Release Notes: Version 2.0.37

for the HP ProCurve Wireless Access Point 420

These release notes include information on the following:

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).

Publication Number

5990-6007
May 2004
Edition 3

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

— This page is intentionally unused. —

Software Management

Downloading Access Point Documentation and Software from the Web

You can download software version 2.0.37 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 **hp420-2037.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.

TFTP Download from a Server

Syntax: **copy tftp file**

For example, to download a file named **hp420-2037.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:hp420-2037.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 v2.0.37
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 2.0.37

Features in Release 2.0.37

Adds 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.

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)		
	IP/Host Name	0.0.0.0
	Port	1812
	Key	DEFAULT
	Timeout	5 seconds
	Retransmit	3
MAC Authentication		
	MAC	Local MAC
	Authentication Session Timeout	0 seconds (disabled)
Local MAC Authentication		
	System Default	Allowed
	Permission	Allowed

Feature	Parameter	Default Value
802.1x Authentication		
	802.1x Status	Disabled
	Broadcast Key Refresh	0 minutes (disabled)
	Session Key Refresh	0 minutes (disabled)
	RADIUS Session Timeout	0 seconds (disabled)
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
	Traps	Enabled
	Trap Receiver IP/Host Name	[*null*]
	Trap Receiver Community	Public
System Logging		
	Syslog	Disabled
	Logging Host	Disabled
	Logging Console	Disabled
	IP Address / Host Name	0.0.0.0
	Logging Level	Error
	Logging Facility Type	16
Ethernet Interface		
	Speed and Duplex	Auto
Wireless Interface		
	SSID	Enterprise Wireless AP
	Radio Working Mode	b & g

Feature	Parameter	Default Value
	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	5.5 Mbps
	Fragmentation Threshold	2346 bytes
	RTS Threshold	2347 bytes
	Beacon Interval	100 TUs
	DTIM Interval	2 beacons
	Maximum Association	128 stations
Wireless Security		
	Closed System	Disabled
	Authentication Type	Open System
	WPA Mode	Dynamic Key
	WPA Client	Supported
	Multicast Cipher	WEP
	Unicast Cipher	TKIP
	WEP Encryption	Disabled
	WEP Key Length	128 bit
	WEP Key Type	Hexadecimal
	WEP Transmit Key Number	1
	WEP Keys	[*null*]
VLAN		
	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 2.0.37 is provided in the following table:

Operating System	Internet Explorer	Netscape	Other Browser	Java
Windows 2000 Professional	5.0[1]	7.0[2] 7.1[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]		
Windows 2000 Server SP4	5.0[1, 2]	7.0[2] 7.1[2]		
Windows XP Professional version 2002 SP1	6.0[1, 2]	7.0[2] 7.1[2]		
Windows 2003 Server	6.0[1, 2]	7.0[2] 7.1[2]		
Mac OS 9.2		7.0		Sun Java 2 Runtime Environment Standard Edition v1.4.2
Linux kernal 2.4.18.44			Mozilla 1.0.1	

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**
WPA Dynamic ONLY 1. Define MAC authentication method 2. Enable IEEE 802.1x 3. Configure RADIUS server 4. Configure WPA type 5. Configure multicast cipher type 6. Configure clients type 7. Configure open authentication 8. Enable encryption	**Global Configuration Level** HP420(config)#mac-authentication server local ***OR*** HP420(config)#no mac-authentication server HP420(config)#802.1x required* 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)#wpa-mode dynamic HP420(if-wireless g)#multicast-cipher <TKIP | AES> HP420(if-wireless g)#wpa-clients required HP420(if-wireless g)#authentication open HP420(if-wireless g)#encryption <64 | 128 | 152>	RADIUS server required. 802.1x supplicant required. WPA supported client required.	
WPA Pre-shared Key ONLY 1. Define MAC authentication method 2. Disable IEEE 802.1x 3. Configure WPA type 4. Configure multicast cipher type 5. Configure clients type 6. Configure key type 7. Configure key 8. Configure open authentication 9. Enable encryption	**Global Configuration Level** HP420(config)#mac-authentication server local ***OR*** HP420(config)#no mac-authentication server HP420(config)#no 802.1x **Context Configuration Level** HP420(if-wireless g)#wpa-mode pre-shared-key HP420(if-wireless g)#multicast-cipher <TKIP | AES> HP420(if-wireless g)#wpa-clients required HP420(if-wireless g)#wpa-psk-type <alphanumeric | hex> HP420(if-wireless g)#wpa-preshared-key <ASCII | HEX> <*preshared key*> HP420(if-wireless g)#authentication open HP420(if-wireless g)#encryption <64 | 128 | 152>	WPA supported client required.	Requires manual key management.

Configuring Encryption in the HP ProCurve Wireless Access Point 420			
Encryption Methods and Process	**CLI Privilege Level and Commands*** **	**Additional Requirements**	**Notes**
WEP Dynamic ONLY 1. Define MAC authentication method 2. Enable IEEE 802.1x 3. Configure RADIUS server 4. Configure multicast cipher type 5. Configure clients type 6. Configure open authentication 7. Enable encryption	**Global Configuration Level** HP420(config)#mac-authentication server local ***OR*** HP420(config)#no mac-authentication server HP420(config)#802.1x required* 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)#multicast-cipher WEP HP420(if-wireless g)#wpa-clients supported HP420(if-wireless g)#authentication open HP420(if-wireless g)#encryption <64 | 128>	RADIUS server required. 802.1x supplicant required. WEP supported client required.	
WEP Static ONLY 1. Define MAC authentication method 2. Disable IEEE 802.1x 3. Configure multicast cipher type 4. Configure clients type 5. Configure key index 6. Configure key 7. Configure shared authentication 8. Enable encryption	**Global Configuration Level** HP420(config)#mac-authentication server remote** ***OR*** HP420(config)#mac-authentication server local ***OR*** HP420(config)#no mac-authentication server HP420(config)#no 802.1x **Context Configuration Level** HP420(if-wireless g)#multicast-cipher WEP HP420(if-wireless g)#wpa-clients supported HP420(if-wireless g)#transmit-key <1 | 2 | 3 | 4> HP420(if-wireless g)#key <1 | 2 | 3 | 4> <64 | 128 | 152> <ASCII | HEX> <*key*> HP420(if-wireless g)#authentication shared HP420(if-wireless g)#encryption <64 | 128 | 152>	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. Parameters "index" and "length" of the **Key** command must match the values entered in the **Encryption** and **Transmit-Key** commands.

* 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 Settings**			**RADIUS**	**Comments**
			MAC Address	**Permission**			
		System Default		**Deny**	**Allow**		
Local MAC authentication	Local MAC	Deny	xx-xx-xx-xx-xx-xx		*	Not needed	All MAC addresses **denied unless permission specifically allowed** in 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 **allowed unless permission specifically denied** in the MAC Authentication Table. Can be combined with other methods for improved security.
Remote MAC authentication	Radius MAC	MAC address permission policy based on RADIUS server configuration.	RADIUS Server Use PAP authentication and 12 contiguous characters for the MAC address i.e. 0030f18c83b4. User and password on the RADIUS server must be the same.			MUST	Works with authentication Open/Shared AND encryption Disabled/ WEP Static.

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 2.0.37

Problems Resolved in Release 2.0.37

- **CLI/Web** — In the web interface, the error message for the SNTP Server configuration for minutes incorrectly shows “Month.” (18-00162)
- **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)
- **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)
- **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 2.0.37 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 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.

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** — When using the web interface to configure WEP shared keys, the key values still appear to be active after being successfully deleted. The CLI should display the status as "Empty." (18-00024, 18-00025, 18-00026, 18-00113, 18-00270, 18-00382)
- **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 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** — 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 setting the system clock in the CLI using the **sntp-server date-time** command, the CLI accepts invalid characters for hours and minutes. (18-00154)
- **CLI/Web** — The web interface Help file specifies a maximum of 22 characters for the system name. A user can enter up to 32 characters. (18-00155)
- **CLI/Web** — The web interface Help file does not have any information on VLAN configuration. (18-00156)
- **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. (18-00158)
- **CLI/Web** — If an invalid date (for example, September 31) is selected when setting the Daylight Saving time period using the web interface, an error message is displayed on the "Configuration has been saved" page. (18-00164)
- **CLI/Web** — In the web and CLI interface, the Ethernet protocol filter type DEC_MOP is actually DEC DNA Remote Console. (18-00186)
- **CLI/Web** — In the web and CLI interface, the Ethernet protocol filter type DEC_MOP_Dump_Load is actually DEC DNA Dump/Load. (18-00187)
- **CLI/Web** — In the web and CLI interface, the Ethernet protocol filter type DEC_XNS is actually DEC Proto. (18-00188)
- **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** — If the login user name is changed using the web interface and is less than three characters or more than 16 characters, there is no error message even though the value is invalid and the change not saved. (18-00217)
- **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** — 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, 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** — 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** — 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 CLI interface does not accept a WPA Pre-Shared Key value with space characters. (18-00251, 18-00287)
- **CLI/Web** — Using the CLI/web interface, invalid IP addresses can be entered for the access point IP and gateway IP. (18-00252, 18-00253)
- **CLI/Web** — Using the web interface, invalid IP addresses can be entered for the SNMP Trap Destination IP Address. (18-00254)
- **CLI/Web** — Using the web interface, invalid IP addresses can be entered for the RADIUS server IP Address (primary and secondary). (18-00255)
- **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** — 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** — When using Netscape 7.0 or 7.1 with Sun Java 2 Runtime Environment Standard Edition 1.4.1 or 1.4.2, the mouse pointer does not change its shape to a hyperlink pointer. (18-00324)
- **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)
- **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** — 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** — 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 some junk text. (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 enterpriseA-pFileTransferMgt 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)
- **Encryption** — When using the web interface to configure WEP shared keys, an alphanumeric string of blank spaces is accepted as a valid key. (18-00092, 18-00167, 18-00168)
- **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 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)
- **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)

- **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)
- **Radio** — Two Country Code settings (Czech and Malaysia) can only use channel 1 and no other channel can be selected. (18-00269)
- **Radio** — Regardless of the speed selected via the user interfaces, the AP will always transmit at the maximum speed rate (11 Mbps for 802.11b and 54 Mbps for 802.11g). (18-00271, 18-00387)
- **VLANs** — The access point allows a client to be assigned a VLAN ID of 4095, which is a reserved ID number. (18-00074)
- **Ethernet Interface** — The access point does not allow the Ethernet interface to be disabled (shutdown) using Telnet or SNMP. The only way to disable and enable the Ethernet interface is using the CLI through a console port connection. (18-00107)
- **System Log** — The System Log does not show an entry when the 802.11g radio channel is changed to "auto." (18-00209, 18-00277)
- **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)
- **SNTP** — When using SNTP the access point indicates the wrong NTP version number in NTP packets (it indicates 1 when it should be 3). (18-00245)
- **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)
- **DHCP** — Some wireless client cards cannot get an IP address from a DHCP Server if their power saving mode is enabled. (18-00284)
- **DHCP** — The access point does not send DHCP decline packet even though another client is using the same IP address. (18-00359)
- **DHCP** — The access point does not sent a Unicast and Broadcast "DHCP Request" packet after 30 seconds of losing connection to a DHCP Server. (18-00360)
- **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 loose association for some minutes. (18-00392, 18-00396)

- **System** — The 128 client association limit is not properly enforced by the access point. (18-00405)
- **System** — The multicast data rate must be set to 1 Mbps in order to operate properly with Agere based radios. (18-00412)

Edition 3, May 2004
Manual Part Number
5990-6007