Release Notes: Version 2.1.3

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 2)
- Features in release 2.1.3 (page 12)
- Clarification of Operating Details for Certain Software Features (page 16)
- Software fixes (page 17)
- Known software issues and limitations (page 26)

Please note:

Software release 2.1.0 was a major update that included many new features and feature enhancements. This release obsoletes most of the limitations and software issues found in previous releases and they are no longer documented in these release notes. All the issues listed in "Known Software Issues and Limitations" on page 16 concern the version 2.1.x software releases only.

Important Software Update Notice

Updating to version 2.1.x software from 2.0.x software versions requires a special procedure that is different from a normal update. Be sure to follow the procedure provided in "Update Procedure from v2.0.x to v2.1.x Software" on page 2.

© Copyright 2003, 2006 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
February 2006

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 Software and Documentation from the Web 1

Downloading Software to the Access Point 1

Update Procedure from v2.0.x to v2.1.x Software 2
- Version 2.1.x Software Update using TFTP/FTP 3

Update Procedure for v2.1.x Software 6
- TFTP Download from a Server 6

New Features

New Features in Release 2.1.3 9
- Dynamic VLAN Assignment for MAC Authentication Clients 9
- De-authentication of Clients Through SNMP 9
- Improved Roaming Performance 9

New Features in Release 2.1.2 9
- Broadcast/Multicast Limit 10
- Pure 802.11g Mode 10

New Features in Release 2.1.1 12

New Features in Release 2.1.0 12
- Multiple SSID Interfaces 13
- Security Setting per SSID 13
- WPA2 Support 13
- Neighbor AP Detection 13
- Management Controls 13
- Manager and Operator Users 13
- Management VLAN 14
- RADIUS Accounting 14
- Secure Shell 14
- Secure HTTP 14
- Readable Text Configuration Files 14
- 802.1X Supplicant 14
- SpectraLink Voice Priority 15

Clarifications

Maximum Number of Associated Clients 16
Web Browser Interface Refresh 16

Software Fixes

Release 2.1.3 17
Release 2.1.2 17
Release 2.1.1 19
Release 2.1.0 20
Release 2.0.41 20
Release 2.0.40 20
Release 2.0.39 20
Release 2.0.38 21
Release 2.0.37 24
Release 2.0.34 25
Release 2.0.29 25

Known Software Issues and Limitations

Limitations 26
Software Issues 26

Software Management

Downloading Access Point Software and Documentation from the Web

You can download software version 2.1.3 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

The software update procedure for the access point depends on the version of software that is currently running on your access point. If updating from v2.0.x software, a special procedure is required that is different from an update from v2.1.x software.

The software update file downloaded from HP's ProCurve Web site contains four files. All of these files are needed for an update from v2.0.x software. An update from v2.1.x software is a simpler process that requires only one of these files.

For access points already running software version v2.1.x software, follow the normal update procedure provided in "Update Procedure for v2.1.x Software" on page 6. To update to v2.1.x software from v2.0.x software, follow the exact procedure provided in "Update Procedure from v2.0.x to v2.1.x Software" on page 2.

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 **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 **HTTP** 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 updating 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 **hp420-2100.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.

Update Procedure from v2.0.x to v2.1.x Software

To update the access point software from v2.0.x to v2.1.x requires a special procedure that is different from a normal update. It is important to follow the exact procedure provided in this section to successfully download and run the v2.1.x software.

Due to the increased size of the v2.1.x runtime software file, the access point requires an update of both the boot code (**bootrom306.bin**) file and the default software (**dflt-img.bin**) file. Because the v2.0.x software does not allow software files of greater than 1.5 Mbytes to be downloaded or the default software file to be overwritten, a temporary software file must first be downloaded to facilitate the update.

Note

This update procedure is only for access points running software version v2.0.x. Access points already running software version v2.1.x or later do not require this procedure.

All the files required for the v2.1.x software update are available from the HP ProCurve Web site (http://www.hp.com/go/hpprocurve). The following table describes the files used in the update procedure.

Update File	Description
hp420-tempimg2.bin	The temporary software that is required to allow the access point to download software files larger than 1.5 Mbytes and update the default software file.
bootrom306.bin	The update boot code that is required for software image files larger than 1.5 Mbytes to load and run on the access point.
dflt-img.bin	The update default software that allows the access point to download software files larger than 1.5 Mbytes.
hp420-2130.bin	The update v2.1.x software.

Version 2.1.x Software Update using TFTP/FTP

Syntax: **copy tftp file**

The initial v2.0.x to v2.1.x software update can only be performed using the CLI, either through a direct console connection or Telnet, or using SNMP. The updating of the boot code cannot be performed using the Web interface.

Note the following points before starting the update procedure:

- Make sure the access point is running a v2.0.x software version.
- Place all the v2.1.x update files into the root directory of the TFTP/FTP server.
- Be sure there is a stable network connection to the access point. If the power to the access point or the network connection is lost, the update may fail and the access point be unable to boot.
- Where possible, use a 100 Mbps connection to the access point's Ethernet port.

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 updating 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.

To Update the Access Point to v2.1.x Software From v2.0.x Software:

1. Download the temporary software file, **hp420-tempimg.bin**.

```
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-tempimg2.bin
TFTP Server IP:192.168.1.10

Removing old runtime! Please wait a few minutes!

Creating file! Please wait a few minutes!
Firmware version of system is v2.0.38.0B037 and Updating Run-Time code
v02.00.40 NOW!
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#
```

2. After a successful download, the prompt "**Do you want to use NEW CONFIG SETTINGS? <y/n> [n]:**" appears. Type "**n**" to retain the current access point configuration. (Typing "**y**" restores factory default settings and reboots the access point.)
3. Reboot the access point.

```
HP420#reset board
Reboot system now? <y/n>: y
```

4. Download the update boot code file, **bootrom306.bin**.

```
HP420#copy tftp file
1. Application image
2. Config file
3. Boot block image
Select the type of download<1,2,3>:  [1]:3
TFTP Source file name:bootrom306.bin
TFTP Server IP:192.168.1.10
Updating Boot code v03.00.06 NOW!
HP420#
```

5. Download the update default software file, **dflt-img.bin**.

```
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:dflt-img.bin
TFTP Server IP:192.168.1.10
Firmware version of system is v2.0.40-temp and Updating Run-Time code
v02.01.00 NOW!

Creating file! Please wait a few minutes!
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 reset to FACTORY DEFAULT SETTINGS? <y/n> [n]:n
HP420#
```

6. After a successful download, the prompt "**Do you want to reset to FACTORY DEFAULT SETTINGS? <y/n> [n]:**" appears. Type "**n**" to retain the current access point configuration. (Typing "**y**" restores factory default settings and reboots the access point.)

7. Download the update v2.1.x software file, **hp420-2130.bin**.

```
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:hp420-2130.bin
TFTP Server IP:192.168.1.10

Removing old runtime! Please wait a few minutes!

Creating file! Please wait a few minutes!
Firmware version of system is v2.0.40-temp and Updating Run-Time code
v02.01.00 NOW!
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 reset to FACTORY DEFAULT SETTINGS? <y/n> [n]:n
HP420#
```

8. After a successful download, the prompt "**Do you want to reset to FACTORY DEFAULT SETTINGS? <y/n> [n]:**" appears. Type "**n**" to retain the current access point configuration. (Typing "**y**" restores factory default settings and reboots the access point.)
9. After all code files have been successfully downloaded, reboot the access point.

```
HP420#reset board
Reboot system now? <y/n>: y
```

Update Procedure for v2.1.x Software

TFTP Download from a Server

Syntax: **copy tftp file**

For example, to download a file named **hp420-2130.bin** from a TFTP server with the IP address of 10.1.0.9:

Note

Updating to version 2.1.x software from previous 2.0.x software versions requires a special procedure that is different from a normal update. Be sure to follow the procedure provided on page 2.

1. Execute the copy command as shown below:

```
HP420#copy tftp file
1. Application image
2. Config file
3. Boot block image
4. Text Config file
Select the type of download<1-4>:  [1]:1
TFTP Source file name:hp420-2130.bin
TFTP Server IP:10.1.0.9
Updating Boot Line in NVRAM, please wait!

Removing old runtime! Please wait a few minutes!

Creating file! Please wait a few minutes!
TFTP transfer succeeded!
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 reset to FACTORY DEFAULT SETTINGS? <y/n> [n]: n
HP420#dir
File Name                      Type   File Size(Bytes)
--------------------------     ----   ----------------
dflt-img.bin                     2        1109249
hp420-2130.bin                   2        1713472
syscfg                           5          41174
syscfg_bak                       5          41174
Boot Rom Version    : v3.0.6
Software Version    : v2.1.0.0

      131072 byte(s) available

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 reset to FACTORY DEFAULT 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.
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.

New Features

New Features in Release 2.1.3

The table below summarizes the new features in this release. The new features are described in detail in the sections following the table.

Feature	Summary
Dynamic VLAN Assignment for MAC Authentication Clients	See "Dynamic VLAN Assignment for MAC Authentication Clients" on this page.
Add SNMP OID for De-authentication of Clients	See "De-authentication of Clients Through SNMP" on this page.
Improved Roaming Performance	See "Improved Roaming Peformance" on this page.

Dynamic VLAN Assignment for MAC Authentication Clients

During remote MAC authentication with a RADIUS server, a VLAN can be assigned to successfully authenticated clients using RADIUS attributes.

De-authentication of Clients Through SNMP

An SNMP object ID has been created, enterpriseApSessionDeauthenticate, for de-authenticating clients using SNMP management tools.

Improved Roaming Performance

Software release 2.1.3 has improved the roaming performance connected 802.1X (WPA) clients by enabling a software retry feature in the wireless driver and reducing the 802.1X EAPOL authentication packet data rate.

New Features in Release 2.1.2

The table below summarizes the new features in this release. The new features are described in detail in the sections following the table.

Feature	Summary
Broadcast/Multicast Packet Limiting	See "Broadcast/Multicast Limit" on page 10.
Pure 11g Only Mode	See "Pure 802.11g Mode" on page 10.

Broadcast/Multicast Limit

The access point can become overloaded when multicast or broadcast traffic from the Ethernet port exceeds the configured multicast data rate. To avoid this condition, a broadcast/multicast traffic limiting function can be enabled on the Ethernet interface. When enabled, the function limits the multicast and broadcast traffic from the Ethernet port at a rate, based on the configured multicast data rate, that cannot overload the wireless interface.

Syntax: [no] bc-mc-limiting enable

For example, to enable broadcast/multicast traffic limiting:

```
HP420(if-ethernet)#bc-mc-limiting enable
```

To disable broadcast/multicast traffic limiting:

```
HP420(if-ethernet)#no bc-mc-limiting enable
```

To display the current broadcast/multicast limit setting, use the **show bc-mc-limit** command.

```
HP420#show bc-mc-limit

BroadcastLimiting Information
============================================================
Status:             Enable
No. of broadcast frames allowed: 17 frames per second
Broadcast frame discard count: 0
============================================================
HP420
```

Pure 802.11g Mode

Software release 2.1.2 supports a proprietary “pure 11g only” radio working mode for enhanced wireless performance. In this mode the access point only supports 802.11g clients at OFDM data rates without the use of the 802.11 “protection” mechanism that is employed when 802.11b devices are detected in the service area.

The following four four radio working modes are supported:

- **b & g mixed mode**: Both 802.11b and 802.11g clients can communicate with the access point. Supports unicast data rates of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps, and multicast data rates of 1, 2, 5.5, and 11 Mbps.
- **b only mode**: Both 802.11b and 802.11g clients can communicate with the access point, but 802.11g clients can only transfer data at 802.11b standard rates (up to 11 Mbps). Supports unicast data rates of 1, 2, 5.5, 11 Mbps, and multicast data rates of 1, 2, 5.5, and 11 Mbps.

- **g only mode**: Only 802.11g clients can communicate with the access point. Supports unicast data rates of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps, and multicast data rates of 6, 12, and 24 Mbps.
- **pure g only mode**: Only 802.11g clients can communicate with the access point. Supports unicast data rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps, and multicast data rates of 6, 12, and 24 Mbps.

Syntax: radio-mode <b | b+g | g | pure11g>

For example, to set the radio working mode to "pure 11g only":

```
HP420(if-wireless-g)#radio-mode pure11g
```

To display the current radio working mode setting, use the **show** command from the wireless interface level or the **show interface wireless g** command from the Exec level.

```
HP420(if-wireless-g)#show

Wireless Interface Common Information
================================================================================
----------------Identification----------------------------------------------
Description                    : Enterprise 802.11g Access Point
Radio mode                     : pure 802.11g only
Channel                        : 11
Supported SSID number          : 8
Supported Total Client number  : 128
Status                         : Disabled
----------------802.11 Parameters--------------------------------------
Transmit Power                 : FULL (17 dBm)
Max Station Data Rate          : 54Mbps
Multicast Data Rate            : 6Mbps
Fragmentation Threshold        : 2346 bytes
RTS Threshold                  : 2347 bytes
Beacon Interval                : 100 TUs
Authentication Timeout Interval : 60 Mins
Association Timeout Interval   : 30 Mins
DTIM Interval                  : 1 beacon
Preamble Length                : LONG
Slot time                      : AUTO
----------------Security----------------------------------------------------
Static Keys :
 Key 1: OPEN    Key 2: OPEN    Key 3: OPEN    Key 4: OPEN
```

```
---------------Antenna-------------------------------------------------
Antenna mode                    : Diversity
Antenna gain attenuation
            Low channel         : 100%
            Mid channel         : 100%
            High channel        : 100%
=============================================================================
HP420(if-wireless-g)#
```

New Features in Release 2.1.1

Software fixes only; no new features.

New Features in Release 2.1.0

The table below lists the new features in release 2.1.0. The features are summarized in the sections following the table. For a detailed description of all features, refer to the latest version of the *Management and Configuration Guide*.

Feature	Summary
Multiple SSID Interfaces	See "Multiple SSID Interfaces" on page 13.
Security Settings per SSID	See "Security Setting per SSID" on page 13.
WPA2 Support	See "WPA2 Support" on page 13.
Neighbor AP Detection	See "Neighbor AP Detection" on page 13.
Management Controls	See "Management Controls" on page 13.
Manager and Operator Users	See "Manager and Operator Users" on page 13.
Management VLAN	See "Management VLAN" on page 14.
RADIUS Accounting	See "RADIUS Accounting" on page 14.
Secure Shell	See "Secure Shell" on page 14.
Secure HTTP	See "Secure HTTP" on page 14.
Readable Text Configuration Files	See "Readable Text Configuration Files" on page 14.
802.1X Supplicant	See "802.1X Supplicant" on page 14.
SpectraLink Voice Priority	See "SpectraLink Voice Priority" on page 15.

Multiple SSID Interfaces

Software release 2.1.0 supports up to eight SSID interfaces. This allows traffic to be separated for different user groups using a single access point that services one area. For each SSID interface, different security settings, VLAN assignments, and other parameters can be applied.

The first SSID interface created on the access point is set as the primary. The primary SSID is the only SSID broadcast in the access point's beacon frames. You should set the SSID for the primary interface before creating secondary interfaces.

Security Setting per SSID

Wireless security can be set separately for each configured SSID interface. This includes WPA settings, 802.1X parameters, RADIUS authentication servers, and MAC address authentication.

Only one WEP key can be applied to an SSID interface, and only then if a key index is open. If there is no key index available, the SSID interface cannot use WEP security until a key index is released by another SSID interface.

WPA2 Support

Software release 2.1.0 includes support for WPA2 security. This includes Advanced Encryption Standard (AES) for robust data confidentiality, Mixed-Mode operation for networks migrating from WPA to WPA2, as well as key caching and preauthentication for fast roaming.

Neighbor AP Detection

The access point can scan all 2.4 GHz radio channels and find other access points within its neighborhood. A database of detected access points and their radio settings is maintained where any unauthorized access points can be identified.

The access point can be configured to scan periodically by setting the interval and scan duration. Alternatively, the access point can scan continuously in a dedicated mode with no clients supported.

Management Controls

To provide more security for the access point, management interfaces that are not required can be disabled. This includes the Web browser interface, Telnet, and Secure Shell (SSH) access, and also the serial console port and Reset button.

Manager and Operator Users

Management access to the access point's Web and CLI interface can be controlled through Manager and Operator user names and passwords. A Manager user name and password allows full read/write privileges for the Web and CLI. An Operator user name and password is restricted to read-only access for specified interfaces. A maximum of only two users can be configured, one Manager and one Operator.

Management VLAN

A management VLAN can be configured for secure management access to the access point. The management VLAN is for managing the access point through remote management tools, such as the Web interface, SSH, Telnet, or SNMP. The access point only accepts management traffic that is tagged with the specified management VLAN ID.

RADIUS Accounting

Software release 2.1.0 supports Remote Authentication Dial-in User Service (RADIUS) Accounting. RADIUS Accounting is an extension to the RADIUS authentication protocol that uses a central server to log user activity on the network. A RADIUS Accounting server runs software that receives user-session information from the access point. The data collected by the server not only provides the information for billing and auditing, but also allows network administrators to monitor usage trends and plan for network growth.

Secure Shell

The release 2.1.0 software supports a Secure Shell (SSH) version 2.0 server. SSH acts as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered. Clients can then securely use the local user name and password for access authentication.

Secure HTTP

The release 2.1.0 software now supports both a Web (HTTP) and secure Web (HTTPS) browser interface. The secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL) provides a secure encrypted connection to the access point's Web interface. Both the HTTP and HTTPS service can be enabled independently.

Readable Text Configuration Files

Software release 2.1.0 supports access point configuration files in a readable text format as well as a binary format. The readable text configuration files allow an administrator to modify an access point configuration using any text file editor. Both the binary and readable text configuration files can be copied to and from an FTP or TFTP server.

802.1X Supplicant

The access point can be enabled to operate as an 802.1X supplicant. This allows the access point itself to be authenticated by a RADIUS server using a configured user name and password.

SpectraLink Voice Priority

SpectraLink Voice Priority (SVP) is a mechanism for priortizing Voice over Internet Protocol (VoIP) traffic in wireless LANs. When SVP is enabled, the access point identifies SVP voice traffic and gives it a higher priority so that it can be transmitted before other data traffic. This mechanism ensures a timely delivery of voice traffic and good audio quality for VoIP telephony.

Clarifications

Maximum Number of Associated Clients

The maximum number of clients that can associate simultaneously to all of the access point's SSID interfaces is 128. However, due to the way the access point handles data encryption keys, the recommended maximum number is reduced depending on the security and VLAN configuration.

The following table indicates the recommended maximum number of associated clients for various security and VLAN confgurations. Exceeding the recommended maximum number of clients impacts the performance of the access point.

Data Encyption	VLAN Support	Recommended Maximum Number of Clients
WEP	No	124
	Yes	124
WPA (TKIP)	No	123
	Yes	124 - number of VLANs configured
WPA (AES)	No	123
	Yes	124 - number of VLANs configured

Web Browser Interface Refresh

To ensure proper screen refresh when using Internet Explorer with Windows XP, be sure that the browser options are configured as follows: Under the menu "Tools / Internet Options / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be set to "Automatically."

Software Fixes

Release 2.1.3

Problems Resolved in Release 2.1.3

- **CLI/Web** — All SNMP traps cannot be enabled or disabled with one CLI command. (18-01102)
- **CLI/Web** — The CLI help text for the speed-duplex command is incorrect for 100MF, describing it as "10Mbps/Full." (18-01152)
- **CLI/Web** — In the Web interface, browsing from the SNMP Trap page to the Port/Radio Settings page causes the access point to reboot. (18-01153)
- **CLI/Web** — In the Web interface, you cannot login if the length of the password equals 16 characters. (18-01154)
- **CLI/Web** — In the Web interface, a user name or password is not accepted when it contains the letter "v." (18-01162)
- **CLI/Web** — When the secure Web interface (HTTPS) is enabled and the HTTP server is disabled, the Java applet tabs at the top of the page do not load properly. (18-01163)
- **SNMP** — Using SNMP, the MAC filter permission state (deny/allow) is not consistent with the Web and CLI interface. (18-01155)
- **Authentication** — Clients may fail to authenticate with the access point during IAPP roaming when the 802.1X re-authentication or re-key is enabled. (18-01156)
- **Authentication** — SVP wireless telephones always start authentication with the access point when two parties begin a conversation causing voice interruption. (18-01158)
- **System** — In a text configuration file, the parameter SNTP timezone is changed after a file export and import. (18-01160)
- **System** — In a text configuration file, the RADIUS, WEP, and PSK key values are all lost after a downloaded text configuration file is uploaded to the access point. (18-01161)

Release 2.1.2

Problems Resolved in Release 2.1.2

- **CLI/Web** — The **show authentication** command still displays configured MAC addresses for SSID interfaces even when all SSID interfaces have been deleted. (18-00981)

- **CLI/Web** — When using the SNMP Web interface page, the options GroupName, AuthType, and Passphrase for an existing SNMPv3 user are not modified even though the message "Configuration has been saved!" is displayed. To work around the problem, use the CLI to modify an existing SNMPv3 user. (1000237325, 18-01042)
- **CLI/Web** — When using the Security Suite Web interface page, the error message "Invalid WEP key!" is displayed when the WEP key type (ASCII or HEX) is initially not specified, even though the key is valid. To work around the problem, either re-select or re-enter the key before clicking the Apply Changes button. (1000237585, 18-01043)
- **CLI/Web** — When using the Web interface to save a configuration file (either a binary or text file) to a TFTP server, the message "Configuration has been saved" appears when an invalid IP address has been specified. Only the CLI console displays an error message for an invalid IP address. (1000238780, 18-01067)
- **CLI/Web** — When using the Web interface, the Preamble length setting reverts to "Short or Long" if the Transmit Power setting is changed. (18-01139)
- **CLI/Web** — Logging into the Web interface multiple times causes a valid user name and password to be rejected. (18-01146)
- **CLI/Web** — The Web interface accepts printable characters (such as, ", :, and spaces) as the value of usernames and passwords, but the new values are not accepted for logging in. (18-01101)
- **CLI/Web** — The Web interface accepts user names of incorrrect length without an error message, but the values are not saved. (18-01115)
- **CLI/Web** — The Web interface accepts a user name of more than 16 characters without an error message, but saves only the first 16 characters of the name. (18-01116)
- **CLI/Web** — Using the CLI to add a MAC address entry to the MAC authentication table of an SSID interface and then trying to delete the entry, causes the system to fail. (18-01132)
- **CLI/Web** — Using the Web interface to add a MAC address entry to the MAC authentication table of an SSID interface and then trying to delete the entry, causes the Web interface not to refresh properly. (18-01133)
- **SNMP** — Saving a binary configuration file to a TFTP or FTP server using the object enterpriseApFileTransferMgt fails. Although the SNMP transfer indicates a success, the file on the TFTP or FTP server is zero bytes in size. (1000239011, 18-01068)
- **SNMP** — When SNMPv2 traps are disabled, SNMPv3 traps are also disabled. (18-01114)
- **Interoperability** — When using an Intel ProWLAN 2100 3B Mini PCI adapter card, a client cannot connect to the access point using 152-bit WEP HEX keys. (1000239808, 18-01070)

- **Authentication** — The access point 802.1X suplicant authentication fails when connected to a switch port configured for multiple client support. To work around the problem, configure the connected switch port for single client authentication only. (1000234170, 18-01018)
- **Authentication** — Wireless clients can still connect to the access point even when they are set to denied in the local MAC authentication table. (1000237612, 18-01046)
- **System** — The access point can experience wireless outages when the Ethernet port recieves too much broadcast traffic. The broadcast traffic is serviced before all other traffic, which gives the appearance of a loss of connectivity for wireless clients. (1000234336, 18-01021)
- **System** — Changing the management VLAN from untagged to tagged changes the tagging status of default VLAN of an SSID from untagged to tagged. (1000239014, 18-01058)
- **System** — When configuring the management VLAN as tagged, the system log messages report the VLAN as untagged. (1000238105, 18-01065)
- **System** — A text configuration file successfully uploaded to a TFTP server fails to download successfully to the access point. (18-01124)
- **System** — The access point default setting for the Preamble should be “Long,” not “Short or Long.” (18-01147)
- **SNTP** — The access point sets the SNTP server status to enabled after resetting to factory defaults. The SNTP server default status should be disabled. (18-01072)
- **SNTP** — The access point does not successfully update the system time by broadcasts from the SNTP server. (18-01073)
- **SNTP** — The access point does not include a configurable time update interval for time updates from an SNTP server. (18-01074)
- **Radio** — When multiple SSIDs are created and the primary SSID is not SSID #1, the access point does not enter into 11g protection mode. (18-01148)

Release 2.1.1

Problems Resolved in Release 2.1.1

- **Radio** — The wireless transmission output power is too low when the Antenna Mode is set to “Single.” (18-01129)
- **CLI/Web** — The model number shown in the Web interface is incorrect. The North American model should be J8130A and the World Wide Model should be J8131A. (18-01137)

- **System** — The access point system hangs after running for a few hours when Radius Accounting is enabled and many clients are associated. (18-01138)

Release 2.1.0

Release 2.1.0 is a major software release for the HP ProCurve Wireless Access Point 420 that obsoletes software issues from previous releases.

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 **sntp-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 SNTP 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 update 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)

- **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 2.1.3 for the HP ProCurve Wireless Access Point 420.

Limitations

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

Software Issues

- **Interoperability** — When using Cisco 350 Series client cards, the unicast throughput of the access point is below 5 Mbps with power saving mode enabled or disabled. (18-00839)
- **Interoperability** — When using a Netgear MA111v.1 USB wireless adapter, the unicast throughput of the access point is less than 1.5 Mbps. (1000234762, 18-01023)
- **Interoperability** — When using a D-Link DWL-AG650 client card and WPA-PSK AES security, connectivity with the access point is lost. (1000234764, 18-01024)
- **Interoperability** — When using a Linksys WUSB54Gv2 USB wireless adapter, the maximum unicast throughput of the access point in any mode is around 3.6 Mbps. (1000234766, 18-01025)
- **Radio** — When set to pure 11g mode, wireless clients can still connect to the access point using data rates 1, 2, 5.5, and 11 Mbps. (18-01126)
- **System** — When broadcast/multicast filtering is enabled for the Ethernet port, the data thoughput of the access point is reduced by 30-40% due to the filtering being performed by software. (18-01134, 18-01135)
- **Authentication** — When using WPA2 over 802.1X with the radio set to b-only mode, wireless clients re-associating with the access point perform full 802.1X authentication instead of using cached Pairwise Master Keys. (18-01136)
- **Authentication** —WPA auto-negotiation (security suites 8 and 9, for mixed use of TKIP/AES security) does not work for client stations using WPA/AES.

© Copyright 2003, 2006 Hewlett-Packard Company, LP. The information contained herein is subject to change without notice.

February 2006
Part Number
5990-6007