



Release Notes:

Version WA.02.15 Software *for the ProCurve Access Point 530*

The WA.02.15 software supports these access points:

- ProCurve Access Point 530 NA (J8986A)
- ProCurve Access Point 530 WW (J8987A)

These release notes include information on the following:

- Downloading access point software and documentation from the Web ([page 1](#))
- Clarification of operating details for certain software features ([page 8](#))
- A listing of software enhancements in recent releases ([page 10](#))
- A listing of software fixes in recent releases ([page 13](#))
- A listing of known software issues ([page 17](#))

Customers in the U.S.:

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

Effective July 20, 2007, new FCC regulations on the use of the 5 GHz 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 AP 530 product (J8986A) are disabled by software version WA.01.24 (and later).

The factory-installed software version WA.01.24 (and later) disables channels 52, 56, 60, 64 (5.25-5.35 GHz) in the U.S. These channels remain available for use in other countries.

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 by software version WA.02.15 (and later).

The factory-installed software version WA.02.15 (and later) 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 2007-2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Publication Number

5991-4720
April 2008

Applicable Products

ProCurve Wireless Access Point 530 NA (J8986A)
ProCurve Wireless Access Point 530 WW (J8987A)

Trademark Credits

Windows NT®, Windows®, and MS Windows® are US registered trademarks of Microsoft Corporation.

Adobe® and Acrobat ® are trademarks of Adobe Systems Incorporated.

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.

Open Source Software Acknowledgement Statement

This software incorporates open source components that are governed by the GNU General Public License (GPL), version 2. In accordance with this license, ProCurve Networking will make available a complete, machine-readable copy of the source code components covered by the GNU GPL upon receipt of a written request. Send a request to:

Hewlett-Packard Company, L.P.
AP 530 Program
GNU GPL Source Code
Attn: ProCurve Networking Support
MS: 5550
Roseville, CA 95747 USA

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

Contents

Access Point 530 Management

Related Publications	1
Software Updates	1
Downloading Access Point 530 Documentation and Software from the Web	1
Updating Software on the Access Point	2
Software updates through a WDS link	2
Using the CLI to Upgrade from a TFTP Server	3
Saving Configurations While Using the CLI	4
Accessing the Web Browser Interface After a Software Update	5
Clearing the Internet Explorer (IE) Browser Cache	5
Software Index for ProCurve Networking Products	6

Clarifications and Updates

SNMP	8
Available Channels with Software Updates	8
Local/Remote MAC Authentication Precedence	8
Using Multiple VLANs On a WDS Link	8
Probe List Feature Default Setting	9

Enhancements

Release WA.01.14 Enhancements	10
Release WA.01.17 Enhancements	10
Release WA.01.18 Enhancements	10
Release WA.01.19 Enhancements	10
Release WA.01.24 Enhancements	10
Release WA.02.10 Enhancements	11
New and Enhanced Features	11
New Features	11
Enhancements	12
Release WA.02.15 Enhancements	12
Customers in the European Union and Selected Countries/Regions*	12

Software Fixes

Release WA.01.14	13
Release WA.01.17	13
Release WA.01.18	14
Release WA.01.19	14
Release WA.01.24	14
Release WA.02.10	15
Release WA.02.15	16

Known Software Issues

Release WA.01.18	17
Configuration	17
Radio	17
WDS	18
General Performance and Limitations	18
Release WA.02.10	19
General Performance and Limitations	19
Known Issues	19
Release WA.02.15	20
Known Issues	20

Access Point 530 Management

Related Publications

For the latest version of any of the publications listed below, visit the ProCurve Networking Web site at <http://www.procurve.com>. Click on **Technical support**, then **Product manuals**.

- *ProCurve Wireless Access Point 530 Installation and Getting Started Guide*
- *ProCurve Wireless Access Point 530 Management and Configuration Guide*

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 Access Point 530 Documentation and Software from the Web

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

To Download a Software Version:

1. Go to the ProCurve Networking Web site at:
<http://www.procurve.com>.
2. Click on **Software updates**.
3. Under **Latest software**, click on **Wireless access points** and select the software version for your product model.

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

1. Go to the ProCurve Networking Web site at <http://www.procurve.com>.
2. Click on **Technical support**, then **Product manuals (all)**.
3. Click on the name of the product for which you want documentation.
4. On the resulting web page, double-click on the desired document.
5. When the document file opens, click on the disk icon  in the Acrobat® toolbar and save a copy of the file.

Updating Software on the Access Point

Note

Downloading new software does not change the current access point configuration. The access point configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another access point of the same model. **It is recommended that you save a copy of the configuration file before updating your access point software.**

After updating your access point, be sure to clear your browser cache. For more information, see [“Accessing the Web Browser Interface After a Software Update” on page 5.](#)

ProCurve Networking periodically provides switch software updates through the ProCurve Networking Web site (<http://www.procurve.com>). After you acquire the new software file, you can use one of the following methods for updating the access point software:

- The AP 530 Web Browser interface allows updates from a remote server using FTP, TFTP, or SCP. Alternatively, you can update the access point from your local system — simply copy the update file to your system and then browse to it.

To access these options, open the AP 530 Web Browser interface, and select **Management > System Maintenance > Software**.

For more information, refer to the *Management and Configuration Guide* for your access point.

- The AP 530 Command Line Interface (CLI) allows updates from a remote server using FTP, TFTP or SCP.

To access this option, initiate a CLI session and use the CLI **copy** command. See [“Using the CLI to Upgrade from a TFTP Server” on page 3.](#)

Software updates through a WDS link

- When updating software through a WDS link, HP recommends using SCP, which is a more reliable transport than TFTP or FTP.
- When updating software on APs that are configured for WDS, always update the remote APs before upgrading the base AP.
- Software version WA.02.07 or greater cannot establish a WDS link with software version WA.01.24 or earlier. Therefore, when upgrading remote WDS APs to version WA.02.07, the WDS link with the base AP will not be established until the base AP has been upgraded to version WA.02.07.

Using the CLI to Upgrade from a TFTP Server

This section describes how to use the CLI to update access point software from a TFTP server. Similar CLI command parameters allow upgrades using FTP or SCP.

Syntax: `copy tftp flash <ip> <file>`

For example, to update a software file named WA.02.01.img from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
ProCurve Access Point 530# copy tftp flash 10.28.227.103 WA.02.01.img
```

2. When the CLI prompt re-appears, it will validate the update:

```
The active software image will be replaced with the downloaded image,  
continue [y/n]? y
```

3. The CLI returns with the option to save the current configuration or the system resets to the factory defaults.

```
Do you want to save the current configuration [y/n]? n
```

4. Use the **show copy** command to verify that the copy operation is successful.

```
Copy Operation Status (FTP/SCP/TFTP)  
Last software image (flash) copy result: in progress  
Last configuration file copy result: not initiated
```

5. The CLI returns with the final confirmation that it is rebooting the new software image:

```
ProCurve Access Point 530#  
Connection to host lost.
```

6. Login again and use the **show version** command to verify that the new software version successfully upgraded.

Saving Configurations While Using the CLI

The access point operates with two configuration files:

- **Running-Config File:** Exists in volatile memory and controls access point operation. Rebooting the access point erases the current running-config file and replaces it with an exact copy of the current startup-config file. To save a configuration change, you must save the running configuration to the startup-config file.
- **Startup-Config File:** Exists in flash (non-volatile) memory and preserves the most recently-saved configuration as the “permanent” configuration. When the access point reboots for any reason, an exact copy of the current startup-config file becomes the new running-config file in volatile memory. The startup configuration contains the settings with which the access point will use the next time it starts up (for example, upon reboot).
- **Custom-Config File:** Exists in volatile memory and once configured controls access point operation. To save your custom configuration, you must save the running configuration to the custom-config file.

When you use the CLI to make a configuration change, the access point 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 access point reboots, the change will be lost. Here are three ways to save configuration changes while using the CLI:

- Execute **write memory** from the Manager, Global, or Context configuration level.
- Execute **copy running-config startup-config** from the Manager, Global, or Context configuration level.
- When executing the **copy x flash** and **reload** commands in the CLI, press **[Y]** (for Yes) at the “save configuration” prompt:

```
Do you want to save current configuration [y/n] ?
```

Accessing the Web Browser Interface After a Software Update

After a software update, we recommend that you complete these steps:

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

Clearing the Internet Explorer (IE) Browser Cache

We assume that you have already updated the software and reset the access point. Use the steps below to clear the browser's cache for IE version 6. For other versions, the steps may vary.

1. Open IE.
2. Select **Tools > Internet Options**. The **Internet Options** window is displayed.
3. Make sure that you are on the **General** tab.
4. In the **Temporary Internet files** section, click **Delete Files**. The **Delete Files** window is displayed.
5. Check the **Delete all offline content** box.
6. Click the **OK** button.
7. In the **Internet Options** window, click the **OK** button.

Software Index for ProCurve Networking Products

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)
U	Switch 2510 Series (2510-48)
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.)

Clarifications and Updates

SNMP

With software release WA.02.10 (or later), the ProCurve Access Point 530 supports an SNMP v3 (Simple Network Management Protocol version 3) agent, in addition to SNMP v1 and v2c agents. For more information, see [“Release WA.02.10 Enhancements” on page 11](#).

For configuration and use of SNMP, see the Web interface Help, and the latest edition of the *Management and Configuration Guide* (5991-2193, December 2007). To download this guide, see [“Downloading Access Point 530 Documentation and Software from the Web” on page 1](#).

Available Channels with Software Updates

With software release WA.02.10 (or later) installed, radio channel allocations may be different from your prior configuration due to product regulatory changes. If your AP 530 was configured with a static channel assignment that is not supported in the new software, the radio will be reset to **Auto**.

To view the available channels for a radio:

1. In the Web interface, select **Network Setup > Radio**.
2. On the **Radio** page, select a radio. Enable the radio by setting **Status** to **On**.
3. On the **Radio** page, view the **Channel** drop-down list. All of the available channels will be displayed.

Local/Remote MAC Authentication Precedence

Local MAC Authentication (via access control lists) will always override Remote MAC Authentication. For example, if a station (MAC) address is contained in a local allow list, that station will be authenticated even if it is contained in a remote deny list. Conversely, if a station address is contained in a local deny list, or the MAC Lockout list, that station will never be authenticated.

Using Multiple VLANs On a WDS Link

Multiple VLANs can be used across a WDS (Wireless Distribution System) link. There are no dependencies of VLAN tagging across a WDS link. The number of VLAN IDs (VIDs) that can be used across a WDS link is the same as for the Ethernet port used by the base AP 530 (the one with the Ethernet connection to the wired network). The base AP 530 does not require VLAN configuration to support VIDs on WDS links to remote access points.

Probe List Feature Default Setting

The AP 530 supports a table of Probe requests from unassociated clients. This Probe Table (or Probe List) may be used by ProCurve Mobility Manager (PMM) for client-location purposes.

In general releases of WA.02.xx software versions prior to WA.02.15, the Probe List feature was *enabled* by default, and could not be disabled. In version WA.02.15 (or later), the Probe List is *disabled* by default, and may be enabled by PMM or SNMP management tools.

Enhancements

Unless otherwise noted, each new release includes the features added in all previous releases. To review significant enhancements since the last general release published, begin with [“Release WA.02.15 Enhancements” on page 12.](#)

Release WA.01.14 Enhancements

- WiFi Certification

Release WA.01.17 Enhancements

No enhancements in this release.

Release WA.01.18 Enhancements

- SNMP Save Running Configuration (PR_1000354174) — Prior to WA.01.18, users could not save the running configuration, from SNMP, and could potentially lose custom configuration information if the configuration is not saved from the serial console or Web interface. This version adds the ability to write the running configuration to the startup configuration, in flash memory, from SNMP.
- SVP Compliance — The AP 530 has been SpectraLink View pre-certified with this release.

Release WA.01.19 Enhancements

No enhancements in this release.

Release WA.01.24 Enhancements

- **Customers in the U.S.: FCC Changes to Dynamic Frequency Selection (DFS) in the 5 GHz Band** — Effective July 20, 2007, new FCC regulations on the use of the 5 GHz 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 AP 530 product (J8986A) are disabled by software version WA.01.24.

The factory-installed software version WA.01.24 disables channels 52, 56, 60, 64 (5.25-5.35 GHz) in the U.S. These channels remain available for use in other countries.

Release WA.02.10 Enhancements

New and Enhanced Features

Note

The *Management and Configuration Guide* (5991-2193, December 2007) has been updated with information on the enhancements and new features in software release WA.02.10. For more information, download this guide. To download this guide, see [“Downloading Access Point 530 Documentation and Software from the Web” on page 1](#).

New Features

The following new features are available with release WA.02.10 software. For more information, see the *Management and Configuration Guide* (5991-2193, December 2007) released with WA.02.10 (or later) software.

Table 1. New Features in WA.02.10 Software

Feature	Description
Adaptive Tx Power Control (ATPC)	Network Setup > Radio > Advanced Settings [Edit]: Dynamically adjusts radio power levels to reduce same-channel interference between access points. Channel power will adjust to provide maximum coverage with minimum interference. ATPC operating modes can be set for least interference between APs (AP mode) or to service obstructed or distant clients (AP + Client mode).
Group Configuration	Management > Group Configuration: Synchronizes configuration of common settings across up to twelve APs on the same subnet. This allows the administrator to configure groups of APs through the administrator interface (Web, CLI or SNMP) of any one of the APs. The shared configuration items include settings that are typically static across all APs (SSID, security, local RADIUS users, MAC Authentication tables). However, radio configuration, IP address and other settings that are typically unique for each AP are not shared across the group.
Web Authentication (Web-Auth)	Network Setup > WLANs > [Edit] > Web Authentication: Provides 802.1X authentication of wireless users on a “per-WLAN” basis <i>without</i> requiring an 802.1X supplicant on the client. When Web Authentication is configured, a user must only open their Internet browser to access the Web Authentication (Web-Auth) login page. A user/password as well as a guest mode (which requires no username/password) is supported.
AP Authentication	Management > AP Authentication: Enables the access point to act as an 802.1X “user” on the network. When this feature is enabled, and the switch port to which the AP is connected requires 802.1X authentication, the AP will provide a pre-configured username and password to the switch port during initialization. PEAP and MD5 EAP types are supported

Feature	Description
SNMPv3	Management > SNMP and Management > SNMP > SNMPv3 Users : SNMPv3 support provides the ability to have an authenticated, encrypted SNMP management connection to the AP 530. Provides SHA (shared key) or MD5 user authentication, and DES or AES data encryption privacy, for up to ten SNMPv3 users.
sFlow	sFlow agents monitor traffic on the Ethernet and two wireless interfaces (radio 1 and radio 2). A statistical sampling of traffic is delivered to sFlow receivers which reside in the management application (such as ProCurve Manager Plus and ProCurve Network Immunity Manager). The management applications analyze the statistical sampling for traffic management, intrusion detection/prevention, security auditing and billing.
MAC Lockout	Special Features > MAC Lockout : MAC Lockout is a list of unwanted station MAC addresses that are global to the entire AP. When an address is added to the MAC Lockout list, that station is de-authenticated (disconnected from) the AP if it is currently associated.
Station De-Authentication	Disassociates a station from the AP, but does not prevent the station from re-associating. This feature, available only through SNMP access, is typically used to analyze a station, and then force that station to another VLAN by forcing it to re-authenticate.
Probe List	A table of unassociated clients is maintained internally and accessible through SNMP access. Signal strength information (RSSI) is provided for each station. ProCurve Mobility Manager (PMM) will use this information to provide locationing services in a future release.

Enhancements

- The dynamic range of attenuation has been increased. With version WA.02.10 (or later) the radio power can be reduced below 0 dBm.
- The Web interface Event Log is now a circular buffer, instead of simply running out of space and then clearing all entries.

Release WA.02.15 Enhancements

Customers in the European Union and Selected Countries/Regions*

In the European Union and selected countries/regions*, AP 530 products purchased after April 1, 2008, are subject to new radar interference requirements in the 5 GHz band. Software version WA.02.15 (and later) 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.

For more information, see [“Customers in the European Union and Selected Countries/Regions*”](#) on the front cover.

Software Fixes

Release WA.01.05 was the first software release for the ProCurve Access Point 530.

Release WA.01.06 through WA.01.13 were not released.

To review the list of fixes since the last general release published, begin with [“Release WA.02.10” on page 15](#).

Release WA.01.14

Problems Resolved in Release WA.01.14

- **SNMP (PR_1000340419)** — add support for forced wireless client deauthentication. Added hpWlanApClientConfigTable with object hpWlanApClientSessionState.
- **WiFi Certification (PR_1000340875)** — WiFi certification requirement fix; RADIUS key length can be up to 64 bytes long.

Release WA.01.17

Problems Resolved in Release WA.01.17 (not a general release)

- **SNMP Neighboring Detection Limitation (PR_1000352286)** — prior to WA.01.17, ad-hoc networks were being identified as "other" by SNMP. They are now being correctly identified as "adhoc".
- **Group Key Corruption (PR_1000339520)** — key prevents client from receiving broadcast traffic. With certain clients, the broadcast key negotiation was failing after the unicast key was properly received. This prevented the client from receiving broadcast traffic. The most common symptom would be for the client to not receive DHCP responses when associating to an SSID that is connected to a different subnet than the client was previously bridged to, resulting in a DHCP timeout.
- **Wireless Process Termination (PR_1000349319)** — one of the software processes that sets up and maintains client associations abnormally terminates. This causes all clients to lose association. The AP can still be configured through all interfaces. Most configuration changes will result in the wireless subsystem process restarting, allowing clients to reconnect.
- **SNMP Trap Send Failures (PR_1000338452)** — if an SNMP trap host was specified with an unreachable IP address, memory would be consumed but notification was not returned to the system for each unsuccessful trap send attempt. In some cases where the trap host was properly configured, traps would still not be transmitted. Eventually the access point would run out of memory and reboot, or the SNMP process would terminate.

Software Fixes

Release WA.01.18

- **SNMP Hex Format Limitation (PR_1000352285)** — prior to WA.01.17, WEP keys could not be configured in hex format through SNMP.
- **SNMP Trap Host Limitation (PR_1000336324)** — prior to WA.01.17, there was no enforced limit to the number of trap hosts configurable using SNMP. The maximum number of traps hosts has now been set to four.

Release WA.01.18

Problems Resolved in Release WA.01.18

- **SNMP AP Detection Duration Limitation (PR_1000354169)** — prior to WA.01.18, users were unable to set AP detection duration from SNMP. This version fixes the SNMP error that is returned and sets the AP detection duration to the specified interval.
- **SNMP Save Running Configuration (PR_1000354174)**
Prior to WA.01.18, users could not save the running configuration, from SNMP, and could potentially lose custom configuration information if the configuration is not saved from the serial console or Web interface. This version adds the ability to write the running configuration to the startup configuration, in flash memory, from SNMP.

Release WA.01.19

Problems Resolved in Release WA.01.19

- **SNMP Add Trap Limitation (PR_1000357838)** — prior to WA.01.19, users were unable to add trap hosts from SNMP. This version fixes the SNMP error that is returned when adding a trap host to a factory default configuration.

Release WA.01.24

Problems Resolved in Release WA.01.24

- **Enhancement (For customers in the U.S.): FCC Changes to Dynamic Frequency Selection (DFS) in the 5 GHz Band** — For more information, see [“Release WA.01.24 Enhancements” on page 10](#).

Release WA.02.10

Problems Resolved in Release WA.02.10

- **DHCP (PR_1000460749)** — DHCP works correctly when the HTTP interface is disabled.
- **NTP (PR_1000392832)** — NTP (Network Time Protocol) time synchronization now operates properly when a static IP address is configured and the AP is rebooted. Previously, an AP reboot with a static IP would prevent NTP from working.
- **Radio (PR_1000408165)** — When selecting a static channel in 802.11a mode in a channel band that is subject to DFS, the AP will not perform an auto-channel select scan.
- **RADIUS (PR_1000409906)** — Loopback address (127.0.0.1) no longer appears in NAS IP field for RADIUS authentication.
- **Security (PR_1000416892)** — When a dynamic VLAN is sent by the 802.1X server, the AP 530 now handles a tag value of `tunnel-pvt-group-id` independent of other tunnel attributes.
- **Security (PR_1000406308)** — The WPA-PSK key can now be specified as a 64-character hex key in addition to an ASCII key (8-63 characters).
- **Security (PR_1000392848)** — The admin password is preserved over a reboot when saved via the Web interface.
- **SNMP (PR_1000394734)** — The AP will not reboot after enabling SNMP and attempting to save the startup-config via TFTP.
- **Vocera (PR_1000766645)** — Vocera phone traffic is now properly bridged when the handset roams to another access point.
- **WDS (PR_1000336904)** — Changes to the WPA type on a WDS link no longer causes a WDS link failure.
- **Web Interface (PR_1000381272 and 1000381276)** — Web interface display issues corrected when SSL (HTTPS) is enabled and HTTP is disabled.
- **Web Interface (PR_1000444207)** — Web interface now accepts special characters for text entry fields (SSID string, shared secret, location, etc.).

Release WA.02.15

Problems Resolved in Release WA.02.15

- **SNMP (PR_1000764578)** — The enable/disable control was not implemented for the probe list feature.
- **SNMP (PR_1000768225)** — Radio 1 was missing from the SNMP radio table after a change was made through the Web Interface or management application.
- **SNMP (PR_1000774455)** — De-authenticate would not allow a user's credentials to be renewed when an external RADIUS server is configured.
- **SNMPv3 (PR_1000765786)** — Users could not be created or deleted through SNMP.
- **Software Updates (PR_0000003817)** — When performing a software update to a version that did not allow the radio to operate on the previously configured channel, the radio would not always initialize, and the access point would not fully boot up to the login prompt.
- **Configuration (PR_1000754580)** — The broadcast key rotation would not be properly refreshed for clients. This caused issues with any broadcast services such as DHCP.
- **Enhancement (For the European Union and Selected Countries/Regions):** Changes to Dynamic Frequency Selection (DFS) in the 5 GHz Band — For more information, see [“Release WA.02.15 Enhancements” on page 12](#).

Known Software Issues

To view the known software issues for the latest general release, see [“Release WA.02.15” on page 20](#).

Release WA.01.18

The following issues have been identified in this release:

Configuration

- **Ethernet assignment** — Changes to Ethernet settings (speed, duplex) are not properly assigned until the access point is rebooted.
- **Local RADIUS 802.1X Authentication** — The local, built-in RADIUS server supports only one EAP type - PEAP-MSCHAPv2. This EAP type must be used when the local RADIUS server is configured for **Internal Server as failover** on the RADIUS Servers tab when configuring WLAN security.

Radio

- **Radio2 configuration (CLI, Radio2 context)** — ProCurve recommends you use the Web browser interface for configuring Radio2. Use the config context in the CLI for only repetitive tasks. In the CLI, radio1 context is used to configure a WLAN; radio2 context only enables and disables WLANs. To set up WLAN security, you can only configure it in radio1 context, even if you are not going to enable the WLAN on radio1. A WLAN may be enabled only on radio2 if your network requires it.
- **Radio power** — The following statements only apply to the J8987A (WW SKU).

The following issue is only a concern when used in countries under the ETSI regulatory domain.

The J8986A (NA SKU) is not affected by this issue (since FCC maximum power limits are considerably higher than ETSI limits).

The following statements apply to BOTH Radio 1 (802.11b/g) and Radio 2 (802.11a/b/g).

- When using the J8448A 2.4 GHz YAGI antenna in 802.11b or 802.11g mode, the conducted transmit power of the radio must not exceed 3.5 dBm.
- The "TX Power Reduction" entry can be used to reduce the conducted transmit power of the radio.
- However, in 802.11b mode, no matter how large a "TX Power Reduction" is applied, the radio will only go down to 10 dBm.
- Therefore, the user must supply an additional loss of 6.5 dB between the radio and the J8448A 2.4 GHz YAGI antenna in order to be compliant with ETSI regulations.
- This loss can be easily supplied using an adequate length of RF cable to connect the radio and the J8448A 2.4 GHz YAGI antenna.

- In 802.11g mode, the radio WILL go down below 10 dBm when adjusted via "TX Power Reduction".
- Therefore, no additional loss is required to operate in 802.11g mode.

NOTE:

802.11g mode = "802.11g mode" in CLI/WebUI software = normal 802.11b/g mode (all CCK and OFDM rates)

802.11b mode = "802.11b mode" in CLI/WebUI software = pure 802.11b mode (CCK rates only)

WDS

■ **Configuring WDS Security** —

- The security settings on WLAN1 must be the same in all link members.
- The table below shows the security settings that may be used with WDS in this release:

WLAN1 Security Mode Choices for WDS links (1-6)
No Security (not recommended)
Static WEP
WPA-PSK, TKIP cipher
WPAA-PSK, AES cipher

- **Local Upgrade** — The Web/UI local upgrade feature is not supported across a WDS connection. If this feature is attempted, the access point may become unreachable through the wireless network until it is rebooted. We recommend using **FTP** or **TFTP** to perform the upgrade. See [“Using the CLI to Upgrade from a TFTP Server” on page 3](#) for more information.

General Performance and Limitations

- **Access Point 802.1X authentication** — There is no supplicant in the access point, so it cannot be authenticated using 802.1X. MAC authentication may be used to prevent unauthorized access points attaching to the network.
- **Messaging** — Syslog messages contain many debug level messages that would normally not be seen at a default logging level. Since there are no configurable logging levels in this release, all messages are sent to syslog.
- **Time Zone** — A time zone cannot be set, so event log files do not reflect local time.
- **VLAN authentication** — If you dynamically assign a VLAN that is statically assigned either by the WLAN settings or it is the management VLAN or untagged VLAN, the authentication is not successful and is continually trying to authenticate.
- **Wireless Statistics** — The Transmit Errors count on the Wireless Statistics screen does not work. It always shows zero.

- **Web U/I Event Log Size** — The Web U/I has a limited amount of memory for containment and display of the event log. When the size of the event log has grown larger than the amount of available memory allocated for Web display of the event log, all messages are purged from the display. A complete list of events is available in the CLI.

Release WA.02.10

The following issues have been identified in this release.

General Performance and Limitations

- **WDS** — A WDS AP can support up to 20 WLANs, whereas a non-WDS AP can support up to 32 WLANs. For WDS operation, we recommend that you dedicate one radio for the WDS link, and the other radio for client associations. In this case, all 16 WLANs on one radio can be configured to service client associations.
- **WDS** — When WEP encryption is used for the WDS link, throughput is lower than WPA-PSK or no-security. WPA-PSK is the recommended security model for the WDS link as it offers maximum security and throughput.
- **Web-Auth (PR_1000765640)** — Web-Auth can only be configured for up to three independent WLANs (six total if both radios are enabled).
- **Configuration Time** — Applying configuration changes to radios or WLANs may require several seconds to a minute or longer if the radios are enabled and multiple WLANs are configured. During AP setup or configuration of multiple parameters, the configuration speed can be improved by disabling the radios during configuration.
- **SNMP** — SNMPv3 users must have an authentication (MD5 or SHA) method. If no authentication is desired, SNMPv2 should be used.
- **TKIP/AES (PR_1000750254)** — Stations will have a higher maximum throughput with TKIP encryption compared to AES.

Known Issues

- **Group Config (PR_1000765775)** — Group Config requires that a Default Gateway be configured even if a Default Gateway is not being used.
- **SNMP (PR_1000765789)** — When upgrading from WA.01.XX to WA.02.XX (or later), SNMP v1/v2c will be enabled, even if it was disabled before upgrading the software.
- **SNMP (PR_1000765786)** — Adding or deleting SNMPv3 users must be done through the CLI. For example, when using SNMP to add or remove users, deleting a user from SNMP deletes it from the USMUserTable but does not delete it from the SECURITY or VIEW tables. This problem has been fixed, see [“Release WA.02.15” on page 16](#).

Known Software Issues

Release WA.02.15

- **SNMP (PR_1000766324)** — The following SNMP v1/v2 traps are only accessible via the Web interface (not SNMP or the CLI):
 - hpWlanMacLockoutStaLockedOut
 - hpWlanMacLockoutStaAuthAttempt
- **AP Detection Settings (PR_1000747438)** — AP detection **Scan Interval**, **Scan Duration**, **Entry Expiration Time**, and **Max Entries** values are not configurable.
- **Ethernet Port (PR_1000418278)** — Ethernet port interoperability issues have been observed when setting the AP 530 Ethernet port to 10 Mbps, half-duplex operation.
- **Rate Limiting (PR_1000446745)** — Broadcast/Multicast rate limiting is not enabled in this release.
- **Authentication/Association (PR_1000765781)** — WPA clients are displayed as “Authenticated” and “Associated”, even if they are “Associated” but not “Authenticated”.

Release WA.02.15

Known Issues

- **SNMP (PR_1000463453)** — Stations missing from the clients table. While the AP 530 Web Interface and CLI correctly display associated stations, the SNMP query is intermittently missing these entries.
- **SNMPv3 (1000765292)** — When creating an SNMPv3 user, an authentication method must be assigned before the user can access the MIB (read or write access).



© 2007-2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

April 2008
Manual Part Number
5991-4720