



Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(7)JA

August 15, 2005

These release notes describe features, enhancements, and caveats for Cisco IOS Release 12.3(7)JA. They also provide important information about Cisco Aironet 350, 1100, 1130AG, 1200, 1230AG, and 1240AG Series Access Points.

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 6](#)
- [Important Notes, page 10](#)
- [Caveats, page 17](#)
- [Troubleshooting, page 22](#)
- [Documentation Updates, page 23](#)
- [Related Documentation, page 23](#)
- [Obtaining Documentation and Submitting a Service Request, page 23](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005 Cisco Systems, Inc. All rights reserved.

Introduction

The Cisco Aironet Access Point is a wireless LAN transceiver that acts as the connection point between wireless and wired networks or as the center point of a standalone wireless network. In large installations, the roaming functionality provided by multiple access points enables wireless users to move freely throughout the facility while maintaining uninterrupted access to the network.

You can configure and monitor 350, 1100, 1130AG, 1200, and 1240AG series access points using the command-line interface (CLI), the web-browser interface, or Simple Network Management Protocol (SNMP).

System Requirements

You can install Cisco IOS Release 12.3(7)JA on all 350, 1100, 1130AG, 1200, 230AG, and 1240AG access points.

**Note**

Software upgrades fail when you use the web-browser interface to install Cisco IOS Release 12.3(7)JA on 1200 series access points. The image size exceeds the access point's 4-MB restriction for software upgrades. Use TFTP to upgrade your access point to this release. For complete instructions on using TFTP to upgrade access point software, see the "Working with Software Images" section in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*. Click this link to browse to that document:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/tsd_products_support_configure.html

You can also install this release on 350 and 1200 series access points that have been converted to run Cisco IOS software. You can tell whether an access point runs VxWorks or Cisco IOS software by looking at the GUI: the GUI on an access point running VxWorks has a yellow and red color scheme, and the GUI on an access point running Cisco IOS software has a green, light-green, and black color scheme.

Your 350 series access point must run one of these VxWorks versions before you can convert to IOS software: 12.03T, 12.02T1, 12.01T1, 11.23T, or 11.21. Your 1200 series access point must run one of these VxWorks versions before you can convert to IOS software: 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T. If your access point runs version 12.04, you must downgrade to a supported VxWorks version before upgrading to IOS software.

The conversion upgrade image for 350 series access points installs Cisco IOS Release 12.2(13)JA1 on your 350 series access point. The conversion upgrade image for 1200 series access points installs Cisco IOS Release 12.2(13)JA2 on your 1200 series access point.

**Note**

Cisco Aironet 340 Series Access Points do not support IOS software. Do not attempt to load an IOS image on 340 series access points or on 350 and 1200 series access points that have not been converted.

Finding the IOS Software Version

To find the version of IOS software running on your access point, use a Telnet session to log into the access point and enter the **show version** EXEC command. This example shows command output from an access point running Cisco IOS Release 12.2(15)JA:

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(15)JA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
```

On access points running IOS software, you can also find the software version on the System Software Version page in the access point's web-browser interface. If your access point does not run IOS software, the software version appears at the top left of most pages in the web-browser interface.

Upgrading to a New Software Release

For instructions on installing access point software for your access point:

-
- Step 1** Follow this link to the Cisco home page:
<http://www.cisco.com>
 - Step 2** Click **Technical Support and Documentation**. The Technical Support and Documentation page appears.
 - Step 3** Click **Wireless**. The Wireless Support Resources page appears.
 - Step 4** Scroll down to the Wireless LAN Access section.
 - Step 5** Select the access point model for which you need the information. The Introduction page for the model you selected appears.
 - Step 6** Under the Configure section, click **Install and Upgrade Guides**. A list of configuration documents appears.
 - Step 7** Click **Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.3(7)JA**.
 - Step 8** Navigate to the Managing Firmware and Software chapter.
-

For information on Cisco IOS software, click this link to browse to the Cisco IOS Software Center on Cisco.com:

<http://www.cisco.com/cisco/software/navigator.html>

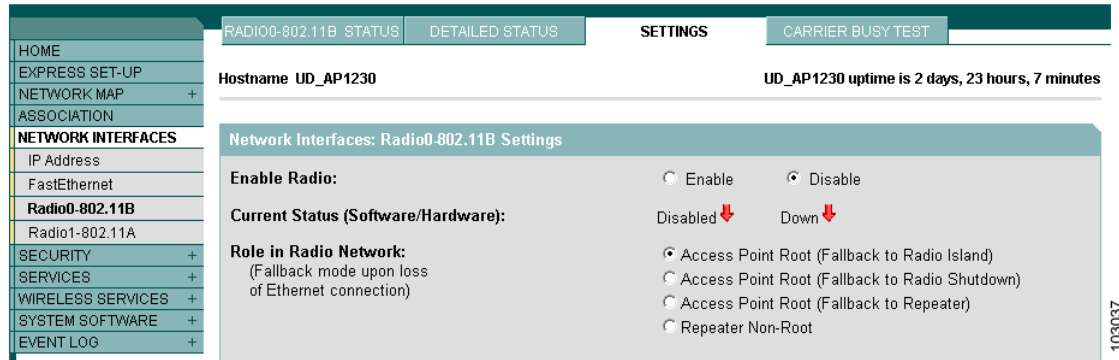
Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

If your access point runs Cisco IOS Release 12.2(11)JA, 12.2(11)JA1, or 12.2(11)JA2, your access point might unexpectedly reboot after you upgrade to a later Cisco IOS Release. Because of a rare timing condition that affects the radios, the access point sometimes reboots immediately after the upgrade when the radios are enabled. However, after the access point reboots the upgrade is complete and the access point operates normally. To prevent the access point from rebooting unexpectedly, disable the radio interfaces before upgrading software.

Follow these steps to disable the radio interfaces using the web-browser interface:

- Step 1** Browse to the Network Interfaces: Radio Settings page. [Figure 1](#) shows the top portion of the Network Interfaces: Radio Settings page.

Figure 1 Network Interfaces: Radio Settings Page



- Step 2** Select **Disable** to disable the radio.
- Step 3** Click **Apply** at the bottom of the page.
- Step 4** If your access point has two radios, repeat these steps for the second radio.

Beginning in privileged EXEC mode, follow these steps to disable the access point radios using the CLI:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio {0 1}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	shutdown	Disable the radio port.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

If your access point has two radios, repeat these steps for the second radio. Use the **no** form of the **shutdown** command to enable the radio.

Converting to Cisco IOS Software

If your 350 or 1200 series access point does not run IOS software, you can use the conversion utility or the conversion upgrade image to convert the access point system to IOS software. Use the conversion utility to maintain the current configuration after the conversion, or load the upgrade image to convert to IOS software without saving the current configuration. Your access point must be running one of these VxWorks firmware versions before you can convert to IOS software:

- 350 series access points must be running VxWorks version 12.03T, 12.02T1, 12.01T1, 11.23T, or 11.21

- 1200 series access points must be running VxWorks version 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T

The conversion upgrade image for 350 series access points installs Cisco IOS Release 12.2(13)JA1 on your 350 series access point. The conversion upgrade image for 1200 series access points installs Cisco IOS Release 12.2(13)JA2 on your 1200 series access point.

**Note**

The upgrade image and the conversion tool do not support VxWorks version 12.04. Access points running version 12.04 must be downgraded to a supported operating system version before you can use the upgrade image or the conversion tool.

**Note**

The upgrade to Cisco IOS software is permanent; you cannot revert to non-IOS software. Product warranties do not cover unintended upgrades.

For complete instructions on using the conversion utility, refer to the *Cisco Aironet Conversion Tool for Cisco IOS Software, 2.0 Administrator Guide for Windows*. Click this link to browse to the Administrator Guide:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/tsd_products_support_configure.html

To download the conversion utility or the upgrade image, click this link to browse to the Cisco IOS Software Center on Cisco.com:

<http://www.cisco.com/cisco/software/navigator.html>

On the Cisco IOS Software Center page, enter your Cisco.com username and password to use the Feature Navigator or the Cisco IOS Upgrade Planner, or click **Wireless Software** to go to the Wireless LAN Software page. Download the conversion utility or the upgrade image for 350 or 1200 series access points. You can also download instructions for using the utility and the image.

Some Fields Not Updated During Upgrade to IOS Software

When you upgrade an access point to run Cisco IOS software, some fields that are reported in the console messages during the upgrade are blank or are populated with zeros. However, blank or zero fields are normal after a successful upgrade, because 350 and 1200 series access points do not support that information. This example shows fields that might appear blank or populated with zeros:

```
32K bytes of flash-simulated non-volatile configuration memory.
Base Ethernet MAC Address: 00:05:9A:38:42:91
Part Number: 0-0000-00
PCA Assembly Number: 000-00000-00
PCA Revision Number:
PCB Serial Number:
Top Assembly Part Number: 000-00000-00
Top Assembly Serial Number:
Top Revision Number:
Product/Model Number: AIR-AP352-IOS-UPGRD
```

New Features

This section lists new features in Cisco IOS Release 12.3(7)JA. [Table 1](#) lists the features that are supported on the devices that support this release.

Table 1 *New Features Introduced for Access Points in Cisco IOS Release 12.3(7)JA*

Feature	350 Series	1100 Series	1130AG Series	1200 Series	1230AG Series	1240AG Series
Access point link role flexibility	–	–	–	x	x	x
AAA cache and profile	–	x	x	x	x	x
SSH v2 server support	–	x	x	x	x	x



Note

The new features included in this release are not supported on the 350 series access points.

Access Point Link Role Flexibility

Access point link role flexibility allows an access point to operate in a combination of radio roles, such as access point root, access point repeater, bridge root (with or without clients), bridge nonroot (with or without clients), and workgroup bridge. This feature provides a more flexible deployment scheme for the Cisco Aironet 1200 Series Access Point supporting various applications requirement.

AAA Cache and Profile

AAA cache and profile is a new capability to cache the information returned from the RADIUS or TACACS+ server a more efficient handling of the administrative authentication process.

SSH v2 Server Support

SSH v2 server support is a standards-based protocol to provide secure Telnet capability for router configuration and administration.

Installation Notes

This section contains information you should keep in mind when installing 350, 1100, 1130AG, 1200, 1230AG, and 1240AG series access points.

Installation in Environmental Air Space

This section provides information on installing 1100 and 1200 series access points in environmental air space, such as above suspended ceilings.

Cisco Aironet 1100, 1130AG, 1200, and 1240AG Series Access Points provide adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the *National Electrical Code* (NEC) and Sections 2-128, 12-010(3) and 12-100 of the *Canadian Electrical Code*, Part 1, C22.1.

**Caution**

The power injector does not provide fire resistance and low smoke-producing characteristics and is not intended for use in extremely high or low temperatures or in environmental air spaces such as above suspended ceilings.

**Note**

If you plan to mount a 1200 series access point with a 5-GHz radio in an area subject to environmental air space, Cisco recommends that you mount the access point horizontally so that its antennas point down. Doing so ensures that the access point complies with regulatory requirements for environmental air space with the 5-GHz radio installed.

Power Considerations

This section describes issues you should consider before applying power to an access point.

**Caution**

The operational voltage range for 1100 series access points is 35 to 57 VDC, and the nominal voltage is 48 VDC. Voltage higher than 60 VDC can damage the equipment.

**Caution**

The nominal voltage for 1200 series access points is 48 VDC, and the access point is operational up to 60 VDC. Voltage higher than 60 VDC can damage the equipment.

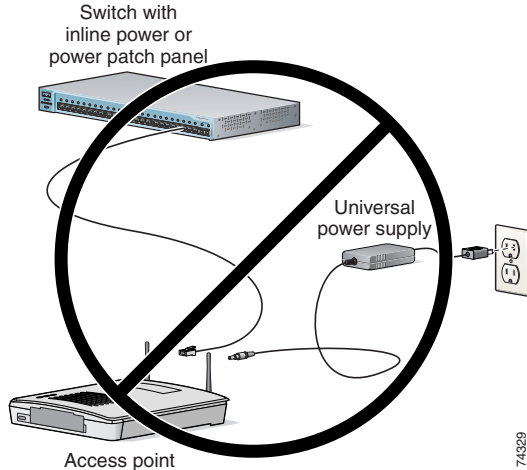
**Caution**

Cisco Aironet power injectors are designed for use with Cisco Aironet access points and bridges only. *Do not use the power injector with any other Ethernet-ready device.* Using the power injector with other Ethernet-ready devices can damage the equipment.

Use Only One Power Option

You cannot provide redundant power to 1100, 1130AG, and 1200 series access points with both DC power to its power port and inline power from a patch panel or powered switch to the access point's Ethernet port. If you apply power to the access point from both sources, the switch or power patch panel might shut down the port to which the access point is connected. [Figure 2](#) shows the power configuration that can shut down the port on the patch panel or powered switch.

Figure 2 *Improper Power Configuration Using Two Power Sources*



Configuring Power for 1130AG, 1230AG, and 1240AG Access Points

The 1130AG, 1230AG, and 1240AG access points disable the radio interfaces when the unit senses that the power source to which it is connected does not provide enough power. Depending on your power source, you might need to enter the power source type in the access point configuration. Use the System Software: System Configuration page on the web-browser interface to select a power option. [Figure 3](#) shows the System Power Settings section of the System Configuration page.

Figure 3 *Power Options on the System Software: System Configuration Page*

System Power Settings	
Power State:	FULL POWER
Power Source:	AC_ADAPTOR
Power Settings:	<input type="radio"/> Power Negotiation <input checked="" type="radio"/> Pre-standard Compatibility
Power Injector:	<input type="checkbox"/> Installed on Port with MAC Address: <input type="text" value="DISABLED"/> (HHHH.HHHH.HHHH)
<input type="button" value="Apply"/>	

121655

Using the AC Power Adapter

If you use the AC power adapter to provide power to the access point, you do not need to adjust the access point configuration.

Using a Switch Capable of IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the access point and the switch supports the IEEE 802.3af power negotiation standard, select **Power Negotiation** on the System Software: System Configuration page.

Using a Switch That Does Not Support IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the access point and the switch does not support the IEEE 802.3af power negotiation standard, select **Pre-Standard Compatibility** on the System Software: System Configuration page.

Using a Power Injector

If you use a power injector to provide power to the access point, select **Power Injector** on the System Software: System Configuration page and enter the MAC address of the switch port to which the access point is connected.

Operating 5-GHz Radio Requires Power Injector, Power Module, or Catalyst 3550-24 PWR Switch

The 1200 series power injector and the 1200 series power module support operation of the 5-GHz radio in the access point. Currently, the Catalyst 3550-24 PWR switch supports power for both the 2.4-GHz radio and the 5-GHz radio. Other switches and power patch panels might not provide enough power for the 5-GHz radio.

Access Point Requires 1200 Series Universal Power Supply and Power Injector

The 350 series universal power supply and power injector are not compatible with the 1200 series access point. If you use a power injector or a power module to provide power to a 1200 series access point, you must use a 1200 series universal power supply. If you need to use a power injector to inject power into the access point's Ethernet port, you must use a 1200 series power injector.

Unpowered 1100 Series Access Points Cause Loopback When Connected to Switches Without Loopback Detection

When you connect an unpowered 1100 series access point to a switch without loopback detection, the access point causes a loopback. To avoid this problem, make sure loopback detection is enabled on the switch to which the access point is connected. If your switch does not have loopback detection, disconnect the access point from the switch when the access point power is off.

Antenna Installation

For instructions on the proper installation and grounding of external antennas for 1200 and 1240AG series access points, refer to the National Fire Protection Association's *NFPA 70, National Electrical Code*, Article 810, and the Canadian Standards Association's *Canadian Electrical Code*, Section 54.



Warning

Do not install the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death.

Important Notes

This section describes important information about the access point.

Change to Default IP Address Behavior

Cisco IOS Releases 12.3(2)JA and later change the default behavior of access points requesting an IP address from a DHCP server:

- When you connect a 350, 1130AG, 1200, 1230AG, or 1240AG series access point with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an address, continues to send requests indefinitely.
- When you connect an 1100 series access point with a default configuration to your LAN, the 1100 series access point makes several attempts to get an IP address from the DHCP server. If it does not receive an address, it assigns itself the IP address 10.0.0.1 for five minutes. During this five-minute window, you can browse to the default IP address and configure a static address. If after five minutes the access point is not reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five-minute window for browsing to the access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

SNMP Configuration `snmp-server ifindex persist` Causes Continuous Reboot

Access points and bridges sometimes continuously reboot when the configuration contains this line:

```
snmp-server ifindex persist
```

Remove this line from the configuration before upgrading to this release. If you upgrade to this release and the configuration contains this line, remove the line and delete the `ifIndex-table` file from NVRAM.

Save Interface Level Configuration Before Upgrading to Release 12.3(7)JA

If the access points have SSIDs configured at the interface level (rather than at the global level), before upgrading to Cisco IOS Release 12.3(7)JA and above, upgrade to Cisco IOS Release 12.3(4)JA, save the configurations and then upgrade to Release 12.3(7)JA. This procedure must be followed to make sure that the SSID configurations are converted from the interface level to global level.

Changes to the Default Configuration—Radios Disabled and No Default SSID

In this release, the radio or radios are disabled by default, and there is no default SSID. You must create an SSID and enable the radio or radios before the access point will allow wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points.

Trunking Fails on Access Point in Workgroup Bridge Mode

When an access point is configured as a workgroup bridge, trunking on its Ethernet port fails for clients belonging to VLANs other than the Native VLAN. This can be corrected by one of two workarounds:

- Configure Ethernet clients to belong to the Native VLAN
- Configure the access point with the **workgroup-bridge client-vlan <vlan-id>** command, where *vlan-id* is the VLAN assigned to wired clients on the Ethernet side.

Clients Using WPA/WPA2 and Power Save May Fail to Authenticate

Certain clients using WPA/WPA2 key management and power save may take many attempts to authenticate or, in some cases, fail to authenticate. Any SSID defined to use authentication key-management *wpa*, coupled with clients using power save mode and authenticating using WPA/WPA2 may experience this problem.

A hidden configure level command, **dot11 wpa handshake timeout**, can be used to increase the timeout between sending the WPA key packets from the default value (100 ms) to a value between 101 and 200 ms. The command stores its value in the configuration across device reloads.

Default Username and Password Are *Cisco*

When you open the access point interface, you must enter a username and password. The default username for administrator login is *Cisco*, and the default password is *Cisco*. Both the username and password are case sensitive.

Some Client Devices Cannot Associate When QoS Is Configured

Some wireless client devices, including Dell Axim handhelds and Hewlett-Packard iPaq HX4700 handhelds, cannot associate to an access point when the access point is configured for QoS. To allow these clients to associate, disable QoS on the access point. You can use the QoS Policies page on the access point GUI to disable QoS, or enter this command on the CLI:

```
ap(config-if)#no dot11 qos mode
```

Some Devices Disassociate When Multiple BSSIDs Are Added or Deleted

Devices on your wireless LAN that are configured to associate to a specific access point based on the access point MAC address (such as client devices, repeaters, hot standby units, or workgroup bridges) might lose their association when you add or delete a multiple BSSID. When you add or delete a multiple BSSID, check the association status of devices configured to associate to a specific access point. If necessary, reconfigure the disassociated device to use the BSSID's new MAC address.

Enabling MBSSIDs Without VLANs Disables Radio Interface

If you use the mbssid configuration interface command to enable multiple BSSIDs on a specific radio interface but VLANs are not configured on the access point, the access point disables the radio interface. To re-enable the radio, you must shut down the radio, disable multiple BSSIDs, and re-enable the radio. This example shows the commands you use to re-enable the radio:

```
AP1134(config)# interface d1
AP1134(config-if)# shut
AP1134(config-if)# no mbssid
AP1134(config-if)# no shut
```

After you re-enable the radio, you can enable VLANs on the access point and enable multiple BSSIDs.

Cannot Set Channel on DFS-Enabled Radios

Access points with 5-GHz radios configured at the factory for use in Europe, Singapore, Korea, Japan, Taiwan, and Israel now comply with regulations that require radio devices to use Dynamic Frequency Selection (DFS) to detect radar signals and avoid interfering with them. You cannot manually set the channel on DFS-enabled radios.

Cisco 7920 Phones Require Firmware Version 1.09 or Later When Multiple BSSIDs Are Enabled

When multiple BSSIDs are configured on the access point, Cisco 7920 wireless IP phones must run firmware version 1.09 or later.

AIR-RM21A/AIR-RM22A Radio Modules Usually Set to Max Transmit Power

AIR-RM21A and AIR-RM22A radio modules measure transmit power in decibels per milliwatt (dBm), but earlier versions of 802.11a radios in Cisco Aironet access points measure power in milliwatts (mW). Because power settings in mW do not translate directly to settings in dBm, the access point usually uses the default power setting of maximum when you install a new AIR-RM21A or AIR-RM22A radio module.

Table 2 lists 802.11a transmit power settings in mW and the power settings that the access point assigns to a new radio module.

Table 2 Transmit Power Settings Assigned to New Radio Modules

Power Settings in mW	Power Setting Assigned to New Radio Module
5	5 dBm (approximately 3 mW)
10	maximum (17 dBm)
20	maximum
40	maximum

GRE Tunnelling Through WLSM Sometimes Requires MTU Setting Adjustments

If client devices on your wireless LAN cannot use certain network applications or cannot browse to Internet sites, you might need to adjust the MTU setting on the client devices or other network devices. For more information, refer to the Tech Note at this URL:

http://www.cisco.com/en/US/tech/tk827/tk369/technologies_tech_note09186a0080093f1f.shtml

TACACS+ and DHCP IP Address Sometimes Locks Out Administrators

When you configure an access point for TACACS+ administration and to receive an IP address from the DHCP server, administrators might be locked out of the access point after it reboots if the administrator does not have a local username and password configured on the access point. This issue does not affect access points configured with a static IP address. Administrators who have been locked out must regain access by using the console port to reset the unit to default settings.

Access Points Do Not Support Loopback Interface

You must not configure a loopback interface on the access point.



Caution

Configuring a loopback interface might generate an IAPP GENINFO storm on your network and disrupt network traffic.

Non-Cisco Aironet 802.11g Clients Might Require Firmware Upgrade

Some non-Cisco Aironet 802.11g client devices require a firmware upgrade before they can associate to the 802.11g radio in the access point. If your non-Cisco Aironet 802.11g client device does not associate to the access point, download and install the latest client firmware from the manufacturer's website.

Throughput Option for 802.11g Radio Blocks Association by 802.11b Clients

When you configure the 802.11g access point radio for **best throughput**, the access point sets all data rates to basic (required). This setting blocks association from 802.11b client devices. The **best throughput** option appears on the web-browser interface Express Setup and Radio Settings pages and in the **speed** CLI configuration interface command.

Transmit Power Set to Maximum When You Install 802.11g Radio

When you replace the 802.11b radio in a 1200 series access point with an 802.11g radio, the 802.11g radio is set to the maximum transmit power allowed in your regulatory domain regardless of the power setting configured on the 802.11b radio. After you install the 802.11g radio and the access point reboots, configure the 802.11g radio to the preferred transmit power.

Use Auto for Ethernet Duplex and Speed Settings

Cisco recommends that you use **auto**, the default setting, for both the speed and duplex settings on the access point Ethernet port. When your access point receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link reboots the access point. If the switch port to which the access point is connected is not set to **auto**, you can change the access point port to **half** or **full** to correct a duplex mismatch and the Ethernet link is not reset. However, if you change from **half** or **full** back to **auto**, the link is reset and, if your access point receives inline power from a switch, the access point reboots.



Note The speed and duplex settings on the access point Ethernet port must match the Ethernet settings on the port to which the access point is connected. If you change the settings on the port to which the access point is connected, change the settings on the access point Ethernet port to match.

Use force-reload Option with archive download-sw Command

When you upgrade access point or bridge system software by entering the **archive download-sw** command on the CLI, you must use the **force-reload** option. If the access point or bridge does not reload the Flash after the upgrade, the pages in the web-browser interface might not reflect the upgrade. This example shows how to upgrade system software successfully using the **archive download-sw** command:

```
AP# archive download-sw /force-reload /overwrite tftp://10.0.0.1/image-name
```

Radio MAC Address Appears in ACU

When a Cisco Aironet client device associates to an access point running IOS software, the access point MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Radio MAC Address Appears in Access Point Event Log

When a client device roams from an access point (such as access point *alpha*) to another access point (access point *bravo*), a message appears in the event log on access point alpha stating that the client roamed to access point bravo. The MAC address that appears in the event message is the MAC address for the radio in access point bravo. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Mask Field on IP Filters Page Behaves the Same As in CLI

In Cisco IOS Release 12.2(8)JA and later, the mask that you enter in the Mask field on the IP Filters page in the access point GUI behaves the same way as a mask that you enter in the CLI. If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address that you entered in the IP Address field.

Repeater Access Points Running IOS Software Cannot Associate to Parent Access Points Running VxWorks

Repeater access points running Cisco IOS software cannot associate to parent access points that do not run IOS software (all 340 series access points, and 350 and 1200 series access points that have not been converted to run IOS software).

Repeater Access Points Cannot Be Configured as WDS Access Points

Repeater access points do not support WDS. You cannot configure a repeater access point as a WDS access point, and if a root access point becomes a repeater in fallback mode, it cannot provide WDS.

Crossover Cable Sometimes Needed When Ethernet Speed and Duplex Set to Fixed on 1100 Series Access Points

If you change the speed and duplex settings from auto to fixed on an 1100 series access point's Ethernet port, the auto-MDIX feature on the port is disabled. When auto-MDIX is disabled, you must determine whether to use a straight-through or a crossover cable to connect the access point Ethernet port to another device. If the Ethernet link goes down after you set the speed and duplex to fixed, try changing the Ethernet cable from crossover to straight-through or from straight-through to crossover.

Cannot Perform Link Tests on Non-Cisco Aironet Client Devices and on Cisco Aironet 802.11g Client Devices

The link test feature on the web-browser interface does not support non-Cisco Aironet client devices nor Cisco Aironet 802.11g client devices.

System Software Upgrade Sometimes Fails Using Microsoft Internet Explorer 5.01 SP2

A system software upgrade sometimes fails when you use Microsoft Internet Explorer 5.01 SP2 to upgrade system software using the TFTP Upgrade page in the web-browser interface. Use a later version of Microsoft Internet Explorer to perform HTTP system software upgrades, or use TFTP to upgrade system software. Click this URL to browse to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for complete instructions on performing software upgrades:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/tsd_products_support_configure.html

1100 Series Access Points with Boot Loader Version 12.2(4)JA Boot into Monitor Mode

When the Ethernet port is disabled on an 1100 series access point running boot loader version 12.2(4)JA, the access point boots into monitor mode when it reboots. To avoid this problem, connect the access point Ethernet port to one of the following:

- a wired LAN
- the Ethernet port on a PC

Remove power from the access point and reapply power to reboot the unit. When the access point senses an Ethernet connection, it boots normally.

Corrupt EAP Packet Sometimes Causes Error Message

During client authentication, the access point sometimes receives a corrupt EAP packet and displays this error message:

```
Oct 1 09:00:51.642 R: %SYS-2-GETBUF: Bad getbuffer, bytes= 28165
-Process= "Dot11 Dot1x process", ipl= 0, pid= 32
-Traceback= A2F98 3C441C 3C7184 3C604C 3C5E14 3C5430 124DDC
```

You can ignore these messages.

When Cipher Is TKIP Only, Key Management Must Be Enabled

When you configure **TKIP**-only cipher encryption (not **TKIP + WEP 128** or **TKIP + WEP 40**) on any radio interface or VLAN, every SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSIDs, client authentication fails on the SSIDs.

Cisco CKM Supports Spectralink Phones

Cisco CKM (CCKM) key management is designed to support voice clients that require minimal roaming times. To date, CCKM supports only Spectralink and Cisco 7920 Version 2.0 Wireless Phones. Other voice clients have not been tested with CCKM and are not supported.

Non-Cisco Aironet Clients Sometimes Fail 802.1x Authentication

Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

Pings and Link Tests Sometimes Fail to Clients with Both Wired and Wireless Network Connections

When you ping or run a link test from an access point to a client device installed in a PC running Microsoft Windows 2000, the ping or link test sometimes fails when the client has both wired and wireless connections to the LAN. Microsoft does not recommend this configuration. For more information, refer to Microsoft Knowledge Base article 157025 at this URL:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;157025&Product=win2000>

Layer 3 Mobility Not Supported on Repeaters and Workgroup Bridges

Repeater access points and workgroup bridges cannot associate to an SSID configured for Layer 3 mobility. Layer 3 mobility is not supported on repeaters and workgroup bridges.

WLSM Required for Layer 3 Mobility

You must use a Wireless LAN Services Module (WLSM) as your WDS device in order to properly configure Layer 3 mobility. If you enable Layer 3 mobility for an SSID and your WDS device does not support Layer 3 mobility, client devices cannot associate using that SSID.

Caveats

This section lists [Open Caveats](#) and [Resolved Caveats](#) in Cisco IOS Release 12.3(7)JA.

Open Caveats

These caveats are open in Cisco IOS Release 12.3(7)JA:

- CSCsa68885—A root access point on which VLANs are configured sometimes forwards multicast packets from the non-native VLAN to an associated repeater, which drops them.
- CSCeg49666—EAP-TTLS class subattributes are dropped when WDS is enabled.

When WDS is enabled, the WDS master access point drops the [25] class subattributes in the tunnelled access accept when sending the accounting request using EAP-TTLS.

Workaround: Disable WDS or use WLSE reports.

- CSCeh68636—1100 series access point logs “CDP_PD-2-POWER_LOW: All radios disabled” and changes both dot11 radio interfaces to a reset state

When a power injector (AIR-PWRINJ3) is inserted between the access point and a Catalyst switch, the power injector provides power to the access point instead of the switch. When the access point boots, it waits for CDP packets from the switch. If the output power of the switch does not support the access point, the access point changes the dot11 radio interface to a reset state.

Workarounds: Disable CDP on either the Catalyst switch or the access point or do not use a power injector; connect an AC power adapter directly to the access point.

- CSCei05154—CLI does not allow open authentication with EAP for CCKM.
Currently, authentication is required for network EAP for CCKM authentication. CCX v4 allows 802.1x types other than LEAP and EAP-FAST (such as PEAP MS-CHAP v2). The CLI should allow open authentication open EAP for CCKM as well. If only open authentication EAP is configured for an SSID, the following error message appears when authentication key management CCKM is configured using the CLI:

```
Error: Network-EAP authentication is required for CCKM
```


Workaround: Configure authentication network-EAP and authentication key-management CCKM first. Then remove authentication network-EAP and add authentication open EAP.
- CSCej08390—Access points and bridges sometimes continuously reboot when the configuration contains this line:

```
snmp-server ifindex persist
```


Remove this line from the configuration before upgrading to this release. If you upgrade to this release and the configuration contains this line, remove the line and delete the ifIndex-table file from NVRAM.
- CSCsa76421—1100 series access point ifInUncastPkts decrease at regular intervals and then increase again.
There is no workaround for this condition.
- CSCsa93231—The 1231G access point does not allow UC/MC4500 or UC/MC4800 devices to associate. The Association Response frame constantly returns a Status Code 12.
Workaround: None
- CSCsb09210—802.11g radio advertises short slot capability when 11b rates are set.
When an 802.11g radio is set to 802.11b rates, it continues to advertise the short slot capability in probe responses and beacons.
- CSCeh64403—Poor performance when performing software upgrade when 1300 Series in Workgroup Bridge mode is associated.
Workaround: Downgrade to Cisco IOS release 12.2(15)JA
- CSCsa94560—Access point fails to forward an EAP reject message to a client in power save mode.
- CSCsa95850—Clients using WPA/WPA2 and Power Save may fail to authenticate.
Certain clients using WPA/WPA2 key management and power save may take many attempts to authenticate, or in some cases, fail to authenticate. Any SSID defined to use authentication key-management WPA, coupled with clients using power save mode and authenticating using WPA/WPA2 may experience this problem.
Workaround: A hidden configure level command, **dot11 wpa handshake timeout**, can be used to increase the timeout between sending the WPA key packets from the default value (100 ms) to a value between 101 and 200 ms. The command stores its value in the configuration across device reloads.
- CSCsa98253—Access point does not display warning when MBSSID is configured on non-MBSSID radio.
An MBSSID can be configured on a radio that does not support the feature.
- CSCeh25902—Access point sends an 802.11 Deauthentication with reason 0.
In the event of an EAP failure, the access point sends an 802.11 deauthentication message with reason 0, which is not in accordance with 802.11 standards.

- CSCsb41187—Cannot change channels on a 350 series access point.
Channels cannot be changed on a 350 series access point using the GUI. They can be changed using the CLI.
Workaround: Change channels using the CLI.
- CSCsb37662—Toggling MBSSID on or off disables access point RM scan.
If an access point configured for participation in Radio Management boots without an MBSSID enabled on a particular radio, RM scan is seen for that radio every 90 seconds until such time that MBSSID is enabled. To get the regular 90 second scan running again on that radio the access point must be reloaded.
The same problem occurs if the AP is booted with MBSSID enabled on a particular radio and MBSSID is subsequently disabled.
- CSCdz53694—Cisco IOS access points provide insufficient association/net map information compared to VxWorks access points.
For troubleshooting purposes, the association table and network map available in the Cisco IOS GUI does not provide the same amount of information as the VxWorks GUI. For example, VxWorks displays infrastructure hosts, wireless clients, multicast clients, bridges, or the entire network. The SSID and VLAN ID of a wireless client can also be displayed.
- CSCsa54608
The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition. Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.
Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.
Only devices running certain versions of Cisco IOS are affected.
Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.
This advisory will be posted at
http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.3(7)JA:

- CSCsb24007
Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:
 - Session Initiation Protocol (SIP)
 - Media Gateway Control Protocol (MGCP)
 - Signaling protocols H.323, H.254
 - Real-time Transport Protocol (RTP)
 - Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCeh43628—1230 series access point no longer exhibits DHCP failure when client is configured for mixed mode (CKIP and 128-key WEP).
- CSCeh49024—Memory leak no longer occurs when an invalid layer 3 WLCCP packet is received.
- CSCsa42443—Autoinstall program now uses hostname from DHCP (if present) when access point is booted with factory defaults.
- CSCsa66924—Access point no longer crashes and reboots when **policy-map** command is issued.
- CSCsa71255—Logging snmp-trap no longer returns to default after reboot.
- CSCeh26214—IP RADIUS source interface no longer disappears after reboot.
- CSCei07867—RM22A radio output power for different channels has been documented in the appropriate hardware installation guides.
- CSCsb06824—Open authentication is no longer added to an EAP SSID when the configuration is loaded.
- CSCsa73846 (duplicate of CSCed16920)—350 series access point no longer shows high CPU and TTY background tracebacks.
- CSCsa78495—LRS configured 1200 series access point now updates unknown username count.
- CSCsa88841—DFS-IAPP constant has been changed to 0x34.
- CSCsb09778 (duplicate of CSCsb06218)—1130 and 1200 access point boot loaders now boot IOS when environment variables are deleted from flash.
- CSCsb27662—Reports greater than 7900 bytes are no longer dropped by WLSE at RM AGG.
- CSCsb06236—CCKM repeater no longer hangs during access point radio scan.
- CSCsa90752—Trunking no longer fails on an 1100 series access point when in workgroup bridge mode.
- CSCeh97288 (duplicate of CSCsa79281)—Spectralink phones no longer reboot after upgrading to Cisco IOS Release 12.3(4)JA
- CSCsb11227—1130 series access points operating as a WDS no longer run out of memory.
- CSCsb14224—Reverse ARP functions on all VLANs
- CSCeb52431—The 1100 series access point no longer sends hundreds of additional authentication requests to a TACACS+ server after successful authentication.
- CSCef95410—WLCCP packets received from an access point no longer causes the radio interface output drop counter to increment.
- CSCsa67267—The **mbssid** command no longer fails on the CLI and the GUI.
- CSCef11167—The access point now returns an accurate value when you poll cDot11ActiveWirelessClients through SNMP.
- CSCeh38024—Access point WPAv2 migration mode now supports Cisco Aironet CB20A client radios running firmware version 2.0.0.184 configured for optional WPAv2.

- CSCsa45650—The 802.11b radio interface in 1200 series access points no longer reports its MAC address as 000000000000 on both the GUI and through SNMP.
- CSCsa68532—The results in the Strength %Out field and the Strength dBm field are no longer reversed when you run a link test from an access point.
- CSCsa74148—Existing SSIDs are no longer invalid when you configure VLANs for the first time.
- CSCsa74153—WPAv2 accounting start/stop records no longer appear in the ACS 3.3 RADIUS accounting log with the client card MAC address as the username instead of the real username.
- CSCsa75865—The radio interface no longer fails and reloads firmware when multiple bssids are enabled and the beacon period is configured for the minimum setting, 20 kilomicroseconds.
- CSCsa76923—The access point no longer sends out deauthentication frames with zero MAC addresses in the source and BSSID fields during a WLSE controlled scan.
- CSCsa77487—After an access point radio scan controlled by a WLSE running software release 2.11, the transmit power is no longer set to -1 dBm on the RM22A 802.11a radio module in 1200 series access points and the 802.11a radio in 1130AG access points.
- CSCed75294—SCHED-3-STUCKMTMR tracebacks no longer appear in Dot11 aaa process.
- CSCeg87732—**show snmp mib ifmib if index** command no longer returns different ifindex values.
- CSCeh30775—Intel 2100 card no longer drops data when CMIC is enabled.
- CSCeh46596—**show dot11 association** command returns correct infrastructure client state.
- CSCeh50286—The dot11 arp cache frees memory when a client disassociates.
- CSCeh59709 (duplicate of CSCeh54960)—Short slot time no longer enables after rebooting.
- CSCeh59723—Shared authentications are now allowed on more than one SSID.
- CSCeh68031—Broadcast storms no longer cause I/O memory depletion on 350 series access points.
- CSCeh68511—Radius VLAN assignments now work with WPA/TKIP.
- CSCeh80318—1200 series access point no longer fails to upgrade the radio firmware.
- CSCeh88870—Infrastructure SSID can now be set using the GUI for a 1200 series access point in workgroup bridge mode
- CSCei02959—GUI and CLI differences for allowed SSID characters is corrected.
- CSCei12722—Access point authentication requests are correct when MBSSID is enabled.
- CSCei18019—Wireless client IP address now learned when Layer 3 Mobility enabled on the access point and mobility trust enabled on the tunnel.
- CSCsa53672—Console history buffer now operates correctly when connected via WLSM console port.
- CSCsa81364—Access point no longer adds two sets of IP/GRE headers if tunnel IP address not resolved.
- CSCsa85447—AES-CCMP messages are no longer replayed when a 1200 series access points reassociates with a 1200 series access point in workgroup bridge mode.
- CSCsa87643—Access point no longer crashes when configuring subinterfaces on the CLI.
- CSCsa90418—WDS access points no longer fail to communicate with WLSE.
- CSCsb04359—NTP configurations are replaced by SNTP configurations.
- CSCsb06768—350 series access points no longer experience high CPU, CPU Hog messages, or watchdog timeouts.

- CSCsb08986—An error message displays when entering 25 characters for a 128-bit WEP key.
- CSCsb12321—The access point bridge table is now correct when a workgroup bridge roams.
- CSCed49127—AAA method list and server group configurations now function normally on reload.
- CSCeg51714—MIC errors no longer occur during FTP session.
- CSCeh71021—Neighbor TLV CDP support has been added to this release.
- CSCsa67267—The **mbssid** and **no mbssid** commands function properly.
- CSCeg45312—Sequence number mismatch no longer occurs for mail protocols.
- CSCeg57140—RADIUS accounting no longer sends incorrect values in ACCT_SESSIONTIME/INPUTPACKET.
- CSCeh03467—Memory leak no longer occurs when logging sync is enabled on the console.
- CSCeh50826—Dot11 arp cache now frees memory when a client disassociates.
- CSCeh54673—EAP-FAST via local RADIUS no longer fails with CCX supplicants.
- CSCsa81634—Access point no longer adds 2 sets of IP/GRE headers when unable to resolve the tunnel IP address.
- CSCsa98961—dot11RetryCount values now increase properly.
- CSCsb27021—Access point software now refers to the correct antenna.
- CSCsa73840 (duplicate of CSCsa55601)—Memory leak no longer occurs when SWAN is enabled using **wlccp ap user <> pass <>** CLI command.
- CSCsb06313 (duplicate of CSCed18557)—Memory leak no longer occurs.

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find select caveats of any severity. Click this URL to browse to the Bug Toolkit:

<http://tools.cisco.com/Support/BugToolKit/>

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/cisco/web/support/index.html>. Click **Technology Support**, choose **Wireless** from the menu on the left, and click **Wireless LAN**.

Documentation Updates

This section lists changes, errors, and omissions from user documentation for access points.

Related Documentation

This section lists documents related to Cisco IOS Release 12.3(7)JA and to 350, 1100, 1130AG, 1200, and 1240AG series access points.

- *Cisco Aironet Conversion Tool for Cisco IOS Software, 2.0 Administrator Guide for Windows*
- *Quick Start Guide: Cisco Aironet 350 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1100 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1130AG Series Access Points*
- *Quick Start Guide: Cisco Aironet 1200 Series Access Points Running Cisco IOS Software*
- *Quick Start Guide: Cisco Aironet 1240AG Series Access Points*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *Hardware Installation Guide for Cisco Aironet 350 Series Access Points Running Cisco IOS Software*
- *Cisco Aironet 1100 Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1130AG Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1200 Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*
- *Installation Instructions for Cisco Aironet Power Injectors*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.