



# Release Notes for Cisco Aironet 350, 1100, 1130AG, 1200, and 1230AG Series Access Points for Cisco IOS Release 12.3(4)JA

---

April 4, 2005

These release notes describe features, enhancements, and caveats for Cisco IOS Release 12.3(4)JA. They also provide important information about Cisco Aironet 350, 1100, 1130AG, 1200, and 1230AG series access points.

## Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Updates to Existing Features, page 5](#)
- [New Features, page 6](#)
- [Installation Notes, page 7](#)
- [Important Notes, page 10](#)
- [Caveats, page 17](#)
- [Troubleshooting, page 22](#)
- [Documentation Updates, page 22](#)
- [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**

Copyright © 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, and 1200 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(4)JA on all 1100 series access points, 1130AG access points, and on 1230AG access points.



### Note

Software upgrades fail when you use the web-browser interface to install Cisco IOS Release 12.3(4)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 1200 series 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](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:

1. Follow this link to the Cisco Aironet Install and Upgrade page:  
[http://www.cisco.com/en/US/products/hw/wireless/ps430/tsd\\_products\\_support\\_install\\_and\\_upgrade.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/tsd_products_support_install_and_upgrade.html)
2. Click this link to browse to the Cisco IOS Software Center on Cisco.com:  
<http://www.cisco.com/cisco/software/navigator.html>  
Log into Cisco.com to use the Cisco IOS Upgrade Planner.

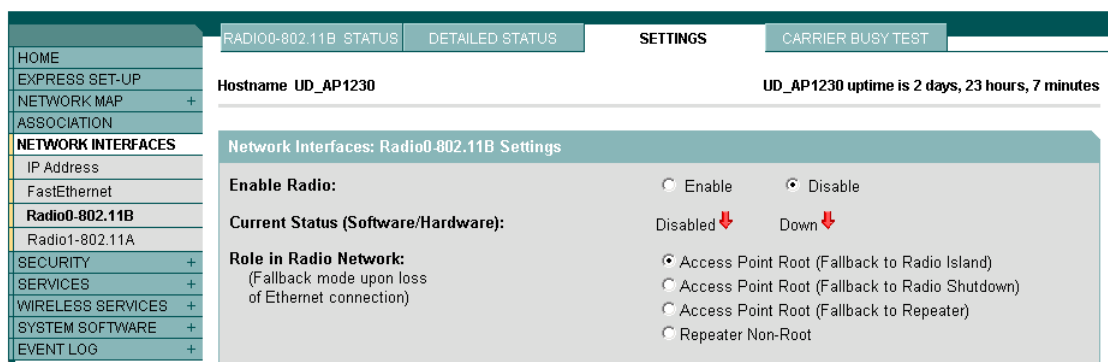
## Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

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
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>interface dot11radio {0   1}</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
<b>Step 3</b>	<b>shutdown</b>	Disable the radio port.
<b>Step 4</b>	<b>end</b>	Return to privileged EXEC mode.
<b>Step 5</b>	<b>copy running-config startup-config</b>	(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, 2.1 Administrator Guide for Windows*. Click this link to browse to the Administrator Guide:

[http://www.cisco.com/en/US/docs/wireless/access\\_point/conversion/ios/administration/guide/tool3ios.html](http://www.cisco.com/en/US/docs/wireless/access_point/conversion/ios/administration/guide/tool3ios.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
```

## Updates to Existing Features

Table 1 lists updates to existing features in Cisco IOS Release 12.2(15)XR and earlier. Cisco IOS Software Release 12.3(4)JA includes these updates for these features and platforms.

**Table 1** Updates to Existing Features in Cisco IOS Release 12.3(4)JA

Existing Feature	1100 Series	1130AG Series	1200 Series	1230AG Series
IP-Based Wireless Domain Services (WDS)	x	x	x	x
Layer 3 Mobility Service via Fast Secure Roaming Tunnels	x	x	x	x
Work Group Bridge (WGB) Mode	x	—	x <sup>1</sup>	x <sup>1</sup>
SNMPv3	x <sup>1</sup>	x <sup>1</sup>	x <sup>1</sup>	x <sup>1</sup>

1. Support for existing feature added in this release.

## New Features

This section lists new features in Cisco IOS Release 12.3(4)JA. [Table 2](#) lists the features that are supported on the devices that support this release.

**Table 2** *New Features Introduced for Access Points in Cisco IOS Release 12.3(2)JA*

Feature	350 Series	1100 Series	1130AG Series	1200 Series	1230AG Series
Support for multiple BSSIDs (mBSSID)	–	x <sup>1</sup>	x	x <sup>2</sup>	x
Support Wi-Fi 802.11h and Dynamic Frequency Selection (DFS)	–	–	x	x	x
Wireless IDS - Excess Management Frame Detection	–	x	x	x	x
Wireless IDS - Authentication Attack Detection	–	x	x	x	x
Frame Monitor Mode	–	x	x	x	x
Location Based Services	–	x	x	x	x

1. Supported only on units that contain 802.11g radios.

2. Supported only on units that contain 802.11g radios or RM21/22A 5-GHz radio modules.

## Support for Multiple Basic Service Set IDs

This feature permits a single access point to appear to the WLAN as multiple virtual access points. It does this by assigning an access point with multiple Basic Service Set IDs (MBSSIDs) or MAC addresses.

To determine whether a radio supports multiple basic SSIDs, enter the **show controllers** command for the radio interface. The radio supports multiple basic SSIDs if the results include this line:

```
Number of supported simultaneous BSSID on radio_interface: 8
```

## Wi-Fi 802.11h and Dynamic Frequency Selection Support

This feature allows Cisco access points configured at the factory for use in Europe and Singapore to detect radar signals such as military and weather sources and switch channels on the access points.

## Wireless IDS – Excess Management Frame Detection

This feature provides scanner access points the ability to detect that WLAN management and control frames exceeded a configurable threshold.

## Wireless IDS – Authentication Attack Detection

This feature requires Cisco access points to detect and report on excessive attempted or failed authentication attempts (Authentication failure detection and Excess EAPoL authentication).

## Frame Monitor Mode

This feature requires a Scan-only access point to forward all 802.11 frames seen to a protocol analysis station for network troubleshooting from remote sites via partner applications or partner Intrusion Detection companies or both.

## Location Based Services (LBS)

This feature enables a Cisco access point to detect frames from LBS tags and send them to a pre-configured IP destination such as a third-party LBS server.

## SNMPv3

This feature enables SNMPv3 support on Cisco access points to provide an additional level of security.

## WGB Mode on 1200 Series Access Points

This feature allows 1200 series access points to support Work Group Bridge (WGB) functionality on either the 802.11b/g or 802.11a radio.

## Installation Notes

This section contains information you should keep in mind when installing 350, 1100, and 1200 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, 1130, and 1200 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 24 to 60 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.

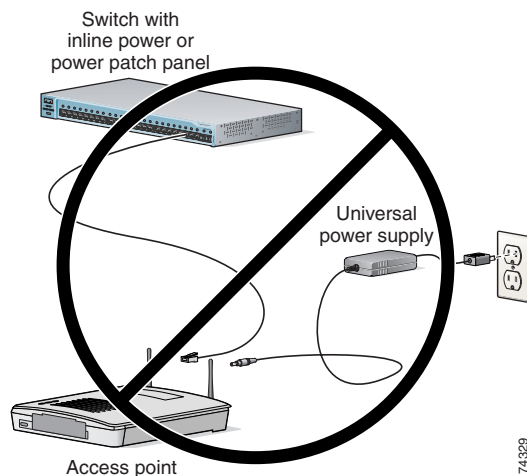
**Caution**

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, 1130, 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 Access Points

The 1130AG access point disables 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)

Apply

121655

### Using the AC Power Adapter

If you use the AC power adapter to provide power to the 1130AG 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 1130AG 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 1130AG 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 1130AG 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 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.

## SNTP Replaces NTP

In Cisco IOS Release 12.3(4)JA, access points and bridges support SNTP instead of NTP. This change improves the reliability of the system time on access points and bridges, allows access points and bridges to synchronize with any NTP server, and prevents client devices from synchronizing to an access point or bridge clock that might not be accurate.

## 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.

## 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.

## 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 and Singapore 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.

## Proxy Mobile-IP Feature Removed

The proxy Mobile-IP feature is not supported in Cisco IOS Releases 12.3(2)JA and 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 3 lists 802.11a transmit power settings in mW and the power settings that the access point assigns to a new radio module.

**Table 3** *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](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 mode button 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 HTTP 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](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", ip1= 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 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.

## 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, or 1200 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.

## Caveats

This section lists [Open Caveats](#) and [Resolved Caveats](#) in Cisco IOS Release 12.3(4)JA.

### Open Caveats

These caveats are open in Cisco IOS Release 12.3(4)JA:

- CSCeb52431—When logging into a TACACS+ server, 1100 series access points sometimes send hundreds of additional authentication requests to the server after a successful authentication.
- CSCef11167—The access point sometimes returns an inaccurate value when you poll cDot11ActiveWirelessClients through SNMP.
- CSCef95410—When an access point is configured to interact with a WDS device, the WLCCP packets that it receives from the WDS device sometimes cause the radio interface output drop counter to increment when it should not.
- CSCeg19614—When a 1200 series access point is configured as a workgroup bridge, it does not display the client devices attached to its Ethernet port.
- CSCeh38024—Access point WPAv2 migration mode does not support Cisco Aironet CB20A client radios running firmware version 2.0.0.184 configured for optional WPAv2.

Workaround: Configure the access point for WPAv2 with TKIP + WEP40/128, or configure the access point for mandatory WPAv2.

- CSCsa44859—350 series access points sometimes display tracebacks when you configure a VLAN and do not assign an SSID to it.

Workaround: Use the CLI to create VLANs on 350 series access points.

- CSCsa45650—The 802.11b radio interface in 1200 series access points sometimes reports its MAC address as 000000000000 on both the GUI and through SNMP. However, the CLI displays the correct MAC address in output for the **show cont d0** command.

Workaround: Use the **show cont d0** command to find the correct MAC address for the 802.11b radio interface.

- CSCsa62900—Spectralink phones configured for fast secure roaming sometimes require up to 10 minutes to register with the call manager.
- CSCsa67267—The **mbssid** command sometimes fails on the CLI and the GUI.

Workaround: If the **mbssid** command fails, disable the radio interface and try the command again.

- CSCsa68532—The results in the Strength %Out field and the Strength dBm field are reversed when you run a link test from an access point.
- 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.
- CSCsa69480—When the access point radio interfaces are in the reset and down state, the GUI operates slowly. The reset and down state occurs when VLANs are configured but no SSIDs have been configured.

Workaround: If you plan to configure several VLANs before configuring SSIDs, avoid the reset and down state by disabling the radio interfaces before you configure the VLANs.

- CSCsa71233—When you configure an 1100 series access point for LEAP authentication and hot standby, the standby access point sometimes reboots when it authenticates to the monitored access point. After it reboots it operates correctly in standby mode.
- CSCsa74148—Existing SSIDs become invalid when you configure VLANs for the first time. When no VLANs are configured, encryption is applied to the radio interface, but when you configure VLANs, encryption is applied to the VLANs.
- CSCsa74153—WPAv2 accounting start/stop records sometimes 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 sometimes fails and reloads firmware when multiple BSSIDs are enabled and the beacon period is configured for the minimum setting, 20 kilomicroseconds.

Workaround: Increase the beacon period.

- CSCsa76662—When multiple BSSIDs are configured, the access point does not send the secondary SSIDL information element (IE) in beacons. However, the access point still sends the SSIDL IE in broadcast probe responses.

Workaround: If multiple BSSIDs are configured on the access point, disable the SSIDL feature.

- CSCsa76923—During an access point radio scan controlled by WLSE, the access point sometimes sends out several deauthentication frames with zero MAC addresses in the source and BSSID fields. This problem wastes bandwidth on the wireless LAN but has no other adverse effects.
- CSCsa77487—After an access point radio scan controlled by a WLSE running software release 2.11, the transmit power is sometimes 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. The problem occurs after an active access point scan, which starts when you select **run now** on the WLSE interface. The problem does not occur after scheduled scans. You must manually reconfigure the transmit power setting on the affected radio.

## Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.3(4)JA:

- CSCeb82510—You can now configure authentication, authorization, and accounting (AAA) methods for telnet and HTTP independent of the console.
- CSCec12884—The AAA user command authorization no longer fails through HTTP access.
- CSCee42617—Users are now correctly authenticated through the RADIUS server, and accounting information is sent to the RADIUS server.
- CSCee87287—Access points no longer fail to generate accounting records when a wireless client is re-authenticated on an automatic interval (for example, when the access point is configured using the **dot1x reauthentication seconds** command).
- CSCee93036—Access points now support the **archive upload rcp:/hostname/file-path** command.
- CSCef43007—Logging system messages to the console is now disabled by default on 1100 series access points.
- CSCef50742—Clients no longer fail 802.1X authentication through Cisco Catalyst 2950 and 3750 switches due to changing State (24) Field values.
- CSCef60659—A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef65076—The access point GUI no longer reports a Bad Request error when you enter a RADIUS server hostname on the access point.
- CSCef75364—350 series access points now support the **exception crashinfo** command.
- CSCef78627—The access point no longer reports an incorrect transmit power value for the 802.11a radio when you change the external antenna position from high-gain to low-gain or from low-gain to high-gain while the access point is on.
- CSCef89795—Access points no longer send IAPP traffic on the wrong VLAN when layer 3 mobility is enabled.
- CSCeg01125—The **show crypto engine qos** command no longer reboots the access point when SSH is enabled.
- CSCeg42686—Client devices using 5-GHz radios now successfully communicate with the access point at up to 54 Mbps.
- CSCeg64999—Access points now support EAP-SIM authentication.
- CSCeg70288—On 1200 series access points, tracebacks no longer occur when you enter the **no dot11 arp-cache** command when ARP caching is already disabled.
- CSCeg81122—You can now use the access point GUI to upload a configuration file larger than 9 KB.
- CSCeg82564—The **encryption mode cipher** command now requires you to specify a cipher.
- CSCeg84849—Access points now correctly add a configured IP address to the *env\_vars* file.
- CSCeh06200—With TACACS configured, administrators can now log into the access point GUI when idle time is configured on the TACACS server.
- CSCeh08952—Access points now correctly filter traffic through the TCP port when an IP filter is configured.
- CSCeh09384—Access points with 5-GHz radios no longer display this error when a client device associates using WPA-LEAP:

```
*Mar 1 00:55:20.083: %DOT11-4-TKIP_MIC_FAILURE_REPORT: Received TKIP Michael MIC
failure report from the station 000a.b7df.1943 on the packet (TSC=0x7507000000000000)
encrypted and protected by group key.
```

- CSCsa40861—Access points configured for a fallback role now assume the fallback role if the LAN interface is down when they reboot.
- CSCsa48698—Access points now correctly block associations from client devices denied access through the **dot11 association** command.
- CSCsa50495—Client devices using the Soliton 1xGATE EAP supplicant can now authenticate when an access point switches from a failed WDS device to a fallback WDS device.
- CSCsa50951—Access points no longer reach maximum CPU usage when you poll or query them using an SNMP walk utility.
- CSCsa51868—When a client device sends an ARP request to an access point configured for ARP caching, the access point no longer indicates that the client IP address is mapped to the access point MAC address.
- CSCsa52462—Access points configured for CKIP or CMIC now indicate CKIP and CMIC support in beacons.
- CSCsa54203—An access point configured as a backup WDS device no longer reboots when it becomes the primary WDS device.
- CSCsa59600—A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCsa57777—The **no speed** command now removes the data rates that you specify from the configuration.

## 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.

## Omissions

Access point quick start guides do not yet describe these features:

- Changes to the default configuration—In the default configuration for this release, there is no default SSID and the radio interface is disabled by default. You must create an SSID and enable the radio interface before the access point allows wireless associations from other devices.
- Default IP address behavior—When you connect a 350, 1130AG, 1310, or 1200 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.

## Related Documentation

This section lists documents related to Cisco IOS Release 12.2(15)JA and to 350, 1100, and 1200 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 1200 Series Access Points*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *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](http://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.