



Release Notes: Version 2.0.41

for the HP ProCurve Wireless Access Point 420

These release notes include information on the following:

- Downloading access point software and documentation from the web (page [1](#))
 - Downloading software to the access point (page [1](#))
 - Features in release 2.0.41 (page [5](#))
 - Clarification of Operating Details for Certain Software Features (page [10](#))
 - Software fixes (page [14](#))
 - Known software issues and limitations (page [19](#))
-

Software Update Notice

Check the HP ProCurve web site frequently for free software updates for the various HP ProCurve access points you may have in your network (see page [1](#)).

**© Copyright 2001, 2005 Hewlett-Packard Company, LP.
The information contained herein is subject to change
without notice.**

This document contains information which is protected by copyright. Reproduction, adaptation, or translation without prior permission is prohibited, except as allowed under the copyright laws.

Publication Number

5990-6007
May 2005

Applicable Product

HP ProCurve Wireless Access Point 420 na (J8130A)
HP ProCurve Wireless Access Point 420 ww(J8131A)

Trademark Credits

Microsoft®, Windows®, MS Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Disclaimer

The information contained in this document is subject to change without notice.

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.hp.com/go/hpProCurve>

Contents

Software Management

Downloading Access Point Documentation and Software from the Web	1
Downloading Software to the Access Point	1
TFTP Download from a Server	3

Features in Release 2.0.41

Features in Release 2.0.41	5
--------------------------------------	---

Clarification of Operating Details for Certain Software Features

Operating Systems, Web Browsers, and Java Support	10
Configuring Encryption and MAC Authentication	11
Maximum Number of Associated Clients	13

Software Fixes

Release 2.0.41	14
Release 2.0.40	14
Release 2.0.39	14
Release 2.0.38	15
Release 2.0.37	18
Release 2.0.34	19
Release 2.0.29	19

Known Software Issues and Limitations

Limitations	19
Software Problems	20

— *This page is intentionally unused.* —

Software Management

Downloading Access Point Documentation and Software from the Web

You can download software version 2.0.41 and the corresponding product documentation from HP's ProCurve web site as described below.

To Download a Software Version:

1. Go to HP's ProCurve web site at <http://www.hp.com/go/hpProCurve>.
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 HP's ProCurve web site at <http://www.hp.com/go/hpProCurve>.
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.

Downloading Software to the Access Point

HP periodically provides access point software updates through the HP ProCurve web site (<http://www.hp.com/go/hpProCurve>). After you acquire the new software file, you can use one of the following methods for downloading the software to the access point:

- For an FTP/TFTP transfer from a server, place the software file in your FTP/TFTP server's default directory. Then do either of the following:
 - Click on **Software Upgrade** on the **Administration** tab of the access point's web interface and use the **Software Upgrade Remote** section.
 - Use the **copy tftp file** command in the access point's CLI (see below).
 - For an HTTP transfer from a PC, do the following:
 - Click on **Software Upgrade** on the **Administration** tab of the access point's web interface and use the **Software Upgrade Local** section.
-

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. HP recommends that you save a copy of the configuration file before upgrading your access point software. See “Transferring Configuration Files” in the *HP ProCurve Wireless Access Point 420 Management and Configuration Guide* for information on saving the access point’s configuration file.

The access point stores two software files in its flash memory. One has a file name such as **hp420-2039.bin**, which is the current version of software the access point runs. The current software file is overwritten when new software is downloaded to the access point. The other software file, called **dflt-img.bin**, contains a default version of the access point software that is used if the current software file is deleted or fails. The **dflt-img.bin** file cannot be deleted from the system or overwritten.

This section describes how to use the CLI to download software to the access point. For more information, refer to the *Management and Configuration Guide* for your access point.

Caution

A configuration file saved under version 2.0.38 or greater is NOT backward-compatible with previous software versions. The user is advised to save a copy of the pre-2.0.38 configuration file BEFORE UPGRADING to 2.0.38 or greater, in case there is ever a need to revert back to pre-2.0.38 software. Instructions for saving a copy of the configuration file are found in the “Transferring Configuration Files” section of Appendix A in the *Management and Configuration Guide* that shipped with the access point.

Note

After an upgrade to software version 2.0.38 or greater from 2.0.34, the following syslog error message is generated:

```
snmpd: trap Error --Can't get IP by host name:  
init_traps: failed to create SNMPv2 Trap session
```

This is due to the default SNMP trap host name for version 2.0.34 being an enabled null value.

TFTP Download from a Server

Syntax: **copy tftp file**

For example, to download a file named **hp420-2041.bin** from a TFTP server with the IP address of 10.1.0.9:

1. Execute the copy command as shown below:

```
HP420#copy tftp file
1. Application image
2. Config file
3. Boot block image
Select the type of download<1,2,3>:  [1]:1
TFTP Source file name:hp420-2041.bin
TFTP Server IP:10.1.0.9

Removing old runtime! Please wait a few minutes!

Creating file! Please wait a few minutes!
Firmware version of system is v2.0.29 and Updating Run-Time code v2.0.41
NOW!
This firmware is compatible with hardware.
Updating Boot Line in NVRAM, please wait!
Warning! Updating firmware may cause configuration settings to be
incompatible.
(Suggestion:Using new default configuration settings lets system be more
efficient,but system will lose current settings.)
Do you want to use NEW CONFIG SETTINGS? <y/n> [n]:n
HP420#reset board
Reboot system now? <y/n>: y
```

2. When the access point finishes downloading the file from the server, a number a messages are displayed as the software is installed before a prompt **“Do you want to use NEW CONFIG SETTINGS? <y/n> [n]:”** appears.
3. Type **“y”** to reset the configuration to default values and reboot the access point to activate the downloaded software. Type **“n”** to continue to use the current configuration settings without rebooting.

Caution

New software that is incompatible with the current configuration automatically restores the access point to default values when first activated after a reboot.

4. If you typed “n” to continue using the current configuration settings, you must type **reset board** to reboot the access point and activate the downloaded software.

Features in Release 2.0.41

Features in Release 2.0.41

Support for the HP ProCurve family of omnidirectional and directional antennas, extending the reach of the HP ProCurve Wireless Access Point 420. Extend wireless connectivity within an office setting, warehouse, or retail environment. Expand your wireless network to provide campus-wide indoor and outdoor coverage. The following antennas are supported.

Antenna Type	Part Number	Mounting	Horizontal Beamwidth (3dB)	Vertical Beamwidth (3dB)
2 dBi indoor omnidirectional diversity	J8442A	Ceiling grid	360 Degrees	80 Degrees
5 dBi indoor/outdoor omnidirectional	J8441A	Ceiling or mast	360 Degrees	31 Degrees
6.5 dBi indoor/outdoor directional diversity	J8445A	Flush wall mount, articulating mount for wall or mast	80 Degrees	55 Degrees
7 dBi indoor/outdoor directional	J8443A	Flush wall mount with integrated articulating feature	65 Degrees	50 Degrees
8 dBi outdoor omnidirectional	J8444A*	Mast	360 Degrees	12 Degrees
11 dBi indoor/outdoor wide angle directional	J8446A*	Flush wall mount, tilt mount for mast	120 Degrees	13 Degrees
* These antennas are not permitted for use in North America.				

For more information visit the HP ProCurve web site at: http://www.hp.com/rnd/products/wireless/420_series/summary.htm.

The access point must be configured to use the type of external antenna that is attached, either a diversity antenna that connects to both access point antenna connectors, or non-diversity antenna that has a single pigtail connection. A configuration setting for the antenna mode has been added to the **Port/Radio Settings** page of the web interface, and the command **antenna-mode** is available from the CLI.

When using an external antenna, the access point's transmit power may also need to be limited to conform to local regulations. Transmit Limit settings for low, middle, and high channels have been added to the **Port/Radio Settings** page of the web interface, and the command **transmit-limits** is available from the CLI.

Features in Release 2.0.41

A list of features supported in release 2.0.41 with system parameter default values is provided in the following table.

System Parameter Default Values in Release 2.0.41		
Feature	Parameter	Default Value
Identification		
	System Name	Enterprise AP
Administration		
	User Name	admin
	Password	[null]
	FTP User Name	[null]
	FTP password	[null]
General		
	IAPP	Enabled
	HTTP Server	Enabled
	HTTP Server Port	80
IP		
	DHCP	Enabled
	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	Primary DNS IP	0.0.0.0
	Secondary DNS IP	0.0.0.0
RADIUS (Primary and Secondary)		
	MAC Address Format	No Delimiter
	VLAN ID Format	Hex
	IP Address	0.0.0.0
	Port	1812
	Key	DEFAULT
	Timeout	5 seconds
	Retransmit	3

System Parameter Default Values in Release 2.0.41		
Feature	Parameter	Default Value
802.1X Authentication	Broadcast Key Refresh	0 minutes (disabled)
	Session Key Refresh	0 minutes (disabled)
	Reauthentication Refresh Rate	0 seconds (disabled)
MAC Authentication	MAC	Local MAC
	Authentication Session Timeout	0 seconds (disabled)
Local MAC Authentication	MAC Table Permission	Deny
Filter Control	Local Bridge	Disabled
	Local Management	Disabled
	Ethernet Type	Disabled
SNMP	Status	Enabled
	Location	[null]
	Contact	Contact
	Community (Read Only)	Public
	Community (Read/Write)	Private
	SNMPv3 Users	[null]
	SNMPv3 Trap Targets	[null]
	SNMPv3 Trap Filters	[null]
	Traps	All Enabled
	Trap Destination (1 to 4)	Disabled
	Trap Destination IP address	0.0.0.0
	Trap Destination Community Name	Public
System Logging	Syslog	Disabled
	Logging Host	Disabled

Features in Release 2.0.41

System Parameter Default Values in Release 2.0.41		
Feature	Parameter	Default Value
Ethernet Interface	Logging Console	Disabled
	IP Address / Host Name	0.0.0.0
	Logging Level	Error
	Logging Facility Type	16
Wireless Interface	Speed and Duplex	Auto
	SSID	Enterprise Wireless AP
	Radio Working Mode	b & g
	Antenna Mode	Diversity
	Channel	0
	Auto Channel Select	Enabled
	Transmit Power	Full
	Transmit Limits	100% (Low, Mid, and High channels)
	Data Rate	54 Mbps
	Multicast Data Rate	1 Mbps (b-only, b+g modes) 6 Mbps (g-only mode)
	Fragmentation Threshold	2346 bytes
	RTS Threshold	2347 bytes
	Beacon Interval	100 TUs
	DTIM Interval	2 beacons
	Maximum Association	128 stations
	Slot Time	Auto
	Preamble	Long
Wireless Security	Closed System	Disabled
	Security Wizard	No security
	802.11 Authentication	Open System
	802.1X	Disabled
	Encryption	Disabled

System Parameter Default Values in Release 2.0.41		
Feature	Parameter	Default Value
VLAN	WEP Cipher	WEP
	WEP Key Length	128 bit
	WEP Key Type	Hexadecimal
	WEP Transmit Key Number	1
	WEP Keys	[null]
	WPA Mode	Dynamic Key
	WPA Client	Disabled
	WPA Multicast Cipher	WEP
	WPA Unicast Cipher	TKIP
	WPA Pre-shared Key Type	Hexadecimal
	WPA Pre-shared Key	[null]
	VLAN Tag Support	Disabled
Native VLAN ID		1

Clarification of Operating Details for Certain Software Features

Operating Systems, Web Browsers, and Java Support

The operating systems, web browsers, and Java support required to manage the access point through the browser interface are incorrectly documented in the first editions of the *Installation and Getting Started Guide* and *Management and Configuration Guide*. The correct system support for software release 2.0.41 is provided in the following table:

Operating System	Internet Explorer	Netscape	Mozilla	Mozilla Firefox	Java
Windows 2000 Professional	5.0 ¹	7.0 ² 7.1 ²	1.7.3 ²	1.0PR ²	¹ Microsoft Java Virtual Machine 5.00.3810. ² Sun Java 2 Runtime Environment Standard Edition v1.4.1 and v1.4.2
Windows 2000 Professional SP4	5.0 ^{1,2}	7.0 ² 7.1 ²	1.7.3 ²	1.0PR ²	
Windows 2000 Server SP4	5.0 ^{1,2}	7.0 ² 7.1 ²		1.0PR ²	
Windows XP Professional version 2002 SP1	6.0 ^{1,2}	7.0 ² 7.1 ²	1.7.3 ²	1.0PR ²	
Windows XP Professional version 2002 SP2	6.0 ^{1,2}	7.0 ² 7.1 ²	1.7.3 ²	1.0PR ²	
Windows 2003 Server	6.0 ^{1,2}	7.0 ² 7.1 ²	1.7.3 ²	1.0PR ²	
Mac OS 9.2		7.0			Sun Java 2 Runtime Environment Standard Edition v1.4.2
Mac OS X 10.3.5	5.2				
Linux kernel 2.4.18.44			1.0.1		

Note

When using Windows XP, the browser's cookies and temporary files may have to be cleared so that the access point can show the most recent configuration settings through the web user interface.

Configuring Encryption and MAC Authentication

The following tables provide additional information and clarification for configuring encryption and MAC authentication on the access point.

Configuring Encryption in the HP ProCurve Wireless Access Point 420			
Encryption Methods and Process	CLI Privilege Level and Commands***	Additional Requirements	Notes
No Security 1. Configure Security Suite wizard option 1	Context Configuration Level HP420(if-wireless g)#security-suite 1		
WEP Static ONLY 1. Define MAC authentication method 2. Configure Security Suite wizard option 2 (encryption only) or as shared-key (includes authentication) 3. Configure key length 4. Configure key index 5. Configure key	Global Configuration Level HP420(config)#mac-authentication server remote** OR HP420(config)#mac-authentication server local OR HP420(config)#no mac-authentication server Context Configuration Level HP420(if-wireless g)#security-suite 2 OR HP420(if-wireless g)#security-suite shared-key HP420(if-wireless g)#key-length-wep <64 128 152> HP420(if-wireless g)#transmit-key-wep <1 2 3 4> HP420(if-wireless g)#wep-key <1 2 3 4> <ASCII HEX> <key>	WEP supported client required.	Requires manual key management. Encryption index, length and type configured in the access point must match those configured in the clients.
WPA Pre-shared Key ONLY 1. Define MAC authentication method 2. Configure Security Suite wizard option 3 (AES cipher) or 4 (TKIP cipher) 3. Configure key	Global Configuration Level HP420(config)#mac-authentication server local OR HP420(config)#no mac-authentication server Context Configuration Level HP420(if-wireless g)#security-suite <3 4> HP420(if-wireless g)#wpa-preskared-key <ASCII HEX> <preskared key>	WPA supported client required.	Requires manual key management.
WEP Dynamic ONLY 1. Define MAC authentication method 2. Configure RADIUS server* 3. Configure Security Suite wizard option 5	Global Configuration Level HP420(config)#mac-authentication server local OR HP420(config)#no mac-authentication server HP420(config)#radius-server address <RADIUS server IP address> HP420(config)#radius-server key <RADIUS server shared secret> Context Configuration Level HP420(if-wireless g)#security-suite 5	RADIUS server required. 802.1X supplicant required. WEP supported client required.	

Clarification of Operating Details for Certain Software Features

Configuring Encryption in the HP ProCurve Wireless Access Point 420			
Encryption Methods and Process	CLI Privilege Level and Commands***	Additional Requirements	Notes
WPA with 802.1X ONLY 1. Define MAC authentication method 2. Configure RADIUS server* 3. Configure Security Suite wizard option 6 (AES cipher) or 7 (TKIP cipher)	Global Configuration Level HP420(config)#mac-authentication server local OR HP420(config)#no mac-authentication server HP420(config)#radius-server address <RADIUS server IP address> HP420(config)#radius-server key <RADIUS server shared secret> Context Configuration Level HP420(if-wireless g)#security-suite <6 7>	RADIUS server required. 802.1X supplicant required. WPA supported client required.	

* The AP 420 supports the following Extensible Authentication Protocol (EAP) methods: MD5, TLS, TTLS and PEAP

** Please refer to the table "Configuring MAC Authentication in the HP ProCurve Wireless Access Point 420"

*** To start, the access point is in the factory default configuration.

Conventions used:

Vertical bars separate alternative, mutually exclusive elements (|).

Braces enclose required elements (< >).

Italics indicate variables for which the user must supply a value when executing the command.

Configuring MAC Authentication in the HP ProCurve Wireless Access Point 420							
MAC Authentication Mode	MAC Authentication	Local MAC Authentication	MAC Authentication Table			RADIUS	Comments
		MAC Table Permission	MAC Address	Permission			
				Active	Inactive		
Local MAC authentication	Local MAC	Deny	xx-xx-xx-xx-xx-xx	*		Not needed	All MAC addresses allowed unless entry set to active in the MAC Authentication Table. Can be combined with other methods for improved security.
Local MAC authentication	Local MAC	Allow	xx-xx-xx-xx-xx-xx	*		Not needed	All MAC addresses denied unless entry set to active in MAC Authentication Table. Can be combined with other methods for improved security.

Configuring MAC Authentication in the HP ProCurve Wireless Access Point 420							
MAC Authentication Mode	MAC Authentication	Local MAC Authentication	MAC Authentication Table			RADIUS	Comments
		MAC Table Permission	MAC Address	Permission			
				Active	Inactive		
Remote MAC authentication	Radius MAC	MAC address permission policy based on RADIUS server configuration.	RADIUS Server Use PAP authentication and enter MAC address as specified by the Radius MAC Address Format. User and password on the RADIUS server must be the same.			MUST	Works with static and dynamic WEP keys. Does not work with WPA with 802.1X or WPA-PSK.

Maximum Number of Associated Clients

The maximum number of 802.11b/802.11g clients that can associate simultaneously to the HP ProCurve Wireless Access Point 420 is 128.

Software Fixes

Release 2.0.41

Problems Resolved in Release 2.0.41

- **System** — The access point reboots when beacon frames have not been transmitted for more than 40 seconds due to RF pollution. (18-00929)

(For v2.0.41 software, the access point does not reboot. Event log messages are generated when beacon frames have not been transmitted for 20 seconds and continue once every minute until the RF pollution is cleared.)

Release 2.0.40

Problems Resolved in Release 2.0.40

- **CLI/Web** — Using the web interface Security Suite page, a static WEP encryption key value is not saved properly. To work around the problem, use the CLI to set static keys. (18-00616)
- **CLI/Web** — In the CLI the Local MAC authentication list shows the status as “AVTIVE” rather than “ACTIVE.” (18-00820)
- **System** — Clients cannot associate when using 64-bit static WEP. (18-00821)
- **Interoperability** — Using an HP IPAQ handheld PC as a client causes the access point to reboot. (18-00822)
- **Radio** — When using channels 9, 10, or 11, the console shows an error message and the access point shuts down the wireless interface. (18-00830)

Release 2.0.39

Problems Resolved in Release 2.0.39

- **System** — The radio is disabled on power-up with a blank configuration file to mitigate the following issues:
 - For v2.0.37 or earlier software: The access point may continuously reboot until the RF pollution is cleared.

- For v2.0.38 software: The radio interface shuts down and an `hpdot11InterfaceFailure` trap is sent to SNMP hosts and targets (if the trap is enabled and the hosts and targets are configured). Note that if the `hpdot11InterfaceFailure` trap is not received by a management station, the behavior of the radio interface may not be noticed.

To prevent environment RF pollution, avoid booting access points that are placed close together, within 2 m (6 ft), such as when performing a test. Also, avoid close proximity to other sources of RF pollution, such as cordless phones, microwave ovens, and Bluetooth devices. (18-00404, 1000191739)

(For v2.0.39 software, the radio is now enabled on power-on. If the channel is not clear due to a polluted RF environment, the radio will disable automatically and an appropriate entry made in the event log.)

- **System** — Antenna configuration lost after rebooting. The **show interface wireless g** command displays the correct configuration, but the antenna mode always operates as “diversity” after a reboot even if it was previously set to “single.” (18-00627)
- **Interoperability** — Broadcom-based wireless clients, such as those included with some HP notebook PCs, fail to associate to the AP 420. (18-00626)

Release 2.0.38

Problems Resolved in Release 2.0.38

- **Management** — The AP 420 with 2.0.38 software can now be managed by AirWave Management Platform (AMP) 3.0.6 and above.
- **CLI/Web** — When using the CLI to reboot the access point, the **reset board** command does not work if the command is typed using upper case characters, such as “**reset Board**,” or “**RESET BOARD**.” (18-00120, 18-00381)
- **CLI/Web** — In the web interface, an error message is not displayed when invalid characters are entered in the Native VLAN ID text field. (18-00158)
- **CLI/Web** — In the web interface, the error message for the SNTP Server configuration for minutes incorrectly shows “Month.” (18-00162)
- **CLI/Web** — In the CLI there is no enable/disable status displayed for the **show interface ethernet** command. (18-00194)
- **CLI/Web** — In the web interface Port/Radio Settings page, when the radio is set to “g only” mode, the Maximum Station Data Rate can still be set to 1, 2, 5.5, 11 Mbps. (18-00215)
- **CLI/Web** — Using the CLI interface the Radius server name must be specified as an IP address and not a host name string. The web interface does not have this problem. (18-00226)

- **CLI/Web** — Using the CLI interface, the **snmp-server daylight-saving** command accepts values for day and month that are a mixture of integer numbers and alphabetic letters. (18-00227)
- **CLI/Web** — Using the CLI interface, invalid IP addresses can be entered for an SNMP server IP (primary or secondary). (18-00228, 18-00273)
- **CLI/Web** — Using the CLI interface, no error message is displayed when invalid IP addresses are entered for a DNS server IP (primary or secondary), even though the new value is not set. (18-00230, 18-00275)
- **CLI/Web** — The CLI interface does not accept a WPA Pre-Shared Key value with space characters. (18-00251, 18-00287)
- **CLI/Web** — The **snmp-server host** command in the CLI interface accepts invalid IP addresses and if the SNMP community is specified using more than 23 characters, this overwrites the host IP address. (18-00256)
- **CLI/Web** — In the CLI interface the **show interface ethernet** command always displays the Admin Status of the Ethernet interface as “Up,” even when the interface has been shutdown. (18-00257)
- **CLI/Web** — The CLI command **transmit-power** does not accept any setting using upper case letters (for example, “FULL” instead of “full”). (18-00267)
- **CLI/Web** — Using the CLI interface, invalid IP addresses and host name characters (for example, @#%^&) can entered for a logging host IP or host name address. (18-00229, 18-00274)
- **CLI/Web** — When the Country Code is not set (the default is 99), the web interface **Port/Radio Settings** page shows an error message and the Maximum Station Data Rates in the drop-down menu are not completely displayed. (18-00288)
- **CLI/Web** — When using the web interface to upgrade software via TFTP, if a wrong file name is specified or any user name and password, the access point reboots. (18-00321, 18-00322)
- **CLI/Web** — In the web interface, the Native VLAN ID text field accepts out-of-range values and invalid characters. The Native VLAN ID is limited to between 1 and 64. (18-00522)
- **SNMP** — Using SNMP management tools, the SNMP Server Location (sysLocation of system Group) cannot accept up to 255 characters. (18-00027)
- **SNMP** — When using SNMP management tools, the maximum wireless data transmission rate (hpdot11OperationalRateSet of enterpriseAPdot11 Group) cannot be set to a new value. (18-00057)
- **SNMP** — The hpdot11WEPDefaultKey11gLength of dot11smt Group can accept the wrong value. (18-00144)

- **SNMP** — The `hpdot11WEPDefaultKey11gValue` of `dot11smt` Group can accept the wrong string length. (18-00145)
- **SNMP** — Using SNMP or the CLI interface, the SNMP Server Contact does not show its data value correctly if the input value is longer than 39 characters. It is recommended to limit the input value to less than 39 characters. (18-00204, 18-00222, 18-00312)
- **SNMP** — Using SNMP management tools, the SNMP Server Location (`sysLocation` of `system` Group) does not show its data value correctly in the CLI if the input value is longer than 40 characters. It is recommended to limit the input value to less than 40 characters. (18-00206, 18-00313)
- **SNMP** — If an SNMP management tool is used to set the Country Code (`swCountry` of `enterpriseApSys` Group), the CLI displays various text that does not effect the AP settings. (18-00258)
- **SNMP** — Using SNMP management tools, the access point IP address (`netConfigIPAddress` of `enterpriseApIpMgt` Group) can be set to an invalid address. (18-00259)
- **SNMP** — Using SNMP management tools, the gateway IP address (`netDefaultGateway` of `enterpriseApIpMgt` Group) can be set to an invalid address. (18-00260)
- **SNMP** — The WEP key length (`dot11WEPKeyMappingLength` of `hpdot11PrivacyTable` Group) cannot be set using SNMP management tools. (18-00261)
- **SNMP** — Using SNMP management tools, RADIUS server IP addresses (`hpdot11AuthenticationServer` of `hpdot11AuthenticationTable`) can be set to an invalid IP Address. (18-00262)
- **SNMP** — Using SNMP management tools, the Country Code (`swCountry` of `enterpriseApSys` Group) does not show an error when it has already been set (it is allowed to be set only once). (18-00293)
- **SNMP** — Using SNMP management tools, the server IP address (`fileServer` of `enterpriseApFileTransferMgt` Group) can be set to an invalid address. (18-00295)
- **SNMP** — The `portspeedDpxstatus` (OID: 1.3.6.1.4.1.11.2.3.7.11.37.3.1.1.8) always shows “half Duplex 10” even when the value is changed. (18-00332)
- **SNMP** — The `portflowCtlstatus` (OID: 1.3.6.1.4.1.11.2.3.7.11.37.3.1.1.9) always shows “none” even when a connected switch enables flow control. (18-00333)
- **SNMP** — The `resetOpCodefile` (OID: 1.3.6.1.4.1.11.2.3.7.11.37.5.1) does not check if a file name already exists, it always accepts the entered value. (18-00334)
- **SNMP** — The tree sequence is wrong for `hpdot11WepDefaultKey11gEntry` (OID: 1.3.6.1.4.1.11.2.3.7.11.37.7.8.1.1.1). (18-00338)

Software Fixes

- **SNMP** — When using SNMP management tools to download new software, invalid code files (not hp-img.bin) are not rejected by the access point. (18-00407)
- **TFTP** — If using the CLI **copy tftp file** command and an invalid software code file or TFTP server IP is specified, the current software code file is deleted before the operation fails. Note that the “dflt-image” file is not deleted. (18-00231)
- **Encryption** — When using WPA Pre-Shared Key mode with some clients that employ power saving states, the client cannot connect to the access point. This is a compatibility issue with the client network card and can be solved by disabling power saving on the client. (18-00272)
- **Radio** — Regardless of the speed selected via the user interfaces, the access point will always transmit at the maximum speed rate (11 Mbps for 802.11b and 54 Mbps for 802.11g). (18-00271, 18-00387)
- **System** — After heavy traffic and more than 20 hours of operation, client stations cannot associate to the access point until it is rebooted. (18-00391)
- **System** — When the multicast streaming rate is higher than the multicast-data rate set on the access point, clients lose association for some minutes. (18-00392, 18-00396)
- **System** — The multicast data rate must be set to 1 Mbps in order to operate properly with Agere based radios. (18-00412)
- **System** — The access point only allows MAC addresses on a RADIUS server to be in a continuous string format. (18-00413)
- **System Log** — The System Log does not show an entry when the 802.11g radio channel is changed to “auto.” (18-00209, 18-00277)

Release 2.0.37

Problems Resolved in Release 2.0.37

- **CLI/Web** — Using the web interface, the status of client stations on the Station Status page is not refreshed until the web interface is re-opened. (18-00213)
- **CLI/Web** — The CLI command **max-association?** displays the accepted value range as 0 - 2007, but the maximum valid value is 128. (18-00266, 18-00325)
- **CLI/Web** — When using the CLI **speed** command with the access point set to “b only” mode, the 11 Mbps option is missing. (18-00368)
- **Encryption** — In WPA Dynamic Key mode, there is no broadcast key packet after the refresh rate has expired. (18-00340)
- **Encryption** — In WPA Pre-shared Key mode, there is no broadcast key packet after the refresh rate has expired. (18-00341)

Release 2.0.34

Problems Resolved in Release 2.0.34

- **CLI/Web** — Sun Java support added to the web user interface.
- **Radio** — Interoperability issues caused by invalid packets.
- **Encryption** — Two WPA clients fail to ping each other when the multicast cipher is set to “WEP”. Using WEP as the multicast cipher results in WPA clients not being able to communicate with WEP clients. (18-00221)

Release 2.0.29

Release 2.0.29 was the first software release for the HP ProCurve Wireless Access Point 420.

Known Software Issues and Limitations

The following sections contain limitations and known software problems in Release 2.0.41 for the HP ProCurve Wireless Access Point 420.

Limitations

- The time stamp of the event log starts from Jan 01 00:00:00 if the AP is not connected to a time server.
- A client that links at 1 or 2 Mbps RX/TX rate will degrade performance if the client card's power saving is enabled.
- When roaming, there may be some authentication or re-authentication issues with Cisco and Nortel wireless network cards.
- The CLI **show system** command does not show the MAC of the WLAN interface.
- The access point does not support RADIUS MAC Authentication for WPA-PSK clients.
- The access point may not pass unicast traffic in a multicast overloading scenario, where the multicast data rate from the traffic source exceeds the multicast data rate set on the access point. To mitigate this problem, it is recommended to set the multicast data rate in the access point to the maximum value of 11 Mbps.
- When VLAN support is enabled or disabled on the access point, or the native VLAN ID changed, the system requires a reboot.

- The parameters for the primary and secondary RADIUS server IP address do not accept a host name. The IP addresses must be specified.

Software Problems

- **CLI/Web** — The CLI limits the configuration of password length up to 10 characters, but the Web UI limits it to 16 characters. It is recommended to only configure the password up to 10 characters.
- **CLI/Web** — The access point displays the incorrect Station Status for clients that fail 802.1X authentication. The status is displayed as “True” when it should be displayed as “Fail.” (18-00116)
- **CLI/Web** — When using the CLI to reset the access point defaults, the **reset configuration** command does not work if the command is typed using upper case characters, such as “**reset Configuration**,” or “**RESET CONFIGURATION**.” (18-00121, 18-00380)
- **CLI/Web** — When using the web interface SNMP page, the “Apply Changes” button does not work unless a valid Trap Destination IP Address is specified. (18-00219)
- **CLI/Web** — Using the CLI interface, the SNMP Server Location does not show its data value correctly if the input value is longer than 79 characters. It is recommended to limit the input value to less than 79 characters. (18-00223)
- **CLI/Web** — In the CLI interface the **show interface ethernet** command always displays the Operational Status of the Ethernet interface as “Up,” even if the cable is removed from the access point’s RJ-45 port. (18-00233, 18-00299, 18-00302)
- **CLI/Web** — In the web interface, when using an SNTP server and enabling Daylight Saving, the start time is always set as 00:00 AM. The start time should be set as 02:00 AM for United States and 01:00 AM for the European Union. (18-00236)
- **CLI/Web** — The access point does not update the new settings of **speed-duplex** command. (18-00339)
- **CLI/Web** — Using the Web interface, any port setting changes made in the Port Settings page does not update in Status page. (18-00346)
- **CLI/Web** — When using the CLI, the WPA-PSK key length cannot be set to 13, 14, 15, 17, 18, 19, 21,...,4n+1, 4n+2, 4n+3,..., 63 characters. (18-00393)
- **CLI/Web** — The access point’s wireless MAC address is not displayed in either the CLI or Web interface. (18-00409)
- **CLI/Web** — When using the Web interface with Netscape 7.0 or Linux Netscape, the Software Upgrade page Reset and Reboot buttons do not work. (18-00422)

- **CLI/Web** — When using the Web interface with Linux Netscape, if the Port Setting is set to “10Base-T Full Duplex” in the Port/Radio Settings page, the Web interface fails. (18-00423)
- **CLI/Web** — The CLI command **snmp-server trap** only allows each SNMP trap to be enabled or disabled individually, there is no argument to enable or disable “all” with one command. (18-00489)
- **CLI/Web** — Using the web interface MAC Authentication page, new MAC addresses added to the Local MAC Authentication Table are not verified. (18-00514)
- **CLI/Web** — The CLI **show station** command does not display the correct VLAN assignment for associated clients. (18-00547)
- **CLI/Web** — In the web interface SNMP Traps page, the trap filter OID details are not displayed in the filters list. (18-00560)
- **CLI/Web** — When the access point Ethernet port is set to autonegotiation, the setting is not displayed in the web, CLI, or SNMP interface. (18-00563)
- **CLI/Web** — Using the web interface, an “empty” error message is displayed when a non-existing SNMP user ID is entered for an SNMP Target ID. (18-00571)
- **CLI/Web** — Using the CLI or web interface, a client station’s Key Type is listed incorrectly as “Dynamic WEP” when connected via WPA-PSK. (18-00591, 1000196985)
- **CLI/Web** — Using the Internet Explorer web browser for MAC OS, the Apply and Clear buttons do not show the text “Apply” and “Clear.” (18-00620)
- **CLI/Web** — Using the Netscape 7.0 web browser on Windows XP-SP2, the access point does not reboot when using “reboot access point” or “reset to factory defaults.” (18-00621)
- **CLI/Web** — Using the Mozilla Firefox web browser for MAC OS, the Java applet will not open even though the Sun Java Runtime Environment is already installed. (18-00622)
- **CLI/Web** — The CLI **show interface wireless** command incorrectly displays WPA security parameters when set to no security after a previous security configuration. (1000199414)
- **CLI/Web** — Using the web interface it is not possible to set the basic SNMP parameters, Location, Contact, and Community Names, due to an error concerning the length of the Engine ID. To work around the problem, either set the Engine ID to 30 characters or use the CLI to set the basic SNMP parameters. (1000199705)
- **CLI/Web** — Using the web interface, a user name of an incorrect length is accepted, but the value is not saved. (18-00827)
- **CLI/Web** — Using the web interface, a password of more than 16 characters is accepted, but only 16 of the characters are saved. (18-00828)
- **CLI/Web** — Using the web interface, user names and passwords are accepted that contain printable characters (" and : and space). (18-00829)

Known Software Issues and Limitations

- **CLI/Web** — Using the web interface, Closed-System can be enabled but not disabled. To work around the problem, use the CLI to disable Closed-System. (18-00831)
- **CLI/Web** — Using Telnet to change the CLI prompt fails. To work around the problem, use a console connection to set the CLI prompt. (18-00964)
- **SNMP** — When using SNMP management tools, the System Name (sysName of system Group) does not show its data value correctly in the CLI if the input value is longer than 39 characters. It is recommended to limit the input value to less than 39 characters. (18-00205)
- **SNMP** — The object portOperStatus (OID: 1.3.6.1.4.1.11.2.3.7.11.37.3.1.1.10) cannot save a new setting. (18-00444)
- **SNMP** — When using SNMP management tools, the administrator password (enterpriseAdminPassword) cannot be set to a null value. (18-00449)
- **SNMP** — The access point still sends trap messages even when the snmpEnableAuthenTraps object is set to disabled. (18-00457)
- **SNMP** — When more than 20 SNMP trap filters are configured, the access point reboots or displays a weird message. (18-00567)
- **SNMP** — When the authentication key and privacy key of a current SNMPv3 user is changed using the SNMP object under usmUserEntry, the user cannot gain access using the new values. (18-00607)
- **SNMP** — SNMPv3 traps do not include correct client MAC address information. To work around the problem, use SNMPv2 traps. (18-00617)
- **SNMP** — The SNMP Engine ID should take up to 32 characters, but it can only take up to 30 characters. (1000191965)
- **SNMP** — All SNMP traps, except dot11stationassociation, are set to disable after upgrading software to v2.0.38 from v2.0.34 or v2.0.37. (1000196995)
- **Encryption** — Using the web interface, the WPA Pre-shared Key can be set to a “blank” value if the Apply Changes button is pressed more than once. (18-00220)
- **Encryption** — When a client using static WEP shared keys is associated with an access point set to 802.1X Supported and then the setting is changed to 802.1X Required, the client remains connected to the network even after the 802.1X reauthentication timeout. It is highly recommended to reboot the access point after changing to 802.1X Required to force all clients to reauthenticate. (18-00249)
- **Encryption** — When set to WPA-supported mode, Agere clients using WEP encryption cannot associate with the access point. (18-00401)
- **Encryption** — AES encryption is not working with Linksys 54G clients. (18-00402)

- **Encryption** — The access point does not accept a hexadecimal WEP key with 2 or more leading zeros. (18-00415)
- **Radio** — The “auto” radio channel scan does not find the least busy channel. It is recommended to manually set the channels of all local access points. (18-00237)
- **Radio** — When a client roams between two access points and IAPP fails, the Station Status (Forwarding Allowed) is displayed as “True” even though the client cannot connect to the network. (18-00246)
- **Ethernet Interface** — When DHCP is disabled and a static IP address set, then the access point quickly rebooted, the IP setting is lost and the default IP is used. (18-00588)
- **System Log** — In the case of an 802.1X authentication failure, the event is logged as “authenticated” instead of “authentication failure.” (18-00427)
- **System Log** — When using security suite 2, the access point does not send client associated/authenticated log messages to the console, web interface, or trap receivers. (18-00619)
- **System Log** — The log message for the “short or long” preamble setting is shown incorrectly as “short.” (1000201205)
- **System Time** — When SNTP is disabled and the system time manually set to “23: 59, Dec 31th, 2100,” after 1 minute the time becomes “00:00, Dec 32th, 2100.” (18-00825)
- **Roaming** — When an 802.1X authenticated client roams between two access points using IAPP, if 802.1X reauthentication fails, the AP reports that the client is authenticated and associated. Still, forwarding traffic is not allowed given the unsuccessful authentication. (18-00247)
- **RADIUS** — During 802.1X authentication, the access point uses the wireless MAC address instead of the Ethernet MAC address for the RADIUS attribute “NAS address” as given in RFC 3580. (18-00428)
- **System** — A Chariot test with multicast traffic set to “unlimited send_data_rate” does not finish and shows an error message. (18-00424)
- **System** — When HTTP is disabled, the user can not upgrade the runtime code. (18-00597)
- **System** — When the access point management access filter is disabled, the access point cannot ping wireless clients. (18-00598)
- **System** — The access point reboots automatically when clients using different encryption ciphers are connected. (18-00823, 18-00832)
- **System** — The CLI displays a large number of error messages when different encryption clients are connected for a long time. (18-00824)
- **System** — System reboots after 16 hours of stress test turning off the power LED and continually repeating the SDRAM test. (18-00836)

Known Software Issues and Limitations

- **Interoperability** — When using Buffalo WLI-CB-G54A and Microsoft MN-720 client cards, the 802.11g performance of the access point is below 1 Mbps when stations are in power saving mode. (18-00581)
- **Interoperability** — When using Netgear WG511 client cards, the 802.11g performance of the access point is below 7 Mbps when stations are in power saving mode. (18-00582)



© Copyright 2001, 2005 Hewlett-Packard Company, LP. The information contained herein is subject to change without notice.

May 2005
Manual Part Number
5990-6007