Release Notes:

Version WT.01.03 Software

for the ProCurve Wireless Edge Services zl Module (J9051A) and the ProCurve Redundant Wireless Services zl Module (J9052A)

These release notes include information on the following:

Publication Number

Part Number 5991-8624
September 2007

Applicable Product

ProCurve Wireless Edge Services zl Module (J9051A)

ProCurve Redundant Wireless Services zl Module(J9052A)

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

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:

1. Go to the ProCurve Networking Web site at: http://www.procurve.com.
2. Click on **Software updates**.
3. Scroll down. Under **Latest software**, click on **Wireless Services Modules**.

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

1. Go to ProCurve Networking's Web site at http://www.procurve.com.
2. Click on **Technical support**, then **Product manuals**.
3. Click on **ProCurve Switch 5400zl/8200zl series**.
4. On the resulting Web page, double-click on a document you want.
5. When the document file opens, click on the disk icon  in the Acrobat® toolbar and save a copy of the file.

Downloading Software to the 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 module's *Management and Configuration Guide* (5991-8626) for instructions and more information.

ProCurve Networking periodically provides software updates through the ProCurve Networking Web site (**http://www.procurve.com**). 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 module's *Management and Configuration Guide* (5991-8626) 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 5406zl(wireless-services-B)#write memory
[OK]
ProCurve Switch 5406zl(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 module's *Management and Configuration Guide* (5991-8626) 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 Series (2510-24)
T	Switch 2900 Series (2900-24, and 2900-48G)
VA/VB	Switch 1700 Series (Switch 1700-8 - VA.xx, Switch 1700-24 - VB.xx)
WA	ProCurve Access Point 530
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

Release WT.01.03

The *Management and Configuration Guide* (5991-8626) includes detailed information on the features in software release WT.01.03. To download this guide, see "Downloading Software and Documentation from the Web" on page 1.

Accessing the Web Browser Interface — In Case of Difficulty

Your web browser or Java cache may trigger problems with initial access to your module. If you have difficulty with access to the Wireless Edge Services zl Module's Web management interface, you may need to complete these steps:

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

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.

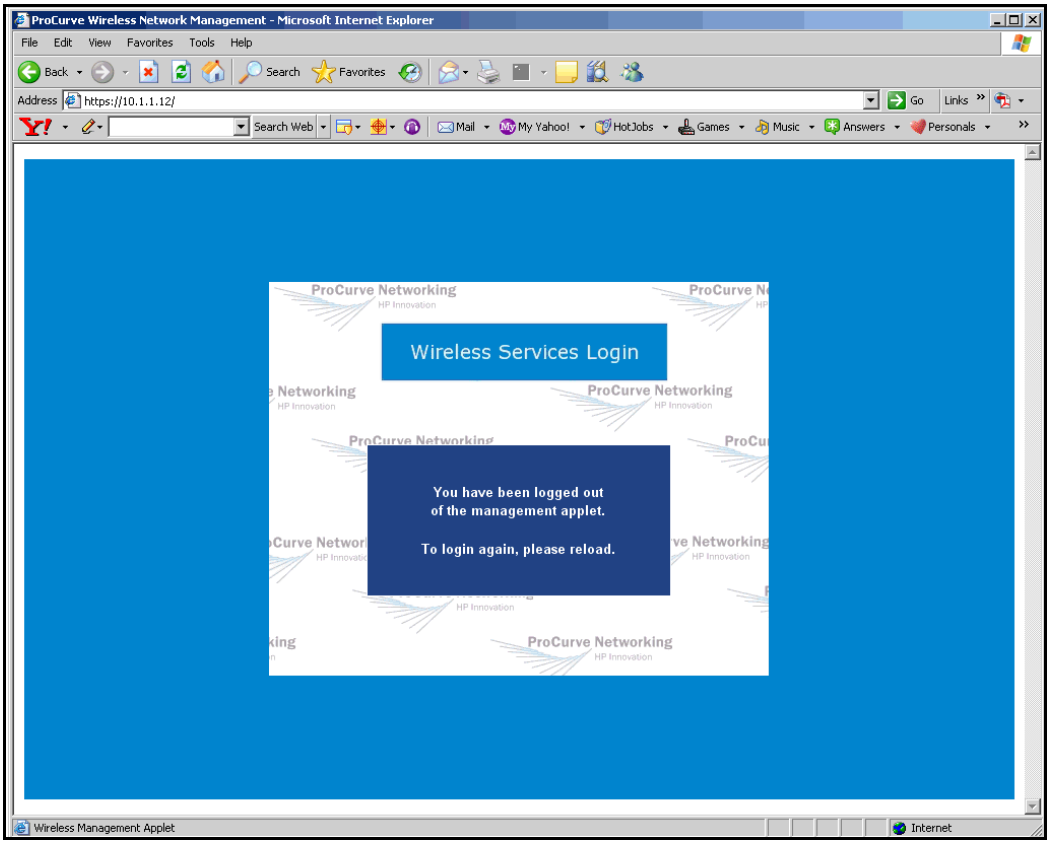

Figure 1. IE Browser

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

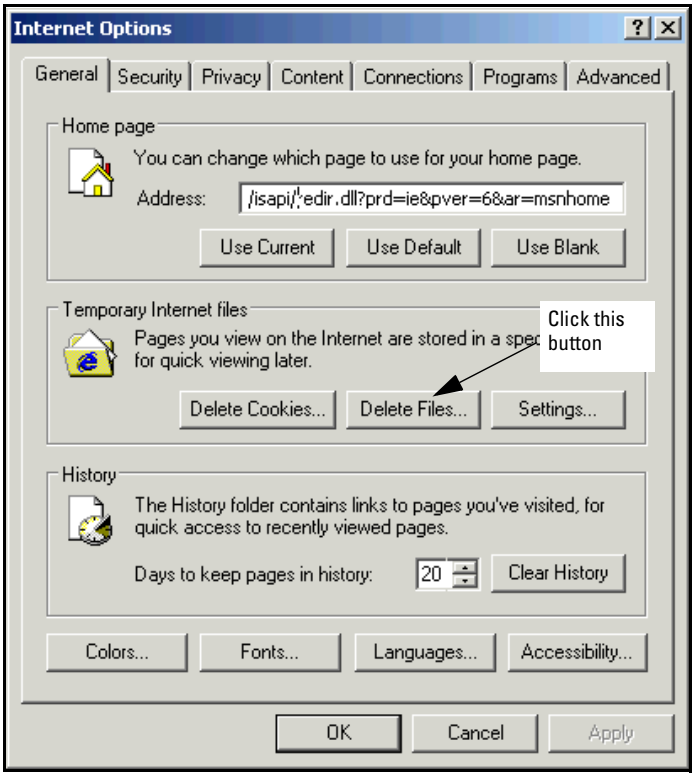

Figure 2. Tools > Internet Options

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.

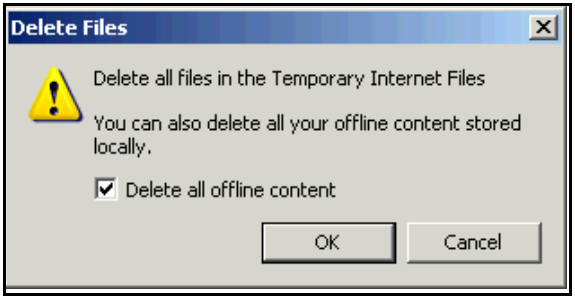

Figure 3. Delete Files

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**.

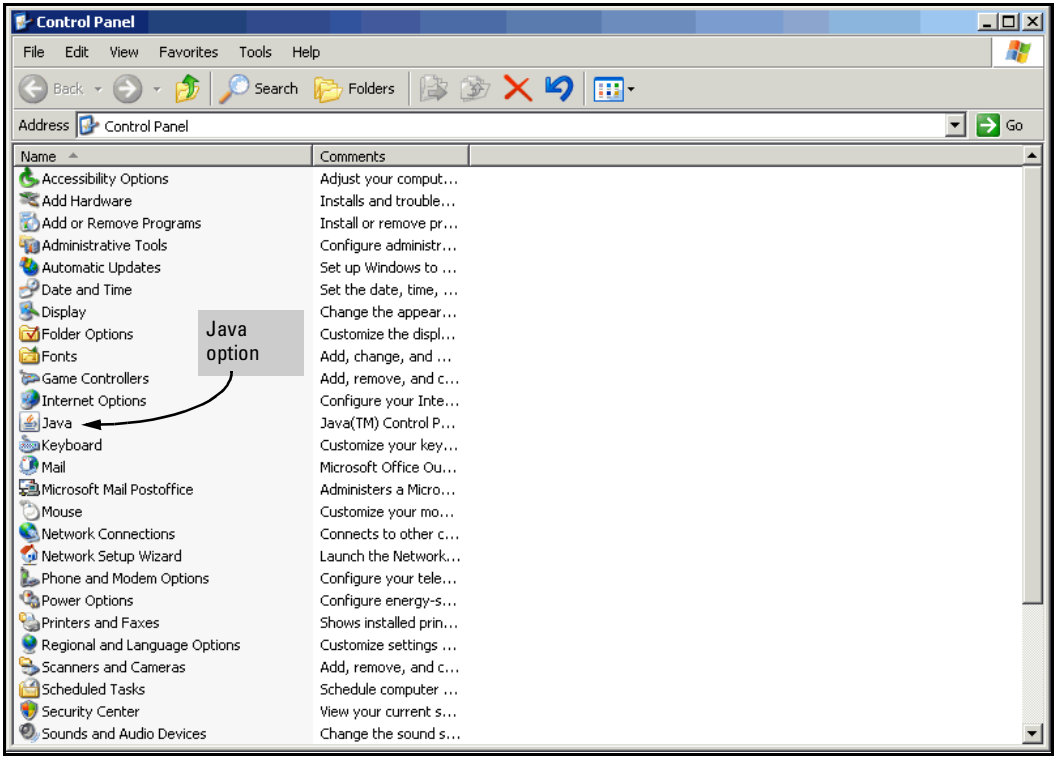

Figure 4. Control Panel

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

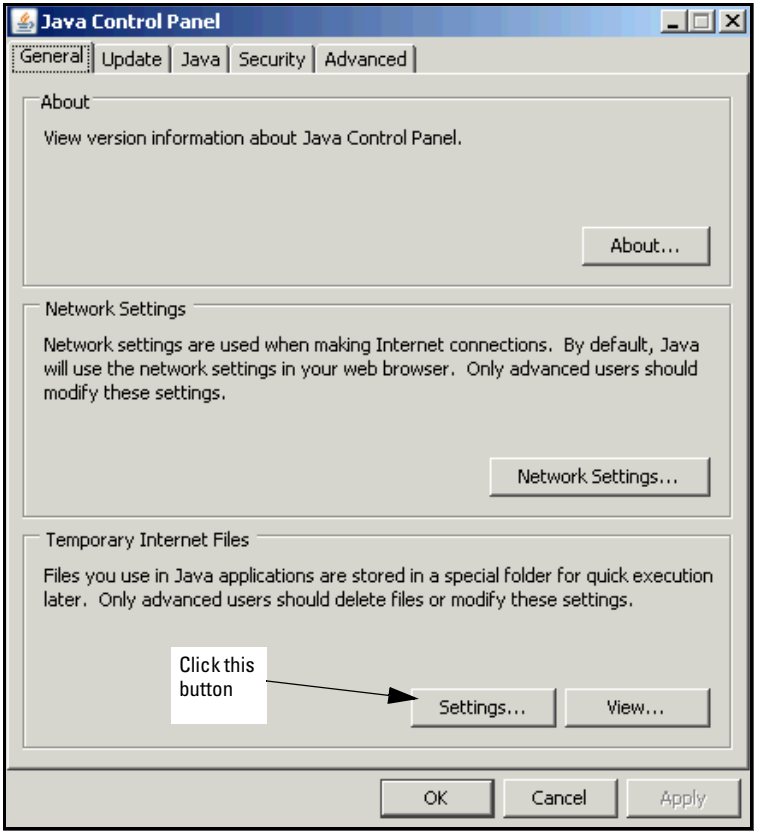

Figure 5. Java Control Panel

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

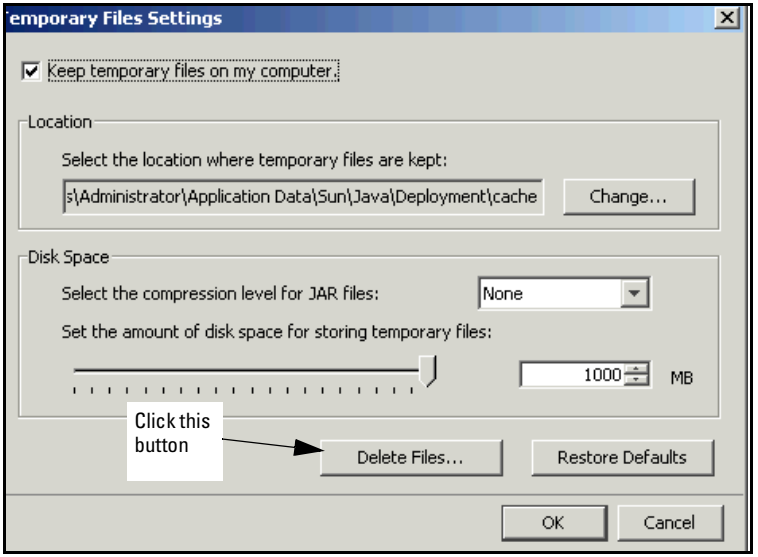

Figure 6. Temporary Files Settings (Java Control Panel)

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

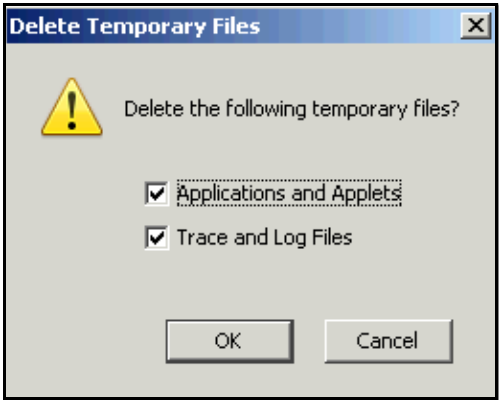

Figure 7. Delete Temporary Files (Java Control Panel)

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**.

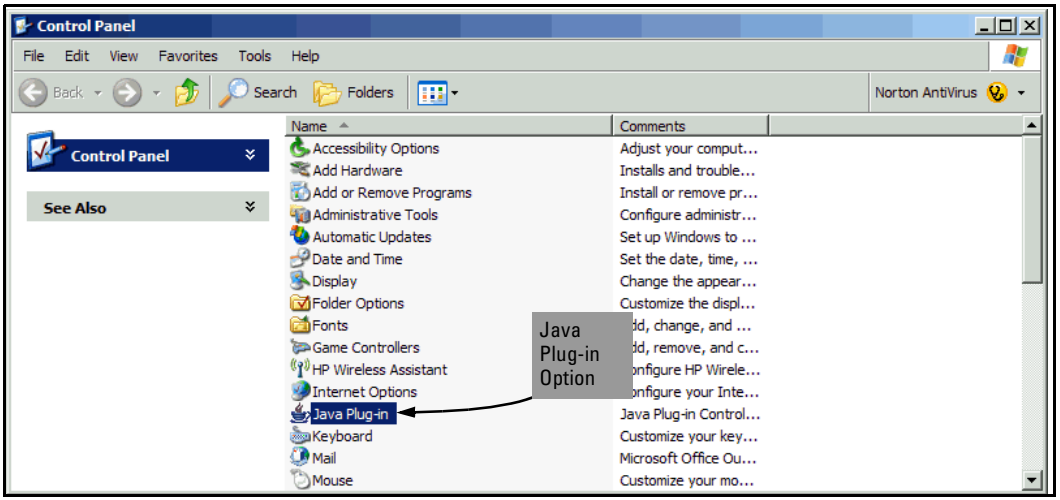

Figure 8. Control Panel

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.

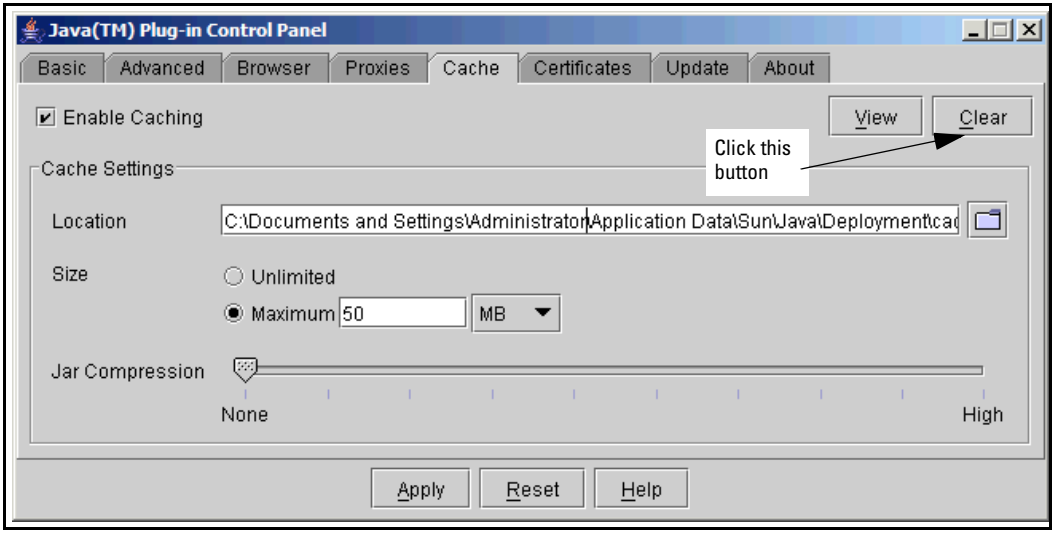

Figure 9. Java Plug-in Control Panel

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

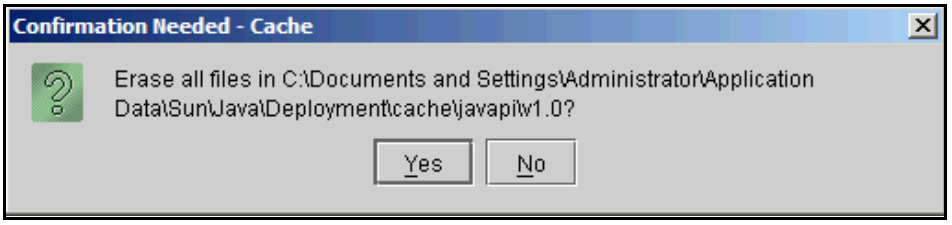

Figure 10. Java Plug-in Confirmation Needed Screen

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

Restart the Browser

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

1. Close and re-open your browser.
2. Enter the IP address (or hostname) of your Wireless Edge Services zl Module in the browser.
3. 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

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

Figure 12. Login Screen for Wireless Edge Services zl Module

Configuring Authentication for Web-Users

Note

Use this section to supplement the information in the chapter "Configuring the ProCurve Wireless Edge Services zl Module" in the *Management and Configuration Guide* (5991-8626).

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 zl 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 1 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 Administrator 18 = System Administrator 19 = WebUser Administrator

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 zl 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* (5991-8626), 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 zl Module" of the *Management and Configuration Guide* (5991-8626) incorrectly states that for the snmptrap user, the default password is "procurve". Instead, the default password is "trapuser."

Enhancements

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

WT.01.03 is the first software version for Wireless Edge Services zl Modules.

Note

The *Management and Configuration Guide* (5991-8626) provides detailed information on the features in software release WT.01.03. Download this guide for more information. To download this guide, see "Downloading Software and Documentation from the Web" on page 1.

Features

The following features are available with release WT.01.03 software. For more information, see the *Management and Configuration Guide* (5991-8626) released with WT.01.03 (or later) software.

Table 2. Key Features in Version WT.01.03 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.

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.

Capabilities

Capabilities and scalability of the ProCurve zl Wireless Edge Services Module are summarized in the following table.

Table 3. Summary of Capabilites and Scalability in WT.01.03

Feature/Function	WT.01.03
Throughput - Unencrypted	2000 mbits
Maximum number of Radio Ports supported	156
Maximum number of associated stations	4096
Maximum number stations per radio	256
Maximum number of modules in Redundancy Group	12
Maximum number of VLANs per module	32
Radio Port Failover time (Layer 2)	20 sec typical
Maximum number of static routes	300
Maximum number RADIUS Authentications per second	4 Internal / 3 LDAP
Maximum number of DHCP Lease Grants per second	15
Maximum number of modules in Layer 3 Roaming Group	12

Software Fixes

Release WT.01.03 is the first software release for the ProCurve Wireless Edge Services zl Module.

Known Software Issues and Limitations

This section identifies issues you may encounter when using a ProCurve Wireless Edge Services zl Module (J9051A) or a ProCurve Redundant Wireless Services zl Module (J9052A).

Release WT.01.03

Release WT.01.03 is the first software release for the ProCurve Wireless Edge Services zl Module (J9051A) and the ProCurve Redundant Wireless Services zl Module (J9052A).

- **Applet (39709)** — Regardless of whether a wireless client station is using the WMM power save feature, the Device Information -> Wireless Stations -> Details -> QoS information reports, "UAPSD enabled for: nothing". This display issue does not affect the function of the unscheduled automatic power save delivery (USPSD) feature.
- **Applet (41087)** — There is an uninformative error message when the user tries to attach more than one ACL to a WLAN. The error message, "Unable to save - Wrong data type" should more accurately indicate that there is already an ACL attached to the interface.
- **Applet (41343)** — After making a configuration change without applying the change, the web management interface allows you to change Network Setup tabs from Configuration to Module Statistics without warning you that your changes will be lost.
- **Applet (41387)** — The "wrong value" error triggered by configuration of overlapping excluded DHCP ranges is uninformative. The error should mention that overlapping IP address ranges are not permitted.
- **Applet (40023)** — The web management interface should disable (gray out) the **Delete** button when both the startup-config and running-config are chosen. Despite the presence of the delete option, running-config cannot be deleted; this is appropriate behavior.
- **Applet (40766)** — The web management interface allows removal of an ACL or ACE when it is in use by NAT.

  Best Practice: Review the configuration and attachment of ACLs as part of the planning process prior to ACL deletion.
- **Applet (40950)** — The list of ACLs displayed by the web management interface is ordered arbitrarily (e.g. not ordered alphabetically, numerically, or by type). Be sure to check the entire list if you are having difficulty finding an ACL you have configured, scrolling to the bottom of the list if necessary.
- **Applet (41184)** — The web management interface Ethernet Configuration screen does not properly gray out all the appropriate fields; enabling DHCP grays out only the subnet mask, but not the IP fields. Additionally, though the mask is grayed out, the dots in the field are not grayed out. This does not have a functional consequence.

- **Applet (41215)** — Since the ability to copy to the running-config has been removed from the web management interface, the **system:** button should not be displayed on the Management -> System Maintenance - Config File -> Transfer -> browse for location popup window.

  Workaround: Attempts at transferring to the file provide a meaningful message in the lower left window of the web management interface.

- **Applet (41372)** — After deleting a dynamic NAT entry and NAT interface from the web management interface, the screen does not properly repaint the area where a popup dialog box was placed.

- **Applet (41423)** — A static NAT entry is deleted if one of the parameters is modified using an invalid value.

  Workaround: If you are having problems with static NAT entries being deleted immediately after using the web management interface for configuration or modification, double check that all your configured parameters are valid and view the configuration file to confirm that the intended NAT rules are in place.

- **Applet (41504)** — The web management interface fails to warn the user if an ACE (Access Control Entry) that already exists is configured again. The ACE is appropriately disregarded rather than saved, but the user is not informed about why this action occurred.

- **Applet (41751)** — In the web management interface, the **Transfer Files** button is enabled even when there are no core or panic files present.

- **Applet (41761)** — When inserting DHCP IP address ranges (Network Setup -> DHCP Server -> Configuration -> Add -> Included Ranges window of the web management interface), use of the tab key cycles the curser between the Start IP and End IP fields without progressing to other fields. The user will have to use the mouse to get to the other parameter fields.

- **Applet (41764)** — The tab key does not allow the user to cycle through the various server fields of the web management interface page for Network Setup -> DHCP Server -> Configuration -> Add -> Servers fields. The user will have to use the mouse to progress through the various parameter fields.

- **Applet (41992)** — The web management interface's Device Information page erroneously displays the Troubleshooting -> Panic Snapshot page. The trigger for this event is unknown.

- **Applet (41768)** — There is inconsistent behavior between CLI and Applet while configuring the preferred and alternate methods for user login. The Applet requires that both a preferred and alternate method be specified, but the CLI does not have any requirement for an alternate method.

- **Applet (38562)** — The web management interface allows the universal broadcast address (255.255.255.255) to be configured as a DNS IP address.

- **Applet (39807)** — There should be an option to generate a Tech-Support file in the web management application, and there is not.

  Workaround: Generate this file using the CLI command. To do this using TFTP transfer, use the following command syntax.

  Host_zl_Switch# wireless-services <*slot id* >

  Host_zl_Switch(wireless-services-*slot*)# support copy tech-support tftp://<ip address of tftp server>/ <filename.tar.gz>

- **Applet (41536)** — In the web management interface L3 mobility page, changes made to the settings take affect without the user hitting the **Apply** button.

  Workaround: **Use caution** - do not click an option that you do not intend to configure on this screen.

- **Applet (40012)** — In the web management interface Special Features -> Station Intrusion Detection, clicking in any of the threshold value fields enables the **Apply** button, even when no changes were made. If the user has a concern that they inadvertently made a change, the **Revert** button may be used.

- **Applet (41721)** — The web management interface produces a Java console error message when a DDNS TTL value of 1 is configured for a DHCP pool. Additionally, the value does not get saved to the running configuration.

  Workaround: Though a DDNS TTL value of 1 would be an unusual setting, if the user desires this setting, reconfiguring it a second time will allow the value to be saved.

- **Applet (1000460321)** — The web management interface Security -> MAC Filters -> Authentication column has a "#" in place of MAC-Auth.

- **Applet (1000460349)** — The web management interface Help section for the Security -> NAT -> Configuration page states that the "list is empty".

- **Chassis (40367)** — The switch does not consistently report the correct module status after execution of the **halt** command. Typing **show wireless-services <*slot-id*>** at the switch CLI after the **halt** has been executed may show a status of "`not responding`" even though the module has been successfully shut down. It is safe to remove the module in that circumstance.

- **Chassis (41075)** — The chassis self test LED should not be extinguished until the module is fully booted and ready. It currently shuts off early.

- **CLI (40764)** — It is possible to configure a duplicate SSID (an invalid condition) using the CLI.

  Workaround: Configure SSIDs via the web management interface or validate your configuration by examination after CLI use.

- **CLI (41227)** — The CLI allows the user to enter the command to remove an access-group that does not exist without producing an error message.

- **CLI (40893)** — The sFlow timeout values that can be configured via the CLI differ from those considered valid by the web management interface. This does not have any significant consequence; values configured in either management context will be honored.

- **CLI (38053)** — There is no support for tethereal on the module.

  Workaround: Use the local or remote mirroring features of the switch to perform packet captures.

- **Infrastructure (41648)** — The web management interface does not display the management interface IP address for layer 3 mobility when the **no layer3-mobility local address** command is executed through the CLI. Although the CLI output to the **show layer3-mobility global** command correctly displays the management VLAN interface as the "local address", the web management interface continues to display the local interface IP address.

  Workaround: View the configuration using the CLI if there is some question about the active configuration.

- **Infrastructure (39772)** — When the primary RADIUS server is unavailable, a valid secondary RADIUS server configuration will successfully authenticate the wireless client, though the error messages generated may mislead the network administrator into thinking authentication did not occur. Syslog messages may be similar to the following (date, time and IP stamps were removed for clarity).

  ```
  %USER-3-ERR: WIOS_SNMP[981]:auth failed:user manager role 0 src 0
  %IMI-5-AUTHNOTIFY: Radius server secret not configured or server not
  reachable. Hence trying next auth method
  %PM-4-PROCNORESP: Process "fileMgmt" is not responding (2/20)
  %PM-4-PROCNORESP: Process "securitymgr" is not responding (1/20)
  %PM-4-PROCNORESP: Process "radconfd" is not responding (2/20)
  %PM-4-PROCNORESP: Process "leaseparsed" is not responding (1/20)
  %PM-4-PROCNORESP: Process "imi" is not responding (2/20)
  %PM-4-PROCNORESP: Process "ccstatsd" is not responding (2/20)
  %PM-4-PROCNORESP: Process "isDiag" is not responding (2/20)
  %PM-4-PROCNORESP: Process "snmpd" is not responding (2/20)
  %PM-4-PROCNORESP: Process "fileMgmt" is not responding (1/20)
  %PM-4-PROCNORESP: Process "radconfd" is not responding (1/20)
  %PM-4-PROCNORESP: Process "imi" is not responding (1/20)
  %PM-4-PROCNORESP: Process "ccstatsd" is not responding (1/20)
  %PM-4-PROCNORESP: Process "isDiag" is not responding (1/20)
  %PM-4-PROCNORESP: Process "snmpd" is not responding (1/20)
  %USER-5-NOTICE: WIOS_SNMP[961]: user ezhil login
  ```

- **Infrastructure (39875)** — Alternate (secondary) methods of user login are designed to function when the primary method is unreachable - not when the primary method fails.

- **Infrastructure (41564)** — The Img-File-Ver parameter in the CLI and the corresponding Management -> System Maintenance -> Update Server -> Software version parameter of the web management application are not required values, and they should be. The image file will not be pulled if the version is empty, even if the force-upload parameter is set.

- **Infrastructure (39890)** — Neither the CLI nor the web management interface allow a domain name string of more than 70 characters in the DHCP server scope configuration.

- **Infrastructure (40734)** — System administrators logged in with operator privileges are not able to execute the **show run** command at the CLI.

  Workaround: view the running configuration from the web management interface.

- **Infrastructure (41442)** — A socket error may be produced during use of the update server function, though the feature is not affected by the error.

- **Infrastructure (1000459250)** — VLAN statistics are not counting properly; both the web management interface and CLI and under reporting inbound and outbound utilization.

- **L2-L3 (41762)** — If a DHCP scope is configured on a VLAN that does not have an IP address, the module will have to be restarted after the IP address is assigned to the VLAN in order to allow the DHCP functionality to initialize properly.

  Best Practice: Configure interfaces first, then configure the services that will be used by the interfaces.

- **L2-L3 (40778)** — The web management interface allows duplicate IP addresses to be set for the DNS server, the default router, and the Netbios server settings. The CLI, given the same parameters, appropriately triggers an error.

  Best Practice: Review the running- or startup-config files for the validity of the IP addresses if problems are encountered.

- **L2-L3 (38070)** — The user is able to configure a DHCP excluded address that is already in use by the static DHCP pool.

  Workaround: Configure the DHCP range and exclusions prior to activating the DHCP server.

- **L2-L3 (39840)** — A second default gateway configuration will not overwrite the originally configured value, but will be ignored.

  Workaround: Remove the default gateway address prior to configuring a new address.

- **L2-L3 (41737)** — Attaching an IP ACL with an *allow any* ACE to the downlink port stops all the traffic on the downlink, even if there is a MAC extended ACL to explicitly allow ARPs.

  Workaround: ACLs attached to the downlink port need to explicitly allow the radio port traffic to get through to the module, as shown by a portion of a **show run** command below.

```
ip access-list extended 100
 permit ip any any rule-precedence 1
mac access-list extended 200
 permit any any type arp rule-precedence 1
 permit any any type 34691 rule-precedence 2
!
interface dnlink
 ip access-group 100 in
 mac access-group 200 in
```

- **L2-L3 (41469)** — The error message, "ERROR: There must be at least one peer in established state to execute this command" is always displayed when doing a reload from within the module CLI redundancy context, even when peers are present.

  Workaround: Execute the **reload** command from either the web management interface, or the module CLI.

- **L2-L3 (40107)** — DHCP boot file names are limited to 63 characters in both the CLI and the web management interface.

- **L2-L3 (40163)** — The DHCP hostname field is unable to accept non-alphanumeric characters.

- **Redundancy (41949)** — A wireless station may show up on multiple modules in a redundancy group after failing over from a module that was removed from the switch. Connectivity and traffic for the wireless station are not affected.

  Workaround: The genuine current wireless station owner is the one with the shortest amount of time in the "Last Active" field in the Device Information -> Wireless Stations -> Details button.

- **Security (36833)** — The integrated firewall feature is supported only for packets received on Layer 3 interfaces. For packets getting switched, no firewall protection is applied. The firewall functionality supports protection against various network level attacks and inspects each packet for possible corruption that can indicate some kind of attack.

- **Security (41086)** — The ACL logging functionality is not available for Layer 2 or WLAN ACLs.

- **Security (39537)** — FTP control packets are not getting appropriately marked when a standard access list is configured for marking TOS bits.

- **Security (1000460306)** — MAC filter rules are designed to apply to the association process. If a wireless station is already associated, a new “deny” MAC filter configured through Security -> MAC Filter in the web management interface does not take effect until the station re-associates. If the administrator wants the filter to take effect immediately, the wireless station should be disconnected via Device Information -> Wireless Stations -> Disconnect. Rules configured in the latter context take effect immediately.

- **Security (1000460347)** — Adding a MAC Filter via the web management interface (Device Information -> Wireless Stations -> Disconnect screen) only associates the rule to WLANs 1-64.

- **SNMP (39709)** — Configuration options that have been initiated but not saved in the CLI context cannot be edited via the web management interface. An "SNMP Exception" message will occur with the failure.

  Workaround: Save any changes made in the CLI from the CLI prior to attempting to edit them through the web management interface.

- **SNMP (40513)** — An SNMP timeout occurs when a DHCP option value containing more than 100 characters is entered in the DHCP pool configuration.

  Workaround: Keep the configuration of option values to 100 characters or less.

- **SNMP (39823)** — An SNMP timeout error may occur while generating a 2048 byte RSA key for use with a certificate.

  Workaround: Confirm that the key was not generated; sometimes the key gets generated but a false error message is produced. If the key was not generated, retrying key generation should resolve the issue.

- **SNMP (41053)** — The dynamic DHCP bindings viewed in the web management interface display the expiration time in GMT rather than accurately reflecting the configured time zone offset.

  Workaround: The expiration time is properly displayed in the output for the CLI command, **show ip dhcp binding**.

- **SNMP (37189)** — The module does not support “noAuthnoPriv” and “AuthnoPriv” security levels for SNMPv3 users, but the CLI supports the commands for setting those levels.

  Workaround: Configure SNMPv3 through the web management interface, which appropriately allows only the “AuthPriv” security level.

- **SNMP (40001)** — The SNMP port number for configuration of the trap destination is a optional parameter in the CLI, while it is a mandatory parameter in web management interface. The module administrator should use the configuration interface that best meets their needs.

- **Wireless (40983)** — Rate limiting is not applied to wireless stations that have roamed or have reconnected to the network if cached PMK is configured.

  Workaround: Disable PMK caching when vendor specific attributes are required for rate limiting a wireless client (e.g. when using IDM). PMK caching is a default WPA2 value, and may be disabled in the web management interface using Network Setup -> WLAN Setup -> Edit -> WPA/WPA2 -> Fast Roaming -> and uncheck PMK Caching.

- **Wireless (41726)** — Setting the country code after Rogue AP detection is enabled may cause the module to reset continuously. This is an unlikely scenario since the country code must be set prior to the module's ability to adopt radio ports and is unlikely to require a second configuration. Best Practice: Set the country code prior to configuring the module.

  Workaround: Disable Rouge AP detection prior to re-configuring the country code.

Part Number 5991-8624
September 2007