



Release Notes: Version WA.01.24 Software *for the ProCurve Access Point 530*

The WA.01.24 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 5](#))
- A listing of software enhancements in recent releases ([page 8](#))
- A listing of software fixes in recent releases ([page 9](#))
- A listing of known software issues ([page 11](#))

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.

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*

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

Publication Number

5991-4720
October 2007

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

Software Updates	1
Downloading Access Point 530 Documentation and Software from the Web	1
Updating Software on the Access Point	1
TFTP Download from a Server	2
Saving Configurations While Using the CLI	3
Software Index for ProCurve Networking Products	4

Clarifications and Updates

SNMP	5
Documentation Clarifications	7
Installation and Getting Started Guide:	7
Management and Configuration Guide:	7

Enhancements

Release WA.01.14 Enhancements	8
Release WA.01.17 Enhancements	8
Release WA.01.18 Enhancements	8
Release WA.01.19 Enhancements	8
Release WA.01.24 Enhancements	8

Software Fixes

Release WA.01.14	9
Release WA.01.17	9
Release WA.01.18	10
Release WA.01.19	10
Release WA.01.24	10

Known Software Issues

Release WA.01.18	11
Configuration	11
Radio	11
SNMP	12
WDS	12
General Performance and Limitations	12

Access Point 530 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 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**.

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**.
3. Click on the name of the product for which you want documentation.
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.

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.

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 downloading it to the access point:

- For a TFTP transfer from a server, do either of the following:
 - Select **Software Tab** in the System Maintenance menu option in the Access Point 530 Web Browser interface and use the **TFTP** option.
 - Use the **copy tftp** command in the access point's CLI (see below).
- Use the local upgrade option on the Management > Systems Maintenance > Software tab.

Note

When updating software an access point through a WDS link, HP recommends using SCP, which is a more reliable transport than TFTP or FTP.

This section describes how to use the CLI to update access point software. You can also use the Web Browser interface for software updates. For more information, refer to the *Management and Configuration Guide* for your access point.

TFTP Download from a Server

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

For example, to update a software file named WA.00.01.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.00.01.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) when you see the “save configuration” prompt:

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

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)
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

The ProCurve Access Point 530's implementation of the Simple Network Management Protocol (SNMP) agent in software release WA.01.14 supports SNMP versions 1 and 2c. Management access from SNMP v1 or v2c stations is controlled by community names. To communicate with the access point, an SNMP v1 or v2c management station must first submit a valid community name for authentication. If you intend to support SNMP v1 or v2c managers, you must configure the read-only and read-write community names.

To configure SNMP community names:

- **Web Interface** - Select Management > SNMP > Settings tab.
- **CLI** - Execute **snmp-server community** command prior to using the **snmp-server host** command from the Manager, Global, or Context configuration level.

You can configure the access point to respond to SNMP requests and generate SNMP traps. When SNMP management stations send GET or SET requests to the access point, the SNMP responds with the requested data or the status of the set operation. This software release supports SNMPv1 and SNMPv2c GET/SET requests. The access point can also be configured to send information to SNMP managers through trap messages. The ProCurve Access Point 530's SNMP agent supports sending SNMPv2c compliant traps to the configured trap destination hosts.

NOTE: SNMPv1 and SNMPv3 traps are not supported in the current release.

The following traps are not supported in the current software release:

- **hpWlanSystemUpNOTIFICATION** - This notification is sent when the access point is fully up and running.
- **hpWlanSystemDownNOTIFICATION** - This notification is sent before the access point is about to reboot.
- **hpWlanMgmtAccessUpdateNOTIFICATION** - This notification is sent when system management access is set to Enable/Disable.
- **hpWlanButtonUpdateNOTIFICATION** - This notification is sent when the RESET and CLEAR button functions are set to Enable/Disable.

Clarifications and Updates

SNMP

- **hpWlanSystemFWUpgradeStatusNOTIFICATION** - This trap contains information about the current status of software update. The sent IP address is the file server's IP address.
- **hpWlanSystemConfigFileTransferNOTIFICATION** - This trap contains information about the file name and server address of the configuration file. The sent IP address is the file server's IP address.
- **hpWlanRadioAntennaUpdateNOTIFICATION** - This notification is sent when the antenna configuration is changed.
- **hpWlanDot1XAuthNotInitiatedNOTIFICATION** - This notification is sent when a station did not initiate 802.1X authentication with the RADIUS server. The notification value includes the MAC address of the station that did not initiate 802.1X authentication.
- **hpWlanApInterfaceUpdateNOTIFICATION** - This notification is sent out when the Ethernet or 802.11 wireless (radio) interface is enabled or disabled.
- **hpWlanApSSIDUpdateNOTIFICATION** - This notification is sent out when an SSID is enabled or disabled.
- **hpWlanVlanUntaggedUpdateNOTIFICATION** - This notification is sent when the VLAN ID is set to untagged.
- **hpWlanMgmtVlanIdUpdateNOTIFICATION** - This notification is sent if the management VLAN ID is changed.
- **hpWlanApDetectionUpdateNOTIFICATION** - This notification is sent when AP detection scan is set to Enable/Disable.
- **hpWlanAdHocNetworkDetected NOTIFICATION** - This notification is sent when AdHoc is detected.
- **hpWlanRadiusAccountingUpdate NOTIFICATION** - This notification is sent when RADIUS Accounting is set to Enable/Disable.

Documentation Clarifications

Installation and Getting Started Guide:

- Initial release of this guide mistakenly listed SNMP agent support for SNMP v3 in this software release. The Web Version has updated this information.

Management and Configuration Guide:

- Incorrect trap identification:
 - AP Trap “hpWlanLocalMacAuthstationsuccess” should be “hpWlanLocalMacAuthClientSuccess”
 - AP Trap “hpWlanRemoteMacAuthstationsuccess” should be “hpWlanRemoteMacAuthClientSuccess”
 - Authentication Trap “hpWlanLocalMacAuthClientFail” should be “hpWlanLocalMacAuthClientFailure”
 - Dot1X Trap “hpWlanRemoteMacAuthstationsuccess” should be “hpWlanRemoteMacAddrAuthSuccess”
 - Dot1X Trap “hpWlanRemoteMacAuthClientFail” should be “hpWlanRemoteMacAddrAuthFailure”

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.01.24 Enhancements” on page 8.](#)

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.

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.01.24” on page 10](#).

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.

- **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 8.

Known Software Issues

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)

SNMP

- **SNMPv3 is not supported.** See [“SNMP” on page 5](#) for more information.

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 [“TFTP Download from a Server” on page 2](#) 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.



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

October 2007
Manual Part Number
5991-4720