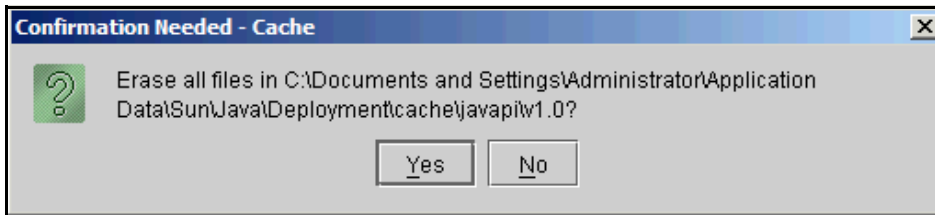


Figure 10. Java Plug-in Confirmation Needed Screen

5. Click the **Apply** button; then close the screen.

Restart the Browser

You are now ready to access the Wireless Edge Services xl Module's Web browser interface:

1. Close and re-open your browser.
2. Enter the IP address (or hostname) of your Wireless Edge Services xl Module in the browser.

- The Java applet should begin to download from the module. You might need to activate the applet (as shown in Figure 11). Press **[Space]** or **[Enter]**.



Figure 11. Activate the Java Applet

- After about a minute, the **Login** screen is displayed.



Figure 12. Login Screen for Wireless Edge Services xl Module Version 02.XX

Configuring Authentication for Web-Users

Note

Use this section to supplement the information in the chapter “Configuring the ProCurve Wireless Edge Services xl Module” of the *Management and Configuration Guide* (5013-5912, May 2007).

Instead of (or in addition to) using the local list to authenticate users, you can use a RADIUS server. If the RADIUS server authenticates a user, that user has the rights configured on the RADIUS database.

Make sure that the configuration on the RADIUS server meets these requirements:

- The user’s password is at least 8 characters.

SNMP v3 requires a password of at least this length. Your RADIUS server, however, may or may not enforce such a requirement. (For example, the Wireless Edge Services xl Module’s internal server does *not*.) Check the accounts for users that need management access to the module and, if necessary, set a new password of the correct length.

- The RADIUS server supports vendor specific attributes (VSAs).

For the RADIUS server to properly authorize the management user, you must set two VSAs in the policy that the RADIUS server uses to authenticate the user. Table 3 shows the proper values for the “HP-Management-Protocol” and the “HP-Management-Role” attributes.

Table 1. VSAs for Authorizing Management Users

| Attribute | Type | Length | Vendor ID | Vendor Type | Vendor Length | Format | Vendor Value Decimal Format |
|------------------------|------|--------|------------|-------------------------------|---------------|---------|--|
| HP-Management-Protocol | 26 | 12 | 11 (HP) | 4 (HP-Management-Protocol) | 6 | Decimal | 5 = HTTP 6 = HTTPS |
| HP-Management-Role | 26 | 12 | 11 | 1 (HP-Management-Role) | 6 | Decimal | 1 = SuperUser 2 = Monitor 16 = HelpDesk Manager 17 = Network Admin- istrator 18 = System Adminis- trator 19 = WebUser Admin- istrator |

If the server does not send the proper VSAs, the user receives the monitor role (read-only) to the Web browser interface.

The module's internal server does not support VSAs, so you should use the local server only to authenticate users that require read-only access.

Note

If you do not correctly configure the RADIUS server, you can lock yourself out of the Wireless Edge Services xl Module Web browser interface.

To fix the problem, access the module CLI through the wireless services-enabled switch. Enter this global configuration mode command to have the module authenticate Web-Users against its local list:

Syntax: aaa authentication login default local

Then configure at least one user in the local list:

Syntax: username <username> password <password>

The password must be between 8 and 32 characters.

Then assign the user rights sufficient to correct the problem. For example:

Syntax: username <username> privilege superuser

Special Characters for the ACL ID Field

As indicated in the chapter “Access Control Lists (ACLs)” of the *Management and Configuration Guide* (5013-5912, May 2007), string names for ACL IDs may contain alphanumeric characters, but spaces and non-alphanumeric characters are not allowed. However, the following special characters may be used:

~ ! @ # \$ % ^ & * () _ - { } [] | : ; ' < > , .

Correction: SNMP v3 Default Password

The chapter “Configuring the ProCurve Wireless Edge Services xl Module” of the *Management and Configuration Guide* (5013-5912, August 2007), pages 2-117 and 2-120, incorrectly states that for the snmptrap user, the default password is “procurve”. Instead, the default password is “trapuser.”

Correction: Stations per Radio

The xl Module's *Management and Configuration Guide* (August 2007), page 1-4, incorrectly states that each RP radio can support up to 64 stations simultaneously. Beginning with software version WS.02.xx, the correct number of local stations per radio is 256.

Correction: Stations per Module in a Layer 3 Mobility Domain

The xl Module's *Management and Configuration Guide* (August 2007), pages 1-84 and 9-6, incorrectly states that a Layer 3 Mobility Domain can include up to 12 modules, each of which can support up to 500 stations. Instead, the number of local stations per module is 4096.

Correction: Disabling TKIP Countermeasures

TKIP countermeasures are used to prevent “man-in-the-middle” TKIP attacks by disabling client connections for a short period of time. In some cases, it may be desirable to disable TKIP Countermeasures. The xl Module's *Management and Configuration Guide* (August 2007) includes a command that is *not* available for disabling TKIP Countermeasures:

no support wireless tkip-countermeasures

The following command effectively disables TKIP Countermeasures:

ProCurve(wireless-services-C)(config-wireless)#wlan 1 dot11i tkip-cnrmeas-hold-time ?

<0-65535> The hold-time in seconds. Default = 60

ProCurve(wireless-services-C)(config-wireless)#wlan 1 dot11i tkip-cnrmeas-hold-time 0

where **1** specifies the WLAN index in this example, and **0** specifies the hold-time (in seconds) in which clients are disconnected.

Clarification: Setting Intrusion Detection with TKIP Countermeasures

Intrusion Detection System (IDS) commands can be used to filter a station that set off IDS. Setting the following IDS parameters will blacklist the client for the amount of time set in the ageout (ageout time can be up to one day).

ProCurve(wireless-services-C)(config-wireless)#ids anomaly-detection tkip-countermeasures enable

ProCurve(wireless-services-C)(config-wireless)#ids anomaly-detection tkip-countermeasures filter-ageout 60

where **60** in this example is the ageout duration (seconds) in which mobile units will be filtered out. A value of 0 - 86400 seconds can be configured.

Enhancements

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

Enhancements are listed in chronological order, oldest to newest software release. To review the latest enhancements since the last general release, see [“Release WS.02.26 Enhancements” on page 21](#).

Release WS.01.11 Enhancements

Release WS.01.11 includes the following enhancements:

- Time zone software now complies with the United States Energy Policy Act of 2005. Under the new law, Daylight Saving Time begins the second Sunday of March and ends the first Sunday of November.
- Effective July 20, 2007, new FCC regulations on the use of the 5GHz band, the band used by radios supporting the IEEE 802.11a standard, prohibit the sale of radios not meeting the new specifications. To comply with these new requirements, WS.01.11 disables channels 52, 56, 60, 64 (5.25-5.35 GHz) in the U.S. These channels remain available for use in other countries.
- The restricted management access feature specifies a single interface (VLAN) for management access to a Wireless Edge Services xl module. SNMP access or access to the module’s Web browser interface is only available on the specified restricted management VLAN. By default, this feature is not enabled.

To display the current management VLAN, use the **show management** command from the module’s CLI. In the example below, the default, not restricted, management VLAN is displayed.

```
ProCurve(wireless-services-A)#show management
Mgmt Interface: vlan1
Management access permitted via any vlan interface
ProCurve(wireless-services-A)#
```

Note:

If you change the management VLAN to a VLAN other than VLAN 1, be sure to enter a default route that is within the subnet associated with the new management VLAN. See the *Management and Configuration Guide* for information on how to add a default route.

To configure a restricted management VLAN, start at the Global Configuration level of the 5300xl CLI and enter the module's CLI. In the following example, VLAN33 is set to be the specified management interface for the Wireless Edge Services xl module in chassis slot A. The **write memory** command saves the configuration.

```
ProCurve# configure
ProCurve(config)# wireless-services a
ProCurve(wireless-services-A)#conf
ProCurve(wireless-services-A)(config)#interface vlan33
ProCurve(wireless-services-A)(config-if)management
ProCurve(wireless-services-A)(config-if)exit
ProCurve(wireless-services-A)(config)#management secure
ProCurve(wireless-services-A)(config)#exit
ProCurve(wireless-services-A) #write memory
```

After creating the restricted management VLAN33 (above), the **show management** command displays the following:

```
ProCurve(wireless-services-A)#show management
Mgmt Interface: vlan33
Management access restricted to Mgmt Interface
```

When a restricted management VLAN is configured, **management secure** appears on a line in the **show running-config** command output, as shown below:

```
ProCurve(wireless-services-A)(config)#sho run
!
! configuration of ProCurveWLANModule Wireless Services version
WS.01.11
! version 1.0
!
management secure
.
.
.
```

Use the **show management** command (above) the see what VLAN is being used for the management interface.

To remove a restricted management VLAN, enter the following command:

```
ProCurve(wireless-services-A)(config)#no management secure
ProCurve(wireless-services-A)(config)#show management
Mgmt Interface: vlan33
Management access permitted via any vlan interface
```

The VLAN previously used as the restricted management VLAN is displayed as the management VLAN, but access is allowed from any VLAN.

Release WS.02.07 Enhancements

New and Enhanced Features

Note

The *Management and Configuration Guide* (5013-5912, May 2007) has been updated with information on the enhancements and new features in software release WS.02.07. Download this guide for more information. To download this guide, see [“Downloading Software and Documentation from the Web” on page 1](#).

New Features

The following new features are available with release WS.02.07 software. For more information, see the *Management and Configuration Guide* (5013-5912, May 2007) released with WS.02.XX (or later) software.

Table 2. New Features in Version WS.02.07 Software

| Feature | Description |
|--------------------------------------|---|
| Layer 3 RP adoption | Adopt Radio Ports (RPs) that are installed on a different subnetwork |
| Internal RADIUS server | Authenticate users with an internal (built-in) RADIUS server. |
| Firewall | Filter routed traffic through an internal firewall. |
| IP and MAC ACLs | Control traffic to and from wireless stations through Access Control Lists (ACLs) based on IP and MAC addresses. |
| Network Address Translation (NAT) | Provide Network Address Translation (NAT) services for traffic routed between two subnetworks, typically between the wireless and wired network. |
| Internal DHCP server | Provide DHCP services for wireless clients on a VLAN. |
| Fast Layer 2 roaming between modules | Wireless stations can disassociate with one Radio Port, and quickly reassociate with a different Radio Port under the control of the same module. |
| Layer 3 mobility | Wireless stations can disassociate with one Radio Port, and quickly reassociate with a different Radio Port under the control of different modules in the same Layer 3 mobility domain. |
| sFlow support | A module's sFlow agent monitors each radio and samples wireless traffic for an sFlow collector. |
| GRE tunnels | A Generic Routing Encapsulation (GRE) tunnel can be established with another device for forwarding all WLAN traffic. |

| Feature | Description |
|--|--|
| Secure NTP | Configure the module to take its time from an Network Time Protocol (NTP) server, or act as a secure NTP server for other devices. |
| Web-Users accounts | Create accounts for Web-Users, allow various levels of access to the module's Web browser interface. |
| ProCurve Identity Driven Manager (IDM) QoS | Supports Quality of Service (QoS) settings created through IDM. |

Enhancements

With release WS.02.07 software, existing features have been enhanced. Redundancy groups can include more members. Web authentication (Web-Auth) can be used with encryption. More digital certificates are supported, and wireless traffic can be monitored more closely. Some features, are configured in a slightly different way, such as Access Point detection and self-healing.

Capabilities and scalability of the ProCurve xl Wireless Edge Services Module have been improved. The following table summarizes some of these improvements.

Table 3. Summary of Feature/Function Changes in WS.02.XX

| Feature/Function | WS.01.XX | WS.02.XX |
|--|----------------|----------------------|
| Throughput - Unencrypted | 290 mbits | 400 mbits |
| Maximum number of Radio Ports supported | 36 | 48 |
| Maximum number of associated stations | 1000 | 4096 |
| Maximum number stations per radio | 64 | 256 |
| Maximum number of modules in Redundancy Group | 2 | 12 |
| Maximum number of VLANs per module | 8 | 32 |
| Radio Port Failover time (Layer 2) | 55 sec typical | 20 sec typical |
| Maximum number of static routes | 1000 | 300 |
| Maximum number RADIUS Authentications per second | n/a | 15 Internal / 5 LDAP |
| Maximum number of DHCP Lease Grants per second | n/a | 15 |
| Maximum number of modules in Layer 3 Roaming Group | n/a | 12 |

Release WS.02.26 Enhancements

Support for Client Location Confidence in ProCurve Mobility Manager

To support the client location confidence feature in ProCurve Mobility Manager 2.0 Automatic Update 1 (AU1), the logging of client probe requests (a “Probe List”) can be enabled through the switch’s Command Line Interface (CLI).

To enable logging of client probe requests, use the **station probe-history enable** command from the wireless configuration context. For example:

```
ProCurve<wireless-services-A><config-wireless># station probe-history enable
```

where the WESM xl is installed in slot A of the switch in this example.

Software Fixes

Release WS.01.03 was the first software release for the ProCurve Wireless Edge Services xl Module (J9001A) and the ProCurve Redundant Wireless Services xl Module (J9003A).

To review the list of fixes since the last general release published, begin with [“Release WS.02.14” on page 28](#).

Release WS.01.05

Problems Resolved in Release WS.01.05

- **Infrastructure (27200)** — Interface's MTU size was not saved in the running config. Now saved correctly.
- **Infrastructure (28463)** — The running-config file includes a time stamp, which makes it appear that the file has changed between fetches. The time stamp has been removed.
- **Security (27441)** — Fixed support for full-size RADIUS packets, and ones that may contain 100 attributes.
- **SNMP (27403)** — SNMP **get** fails for an instance of `hpicfWsmWsInfraFileMgmtImageVersion` after reboot until a walk or **getNext** is done on table entries. Now operates properly.
- **Wireless (27165)** — Password encryption secret configuration issue. Unable to configure 802.11i key with password-encryption secret or specified UNENCRYPTED password. Now operates properly.
- **Wireless (27199)** — Added support for CHAP as an optional authentication type for Web-auth. This is configured via the CLI only.
- **Wireless (27438)** — Thirteenth RP needs to be seen in unadopted list. Now operates properly.
- **Wireless (27439)** — Attribute (Calling-Station-Id) was missing for Web-auth, causing interoperability problems with IDM server. This has been fixed.
- **Wireless (27443)** — Framed-MTU and Connect-Info in RADIUS request packet for Web-auth and 802.1X were missing. They have been added.
- **Wireless (27214)** — Web-Auth/IDM did not work if there were more than four ACLs or if the RADIUS packet length was more than 250. This has been fixed.
- **Wireless (27437)** — Web-auth redirection did not always work.

Release WS.01.11

Problems Resolved in Release WS.01.11

- **Security (33010)** — Module can be managed through non-management interfaces. This software change allows the management VLAN access to be restricted.
- **Security (35037)** — Unable to block access to the management applet login screen from web-authentication clients.
- **Wireless (35851)** — Broadcast-Multicast (BCMC) traffic was dropped when DTIM period is set to 1 resulting in SVP "push to talk" feature failure.
- **Wireless (36024)** — BCMC Traffic was sent out at the wrong DTIM, resulting in SVP "push to talk" feature failure.
- **Wireless (37485)** — Malformed Ethernet packets cause a kernel panic from crypto.c

Releases WS.02.01 — WS.02.06

Software versions WS.02.01 through WS.02.06 were never released.

Release WS.02.07

Problems Resolved in Release WS.02.07

- **Applet (27436)** — In the **Wireless Statistics** page, sort by **Radio Index** and sort by **Bit Speed (Avg.) Mbps** do not work.
- **CLI (27202)** — The **redundancy hold-period** is incorrectly shown as the **redundancy holdtimeperiod** in the configuration file.
- **CLI (27213)** — Output from the command **show wireless ids** displays the **filter-ageout** as **filter-agetout**.
- **Infrastructure (34591)** — The **Log File Creation** date displayed in the web interface is incorrect.
- **Infrastructure (41263)** — Module may fail to boot or boot to a diagnostics prompt after it is reset using either software or cold booted.

Software Fixes

Releases WS.02.08 — WS.02.10

- **SNMP (41244)** — The following OID changes have occurred

Deprecated OIDs:

wsTrapWirelessIdsExcessiveAuthAssociation: 1.3.6.1.4.1.388.14.5.1.7.5.1
wsTrapEnableWirelessIdsExcsAuthAssoc: 1.3.6.1.4.1.388.14.5.1.7.5.2
wsTrapWirelessIdsExcessiveProbes: 1.3.6.1.4.1.388.14.5.1.7.5.3
wsTrapEnableWirelessIdsExcsProbes : 1.3.6.1.4.1.388.14.5.1.7.5.4

New (Added) OIDs:

wsTrapEnableAllWirelessIdsTrap : 1.3.6.1.4.1.388.14.5.1.7.5.5
wsTrapDisableAllWirelessIdsTrap : 1.3.6.1.4.1.388.14.5.1.7.5.6
wsTrapWirelessIdsMuEvent: : 1.3.6.1.4.1.388.14.5.1.7.5.7
wsTrapEnableWirelessIdsMuEvent: : 1.3.6.1.4.1.388.14.5.1.7.5.8
wsTrapWirelessIdsRadioEvent: 1.3.6.1.4.1.388.14.5.1.7.5.9
wsTrapEnableWirelessIdsRadioEvent: 1.3.6.1.4.1.388.14.5.1.7.5.10
wsTrapWirelessIdsSwitchEvent: 1.3.6.1.4.1.388.14.5.1.7.5.11
wsTrapEnableWirelessIdsSwitchEvent: 1.3.6.1.4.1.388.14.5.1.7.5.12

- **Wireless (27199)** — Support for CHAP as an optional authentication type for Web-authentication is configurable using either the CLI or web management interface now.
- **Wireless (37490)** — Crash of the redirected daemon is causing Web-authentication to stop working.
- **Wireless (40210)** — SVP roaming delay and packet loss experienced during roaming to different radio ports within a single controller.

Releases WS.02.08 — WS.02.10

Software versions WS.02.08 through WS.02.10 were never released.

Release WS.02.11

Problems Resolved in Release WS.02.11

- **Applet** — If the network administrator configures a self-signed certificate with a space in the trustpoint name, the configuration will be allowed, but the local RADIUS services will then fail. This fix triggers a popup warning, stating that spaces are not allowed in the trustpoint name.
- **Applet (41724)** — Sorting items by clicking the column heading in the Web UI does not function properly in all screens.
- **Applet (41766)** — Neither static nor dynamic NAT values are displayed on the NAT statistics page of the Web Management Interface.

- **Applet (40701)** — The Web Management Interface becomes unresponsive if the user refreshes the alarm log more than 5 times when there are over 500 alarms present.
- **Applet (40908)** — The Web Management Interface login page is displayed (and should not be) even when SNMPv3 is disabled. Then, although login attempts are unsuccessful as intended by the design, the error message, “You supplied an invalid username/ password pair” is inaccurate, and the syslog message inaccurately reports authentication success.
- **Applet (40538)** — Some valid combinations of IP address and subnet mask produce a misleading error message.
- **Applet (40593)** — The Trustpoint for certificate configuration gets deleted when the **Back** button is selected from the later configuration screens.
- **Applet (40871)** — When adding a MAC Extended ACL rule, the Ethertype pulldown menu should be enabled or disabled according to whether the Ethertype checkbox is populated, rather than always being enabled.
- **Applet (40940)** — Repeatedly refreshing the ACL statistics in the Web Management Interface will occasionally reveal a blank screen.
- **Applet (41044)** — The percentage of Undecryptable Packets is showing an invalid value of 100% or more in the WLAN and Radio statistics areas, though it is displaying appropriate values in the wireless statistics detail popup.
- **Applet (41308)** — The ACL statistics screen shows invalid protocol values and invalid rows.
- **Applet (41337)** — A java.lang.NULL pointer exception may occur during configuration of a DHCP pool in the Web Management Interface.
- **Applet (41338)** — When DHCP relay is already enabled on a VLAN, and a DHCP scope is added for that same VLAN, an error should occur on the bottom left corner of the Web Management Interface warning the user of the conflicting DHCP strategies.
- **Applet (41486)** — If the administrator of the Web Management Interface tries to modify ACE rule precedence by using the rule precedence of an different ACE within the same ACL, one of the access control entries will be deleted.
- **Applet (42562)** — A duplicate CA certificate for the same trustpoint entry may be displayed by the Web Management Interface.
- **Applet (41468)** — The radio statistics page in the Web Management Interface may display a larger value for "last 30s" than for "last hr".
- **Applet (41323)** — After enabling DHCP Relay and committing to the change, the **Cancel** button still appears but does not function.

- **Applet (42565)** — The Web Management Interface does not allow changes to the GRE tunnel interface IP address.
- **Chassis (40486)** — The running configuration on the module is not erased as it should be when the startup configuration of the chassis is erased and the host switch is reloaded.
- **CLI (41567)** — The CLI fails to display buffered log messages when debug is enabled.
- **ESPD (41183)** — When an invalid file name is used for the configuration file in the update server, the result is an oddly corrupted configuration.
- **Infrastructure (40782)** — After setting up the update server parameters and reloading, the module loses its IP address and local RADIUS settings.
- **Infrastructure (40840)** — Disabling and re-enabling SNMPv3 support or enabling the Secure Management VLAN may cause the module to hang.
- **Infrastructure (41391)** — Valid login password credentials for the Web Management Interface do not successfully allow authentication on the second attempt after a security scan.
- **Infrastructure (41384)** — The update server functionality continues to pull the redundancy-config file even when the unreachable flag is set.
- **Infrastructure (41257)** — A Logd core file is produced after enabling "debug all" messages in the CLI.
- **Infrastructure (42759)** — The module may reboot with a Kernel Panic ("missing device") when iPerf tests are run against it.
- **Infrastructure (44596)** — Presence of a carriage return in the Web Auth configs page corrupts the configuration. This fix strips out the carriage return character and adds some text to the Web Management Interface to encourage the use of a carriage return alternative in the configuration.
- **Infrastructure (43038)** — Redundancy peers toggle offline and then back online when a show running configuration command is executed.
- **L2-L3 (41339)** — There is intermittent log message accuracy when there are multiple VLANs with different DHCP strategies in place (some with DHCP relay and others with DHCP server scopes).
- **L2-L3 (40237)** — An FTP transfer is erroneously allowed between devices in different VLANs in the absence of routing.
- **L2-L3 (41385)** — A DHCP server core file may be produced during normal operation.

- **L2-L3 (41390)** — When DHCP relay is configured on a VLAN that already has a scope and DHCP services defined, once the change is saved and followed by a module reload, the IP-helper setting is not successfully copied from the startup configuration to the running configuration.
- **L2-L3 (41309)** — When a rule to apply ToS packet marking is added to an ACL that is applied to NAT, the NAT functionality fails.
- **L2-L3 (41612)** — The ccsrvr process may crash and produce a core file when the administrator is walking the MuProbeStatusTable.
- **Security (41760)** — The module administrator is unable to access either the Web Management Interface or the CLI when the RADIUS server host IP address is not reachable for authentication of login credentials.
- **Security (41231)** — A "Failed to save - Inconsistent Value" error message may be displayed while attempting to attach an IP ACL to a VLAN; however, after hitting cancel and refreshing the parent screen, the ACL attachment may indeed be present.
- **SNMP (41219)** — In the Web UI, even after seeing confirmation that a valid config file transfer to the startup-config file was successful, users may note after rebooting the WES Module that the changes to startup-config were not truly saved.
- **SNMP (40842)** — Configuration of an SNMPv3 manager for Web Management access may cause the module to become unresponsive.
- **SNMP (40252)** — The applet allows a different maximum number of SNMP trap receivers than the CLI. This fix limits the total number of SNMP trap receivers to 10 addresses regardless of the management access method.
- **SNMP (40867)** — Adding an ACL with a space in the name fails and does not produce an error message.
- **SNMP (42856, 42688)** — The configuration of a 63-character WPA encryption passphrase results in an error when attempted through the Web Management Interface.
- **Wireless (40242)** — Wireless clients may intermittently fail WPA authentication with the following message reported to syslog:

```
Station <mac address> failed dot11i tkip ccmp handshake on wlan <id>.
```
- **Wireless (41650)** — L3 roaming may fail between two modules installed in different switches when the host switches provide connections to multiple devices over physical links that possess identical VLAN port assignments.
- **Wireless (41738)** — The ProCurve IDM QoS setting is not properly marking packets when layer 3 mobility is enabled on an SSID.
- **Wireless (41710)** — The Radio Port 220 (J9005A) may become unresponsive when the 802.11bg radio is set to detector mode in **Network Setup -> Radio -> Edit**.

- **Wireless (41324)** — Access point detection requires that either the **Single channel scan for Unapproved APs** or **Dedicate this Radio as a Detector** is enabled in the radio configuration, but **Single channel scan for Unapproved APs** has no affect if the **Self Healing** feature is enabled. With this fix, rogue radios no longer show up when a radio port is part of a self-healing group unless single channel scan is enabled.
- **Wireless (41389)** — The ProCurve IDM QoS setting is not being applied in the proper direction.
- **Wireless (41482)** — When devices using power save mode re-associate with a radio port, they may have connectivity issues. When this happens to SVP phones, the phones will display a message similar to `Unable to contact PRI gateway` when they try to re-associate.
- **Wireless (41320)** — The TIM bit (in the wireless beacon) is not getting cleared when SVP phones in power save mode re-associate.
- **Wireless (41711)** — Wireless stations should be allowed to transmit and receive data directly following a 4-way WPA handshake, rather than waiting for the 2 message group key handshake messages afterward. This causes communication failure in certain clients.
- **Wireless (41341)** — Rogue AP detection continues to detect unapproved AP's even when AP detection and (self-healing) scanning are both disabled.

Release WS.02.12

Problems Resolved in Release WS.02.12

- **Applet (42774)** — The Web Management Interface does not allow variable length subnet masks in the screens that add a DHCP Network Pool for a VLAN interface.
- **IDM (746917)** — The IDM process was not available.
- **SFlow (746921)** — The sFlow process was not available.

Release WS.02.14

Problems resolved In Release WS.02.14 (not a general release)

- **Wireless (45552)** — Pairwise Master Key (PMK) caching allows the module to store a station's PMK after the station disassociates with a Radio Port so that the key remains in place if the station re-associates with a different Radio Port. Prior to this fix, network administrators had to disable PMK caching to use the ACL features in IDM. This fix will ensure that IDM ACLs will remain in place after a roam, with PMK caching enabled.
- **Wireless (45775)** — ACL statistics were not being reported.

Release WS.02.21

Problems resolved in Release WS.02.21 (Manufacturing release only)

- **Infrastructure (43037)** — Even when the redundancy heartbeat-period has been configured to a non-default value and that configuration change has been saved, the module reverts to the default value of 5 seconds following a reload.
- **Infrastructure (45549)** — The allowed configuration value range for the RADIUS client shared secret was not consistent between the CLI and Web management interface. This fix removes the 4 character minimum from the Web management interface.
- **Infrastructure (45577)** — The Web management interface does not provide the ability to configure the local RADIUS server's IP address.
- **Radio Port/Wireless (46298)** — An incorrect DNS string was pushed to the radio ports when they are first adopted by a module on a software version capable of layer 3 adoption.
- **Security (45431)** — The securitymgr process restarts every 10 to 15 minutes, creating a crash log entry.
- **Wireless (44760)** — Radio port/controller communication protocol update.
- **Wireless (46458 and 46291)** — In the European Union and selected countries/regions (including South Africa, Turkey, Morocco, and Croatia), ProCurve Wireless Edge Services Modules, Access Points and Radio Ports purchased after April 1, 2008, are subject to new radar interference requirements that limit the available channels in the 5 GHz band. To comply with these new requirements, the operating channels impacted by this change have been removed. The available 5 GHz channels are now 36, 40, 44 and 48 (5.150 - 5.250 GHz).
- **Wireless (43147)** — Performance delays are seen with file transfers/ping traffic that passes through a network infrastructure device with eight 802.1p priority queues.

Release WS.02.26

Problems resolved in Release WS.02.26 (not a general release)

- **Infrastructure (46124)** — Kernel Panics may occur in the Probe Table functionality.
- **Infrastructure** — The module does not return to a functional state following a reload from either the CLI or Web Management Interface. Workaround: reseal the module or reload the chassis to recover functionality.
- **Wireless (46289)** — The station probe table was added for support of ProCurve MM 2.0 Automatic Update 1 (AU1) and its Location Confidence feature. For more information, see [“Release WS.02.26 Enhancements” on page 21](#).

Release WS.02.27

Problems resolved in Release WS.02.27

- **Wireless (00677)** — An incorrect RSSI value is displayed in response to an SNMP walk.
- **Wireless (00681)** — All the wireless stations in the Probe list inaccurately report the same RSSI.
- **Wireless (01085)** — CPU utilization in the module may approach 100% the day following application of ProCurve's Mobility Manager 2.0 Automatic Update 1 (AU1) release.
- **Wireless (14986)** — A faulty radio port may trigger repeated reboots due to the module experiencing cserver crashes. This fix prevents the module from adopting faulty radio ports.
- **Wireless (46296)** — Debug capability for SNMPd was added.

Known Software Issues and Limitations

This section identifies issues you may encounter when using a ProCurve Wireless Edge Services xl Module (J9001A) or a ProCurve Redundant Wireless Services xl Module (J9003A).

To review the most recent list of issues and limitations since the last general release published, begin with [“Release WS.02.11” on page 34](#) and [“Release WS.02.12” on page 34](#).

Release WS.01.05

- In the Web browser interface, radio information is missing in the Wireless Statistics Screen. **MAC Address**, **Throughput**, **Bit Speed (Avg.)**, **% Non Unicast**, and **Retries** fields are displayed as blank for radio index 2 (27289).

Release WS.01.11

- **Applet (27436)** — In the Wireless Statistics page, sort by **Radio Index** and sort by **Bit Speed (Avg.) Mbps** do not work.
- **CLI (27202)** — The **redundancy hold-period** is incorrectly shown as the **redundancy holdtime-period** in the configuration file.
- **Security (41136)** — MAC filters are not retained across a reboot
- **Wireless (27199)** — Support for CHAP as an optional authentication type for Web-authentication is configurable only using the CLI.
- **Wireless (37490)** — Crash of the redirected daemon is causing Web-authentication to stop working.

Release WS.02.07

- **Applet** — If the network administrator configures a self-signed certificate with a space in the trustpoint name, the configuration will be allowed, but the local RADIUS services will then fail.
- **Applet (35919)** — There is no way to edit the radius clients and proxy servers. The workaround is to delete and reconfigure them.
- **Applet (40444)** — Web management allows the edit of an attached ACL which does not exist; this invalid action will result in a "communication error" which does not provide information about why the action failed.

- **Applet (37818)** — When the user leaves the DHCP Configuration page without saving changes, no warning message is displayed.
- **Applet (39451)** — The user is unable to copy a configuration file from TFTP to the running-config. The recommended method for configuration file transfer is to copy to the startup-config and reboot into the intended configuration.
- **Applet (38687)** — There are no warning messages displayed when the user tries to configure the DHCP server on an interface which has DHCP relay enabled, nor when the user tries to configure DHCP relay for an interface which already has the DHCP server configured (essentially creating conflicting DHCP strategies).
- **Applet (39224)** — There is an inability to copy running or startup config files from one Wireless Edge Services Module to another. Files will have to be transferred to an intermediate FTP or TFTP server in order to be moved onto a different module.
- **Applet (39362)** — The web management interface does not allow SNMPv3 password edits. This is due to the web interface's dependence on SNMPv3 for connectivity. To configure a change, SNMPv3 passwords should be deleted and reconfigured through the module's CLI.
- **Applet (35584)** — Trustpoint configuration in the web management interface does not allow selection of fields that already have data in them (i.e. using the **Back** button).
- **Applet (35251)** — A DHCP scope must be configured and applied to an interface before the DHCP server can be enabled; an error will be received if the user tries to enable the DHCP server without the prerequisite configuration.
- **Applet (36593)** — The applet is missing some of the ACL statistics.
- **Applet (35797)** — Error messages displayed in the CLI may not match the text of the corresponding error messages displayed by the web management interface.
- **Applet (36557)** — When an invalid time format is used to configure the time (in **Network Setup > Configuration**), the error message lacks a display of the correct time format.
- **Applet (37252)** — The web management interface displays the radio port IP address in a column labeled **Protocol** rather than **IP address**.
- **Applet (36778, 36785)** — The **Revert** and **Apply** buttons are not consistently placed on the right side of the screen in the various web management interface pages that contain those options.
- **Applet (38332)** — The local RADIUS server does not automatically sort the users into their assigned groups in the display table. The field names can be clicked to trigger the sorting action.
- **Applet (36448)** — Placing an invalid time of access value in the RADIUS server configuration will result in a vague "communication error" message which does not indicate which field had an invalid value.

- **Applet (38198)** — The tab button does not allow the user to navigate from the DHCP Scope **Start IP** to the **End IP** field.
- **Applet (38133)** — If invalid syntax is used to configure any of the **Radio > Global Settings**, a generic "communication error" message is sent to the web management interface.
- **Applet (38532)** — Changing screens in the **WLAN Setup > Assignment** page may trigger a message that warns that the user has un-applied changes, even when no changes have been made.
- **Applet (37520)** — If an invalid value is entered into the **Redundancy Group > Discovery Period**, that field will not auto-correct with a valid value.
- **Applet (38796)** — The user is allowed to delete both the running-config and startup-config, resulting in a reset to factory defaults.
- **CLI (40764)** — The user is allowed to create an invalid configuration in which duplicate SSIDs are configured.
- **Infrastructure (38600)** — Copying to the running configuration through the web management interface is not allowed. The workaround is to conduct this copy from the command line interface. Note that copying to the running configuration appends the running configuration rather than overwriting it in its entirety.
- **Infrastructure (40054)** — Copying into the running-config or the startup-config with files opened and edited in native Windows applications yields an error due to the placement of a **Ctrl M** character into the file. In order for a text-edited configuration file to be recognized and loaded by the module, it must not have the **^M (ctl-M)** character in it. One workaround would be to edit in a text editor, such as WinVi (<http://www.winvi.de/en/>), that does not automatically insert that character.
- **Security (32870)** — When a restricted access-list is in use, there must be an extended MAC ACL rule used in conjunction with it to permit ARPs to get through. Please see the ProCurve Support web site for a configuration example.
- **Security (32558)** — SYN attack detection and blocking triggers a cryptic log message, "allowed forw creation rate exceeded".
- **Security (36945)** — Modifying a NAT configuration with an incomplete ACL entry appropriately yields an error message, but that message is somewhat vague about its trigger (the incomplete ACL syntax).
- **Security (34041)** — The user is able to remove ACLs and ACL rules when they are in use by NAT.
- **Security (36658)** — Dynamic NAT allows you to create a deny rule, which is an explicit (redundant) configuration of the default state.

Known Software Issues and Limitations

Release WS.02.11

- **Security (40983)** — Pairwise Master Key (PMK) caching allows the module to store a station's PMK after the station disassociates with a Radio Port so that the key remains in place if the station reassociates with a different Radio Port. If PMK caching is enabled, setting ACLs through ProCurve Identity Driven Manager (IDM) will not work. To use the ACL features in IDM, disable PMK caching. When PMK caching is disabled, stations will properly authenticate with the RADIUS server when roaming using the IDM ACLs.
- **SNMP (39533)** — Only alphanumeric LLDP names are allowed in configuration of the radio port names. If a special character is used as part of the name, an "invalid LLDP name" message is triggered.
- **Wireless (30591)** — Some external RADIUS servers do not send access-reject messages to the module in response to certain EAP authentication failures; if a client is sending excessive EAP authentication requests and the RADIUS server does not send access-reject messages, the IDS will not be able to log an alert.

Release WS.02.11

- **Infrastructure (43037)** — The redundancy Heartbeat-Period is resetting its value to the default (5) after the module is reloaded.
- **Management (42857, 42858)** — In ProCurve Manager 2.2.1 and Mobility Manager 1.1, the MAC address of the Radio Port 220 (J9005A) is displayed in the serial number field, and under model number, "RP220" is displayed instead of the product number "J9005A".
- **Security (42622)** — The ACL statistics are not reflecting accurate values.
- **Wireless (43146)** — Under certain conditions, FTP transfer performance may be impaired.
- **Wireless (42632)** — The Tx_Retries counter in CCAPI_RADIO_STATS is inaccurately high; packet capture does not show many retries.
- **Wireless (42709)** — The ccserver process generates a core file when 4097 wireless stations are associated with a module using open security.

Release WS.02.12

- **FTP Performance** — FTP *get* operations may experience poor performance.



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

Part Number 5991-3775
July 2008