



Release Notes for Cisco Aironet 350, 1100, and 1200 Series Access Points for Cisco IOS Release 12.2(13)JA4

April 19, 2004

Cisco IOS Release 12.2(13)JA4 resolves caveats CSCdz32659, CSCed27956, CSCed38527, and CSCed40563 but does not introduce new features. These release notes describe caveats for Cisco IOS Release 12.2(13)JA4 and features and enhancements introduced in Cisco IOS Release 12.2(13)JA.

Contents

These release notes contain the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Installation Notes, page 6](#)
- [Important Notes, page 8](#)
- [Caveats, page 13](#)
- [Troubleshooting, page 17](#)
- [Related Documentation, page 18](#)
- [Obtaining Documentation and Submitting a Service Request, page 18](#)

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.



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

You can configure and monitor 1100, and 1200 series access points using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

System Requirements

You can install Cisco IOS Release 12.2(13)JA4 on all 1100 series access points and on model AP1230 access points.

You can also convert 350 and 1200 series access points that run VxWorks to run Cisco IOS software. After the conversion, you can install Cisco IOS Release 12.2(13)JA4 on 350 and 1200 series access points.

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.

To install Cisco IOS software on access points that do not run IOS software, use the conversion utility to convert to IOS software without losing your current configuration. To convert to IOS software without saving your configuration, load the conversion upgrade image. The access point reboots with IOS software and factory default settings.

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 to IOS software.

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(11)JA1:

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(11)JA1
Copyright (c) 1986-2003 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
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 or 12.2(11)JA1, your access point might unexpectedly reboot after you upgrade to Cisco IOS Release 12.2(13)JA4. 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 to Cisco IOS Release 12.2(13)JA4. See the “[Disable Radio Interfaces When Upgrading from Cisco IOS Release 12.2\(11\)JA to 12.2\(13\)JA4](#)” section on page 8 for instructions on disabling the radio interfaces.

Converting to Cisco IOS Software

If your 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:

- 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T

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 using the upgrade image or the conversion tool.

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

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 1200 series access points. You can also download instructions for using the utility and the image.

**Note**

The upgrade to Cisco IOS software is permanent. You cannot revert to VxWorks software after the upgrade. Product warranties do not cover unintended upgrades.

New Features

Cisco IOS Release 12.2(13)JA4 does not provide any new features but supports all the features of the previous software release.

This section lists new features in Cisco IOS Release 12.2(13)JA for access points. [Table 1](#) lists the features that are supported on the devices that support this release.

**Note**

Cisco Aironet 1400 Series Wireless Bridges do not support any of the new features in this release. This release provides only caveat resolution support for 1400 series bridges.

Table 1 *New Features Introduced in Cisco IOS Release 12.2(13)JA for Access Points*

Feature	350 Series Access Points ¹	1100 Series Access Points	1200 Series Access Points
Radio management	x	x	x
Radio Management Aggregation	—	x	x
Support for IEEE 802.11g radio	—	x	x
Client ARP caching	x	x	x
Wi-Fi Alliance Wireless ISP Roaming (WISPr) RADIUS Attributes	x	x	x
Transmit Power Control (TPC)	x	x	x
RADIUS server per SSID	x	x	x

1. Cisco Aironet 350 Series Access Points support the same feature set as an 1100 series access point running Cisco IOS Release 12.2(11)JA, except that a 350 series access point cannot serve as a WDS access point.

Radio Management

This feature allows a Cisco Aironet access point to take radio measurements and continuously scan and monitor the radio frequency environment.

Radio Management Aggregation

This Wireless Domain Services (WDS) feature enables various Cisco Structured Wireless-Aware Network (SWAN) capabilities, including rogue access point detection and location, radio frequency interference detection, the assisted site survey tool, and future enhancements.

IEEE 802.11g Wireless Standard

This feature provides support for the IEEE 802.11g standard for wireless networking using 802.11g access point radio modules.

Client ARP Caching

This feature allows Cisco Aironet access points to respond to Address Resolution Protocol (ARP) requests on behalf of IEEE 802.11 Cisco and Cisco-compatible wireless client devices. This feature enables IP address resolution without requiring the Cisco and Cisco-compatible wireless client device to leave power save or idle modes, resulting in extended client device battery life.

Wi-Fi Alliance Wireless ISP Roaming (WISPr) RADIUS Attributes

This feature supports the Location-ID and Location-Name RADIUS vendor-specific attributes (VSAs) recommended by the Wi-Fi Alliance WISPr hot-spot service provider roaming initiative. These VSAs are used in public-access networks to support roaming billing arrangements between service providers.

Transmit Power Control (TPC)

This feature supports Transmit Power Control (TPC) for Cisco Aironet access points. TPC is used by Cisco Aironet access points to relay transmit power information to Cisco and Cisco-compatible wireless client devices. Client devices use the TPC information in conjunction with the access point's signal strength to calculate path loss and the transmit power necessary for the client to reach the Cisco Aironet access point. This feature extends client device battery life.

RADIUS Server per SSID

This feature allows for RADIUS servers to be specified for each SSID. This feature benefits multi-tenant sites such as airports and deployments where a separate server for different authentication methods is desirable.

Installation Notes

This section contains information you should keep in mind when installing 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 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 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.

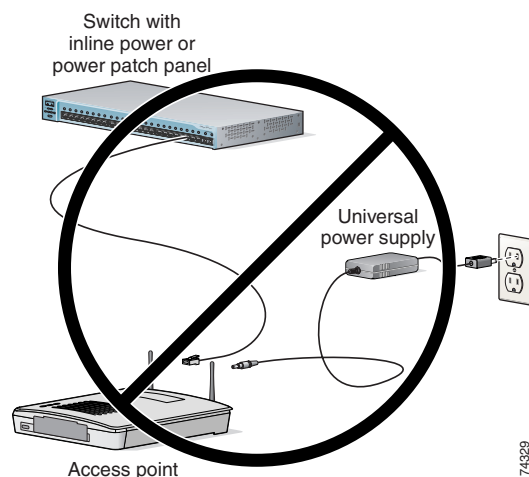
**Caution**

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 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 1](#) shows the power configuration that can shut down the port on the patch panel or powered switch.

Figure 1 *Improper Power Configuration Using Two Power Sources*



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.

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.

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.

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.

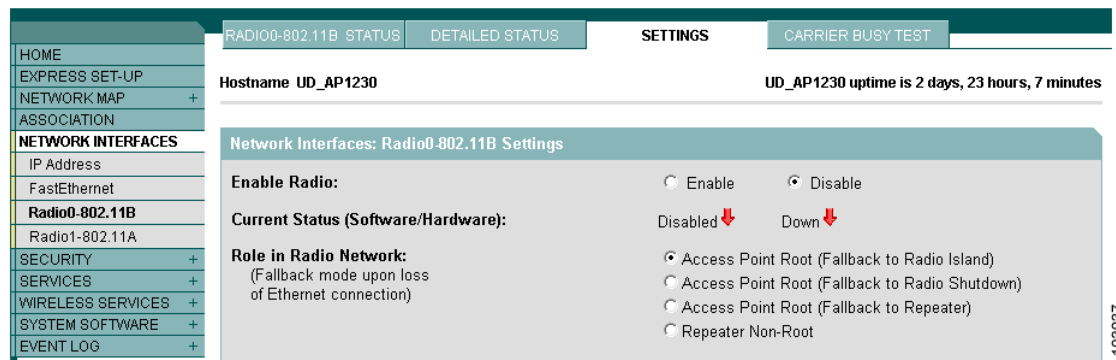
Disable Radio Interfaces When Upgrading from Cisco IOS Release 12.2(11)JA to 12.2(13)JA4

If your access point runs Cisco IOS Release 12.2(11)JA or 12.2(11)JA1 the access point might reboot immediately after you upgrade to Cisco IOS Release 12.2(13)JA4. 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, when the access point reboots after the crash, the upgrade is complete and the access point operates normally. To prevent the access point from rebooting unexpectedly, disable the radio interfaces before upgrading to Cisco IOS Release 12.2(13)JA4.

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

- Step 1** Browse to the Network Interfaces: Radio Settings page. [Figure 2](#) shows the top portion of the Network Interfaces: Radio Settings page.

Figure 2 Network Interfaces: Radio Settings Page



- Step 2** Click **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 port.

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.

System Software Upgrade Sometimes Fails Due to Insufficient Memory

When you use the web-browser interface to upgrade access point system software, this error might appear:

```
ERROR: Not enough system memory for HTTP upgrade.
```

This error indicates that your access point or bridge does not have enough free processor memory to transfer the entire system image over HTTP. The memory shortage might be caused by memory fragmentation, which can happen over long-term operation of the unit, or by features that require significant memory, such as WDS. To complete the upgrade using the web-browser interface, free the required memory by disabling the radio interfaces and high memory-usage features such as WDS, and reboot the access point. After the access point reboots, try the upgrade again.



Note If you use the CLI to disable access point features, remember to save the configuration to flash memory before rebooting.

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 Not Running IOS Software

Repeater access points running Cisco IOS software cannot associate to parent access points that do not run IOS software (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 version 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

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 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.

Caveats

This section lists [Open Caveats](#) and [Resolved Caveats](#) in Cisco IOS Release 12.2(13)JA4.

Open Caveats

These caveats are open in Cisco IOS Release 12.2(13)JA4:

- CSCeb02792—The 802.11a radio in 1200 series access points sometimes erroneously reports 100% busy for all frequencies when you run the Carrier Busy test.
- 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.
- CSCeb50727—Unpowered 1100 series access points sometimes cause a loopback when connected to switches without loopback detection. When you connect an unpowered 1100 series access point to some switches without loopback detection, the access point sometimes 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.
- CSCec02800—The access point web-browser interface sometimes displays cached information for the Associations page and does not list all associated client devices.

Workaround: Refresh the Associations page in the web-browser interface to display current client associations.

- CSCec23329—Access points with PMIP enabled sometimes misinterpret an ARP sent by some client devices that check to make sure that their IP addresses are not in use. When the access point receives the ARP from the client, the access point interprets the ARP as a DHCP request and disables PMIP for the client session.

Workaround: If possible, disable the feature on the client device that automatically sends an ARP to the access point to check IP address availability.

- CSCec25559—When both 802.11g and 802.11a client devices transmit data simultaneously to the 802.11g and 802.11a radios in a 1200 series access point, the throughput of the 802.11a radio might decrease.

- CSCec28612—ACL logging is not supported on access point radio interfaces. You must remove the **log** option from the command for the ACL to take effect. However, ACL logging is supported on access point BVI interfaces.
- CSCec33268—When the access point is configured for optional or mandatory WPA authentication, client adapters in Windows XP platforms sometimes experience a delay when initially authenticating to the access point immediately after it starts up.
- CSCec33519—Administrative users assigned the **admin-capability** attribute sometimes cannot log into the access point using Telnet.
- CSCec43008—When you update a WEP key using SNMP, the access point radio does not restart automatically, and the access point continues to use the old WEP key.

Workaround: Restart the access point radio after using SNMP to update a WEP key.

- CSCec43849—When you configure your access point for MAC address authentication for a large number of MAC addresses, client devices sometimes experience long delays when several clients roam from one access point to another at the same time.
- CSCec55763, CSCec55820—When both the 802.11g and 802.11a radios in a 1200 series access point simultaneously operate under extremely high data loads for an extended period, the 802.11a radio sometimes hangs or the access point reboots.
- CSCec59848—The access point uses only multiples of 8 for the Max Data Retries setting on the 802.11g radio. If you set the Max Data Retries setting to a value that is not a multiple of 8, the access point rounds down to the closest multiple of 8. For example, if you set Max Data Retries to 20, the access point rounds the setting down to 16.
- CSCec60868—Changing the TKIP MIC failure holdoff time to a non-default value triggers the holdoff timeout in these situations:
 - Immediately after you set the timeout to a non-default value, the holdoff timeout is in effect and clients cannot associate for the specified holdoff period. However, if you set the holdoff timeout to the default value (60 seconds), the timeout is not triggered immediately after you set it.
 - When the access point reboots, the holdoff timeout is triggered and clients cannot associate until the timeout expires. However, the timeout is not triggered after a reboot if the timeout is set to the default value (60 seconds).
- CSCin60014—These invalid configurations cause radio errors:
 - WPA optional with the TKIP cipher
 - WPA mandatory with TKIP+WEP40
 - WPA mandatory with TKIP+WEP128

Configuring WPA is a two step process and the access point can be in an invalid configuration when client devices associate resulting in radio errors. This invalid condition occurs when the access point is changed from a WPA mandatory configuration to a WPA optional configuration or vice versa.

Workaround: To prevent client devices from associating to the access point during the invalid WPA configuration period, you must deactivate the radio prior to changing the configuration and reactivate the radio when the configuration changes are complete.

- CSCec72841—The ARP cache feature is not supported on repeater access points.
- CSCec73044—When WPA is configured on the access point, associated client devices occasionally report MIC failures on packets from the access point.
- CSCec73037—Packet replay detection messages occasionally appear when a WPA client reauthenticates to the access point. The client sometimes loses its connection to the access point, but the client attempts to reconnect.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.2(13)JA4:

- CSCdz32659—Memory allocation failure (MALLOCFAIL) messages no longer occur for Cisco Discovery Protocol (CDP) processes.

- CSCed27956—

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed38527—

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed40563—Problems with the CDP protocol have been resolved.

These caveats are resolved in Cisco IOS Release 12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, and 12.2(13)JA3:

- CSCed21588—Access points no longer disassociate client devices when WEP is enabled on the access point.
- CSCed26579—When you upgrade a 1200 series access point in the EMEA regulatory domain from VxWorks to Cisco IOS software, the upgrade no longer changes the maximum transmit power on the 2.4-GHz radio to 100 mW.
- CSCed50731—Access points using 802.11g data rates and with security enabled (WEP, LEAP, or EAP) no longer report decryption errors.
- CSCec55720—The access point now allows multiple IEEE 802.11b clients to simultaneously associate without losing connectivity to some of the clients.
- CSCec85569—The access point radio firmware correctly reads the IEEE 802.11b radio power tables and no longer causes the radio to become inoperable.
- CSCdx45005, CSCeb84981, CSCeb87018—SSH now operates correctly with RADIUS authentication and authorization.
- CSCea79363, CSCec03974, CSCec09390—The Compaq Wireless LAN Multiport W200 client device now associates successfully to 1100 or 1200 series access points.
- CSCea82021—When DNS is configured on the access point, the show running-config command sometimes displays a server's IP address instead of its name. This expected behavior is now accurately described in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.
- CSCea88706, CSCeb51208, CSCec03118, CSCec16687, CSCec16708—You can now modify existing MAC address and EtherType filters on the access point web-browser interface.
- CSCea88862—You can now run a link test using thousands of packets on the web-browser interface.
- CSCea89985—The access point no longer generates a traceback when you configure hot standby mode using a broadcast MAC address to specify the access point to be monitored.
- CSCea91378—When you run a carrier busy test on the web-browser interface when the access point radio is disabled, the web-browser interface no longer reports that the test failed.
- CSCea91424—When a CCKM client device roams successfully to a foreign network using proxy Mobile IP, the access point no longer displays error messages.
- CSCeb06139—When several mobile clients are using Cisco Centralized Key Management (CCKM), the access point no longer reboots when you enter the **show wlccp wds mn detail** command.
- CSCeb15588—The access point now accepts the *aironet* RADIUS attribute in the Cisco vendor-specific attribute (VSA), and the Cisco PEAP supplicant now works correctly with Cisco ACS version 3.1.1.
- CSCeb36095—Access points running Cisco IOS software now send the same RADIUS NAS-port-type value as access points running VxWorks.
- CSCeb36192—The access point now assigns user VLANs correctly whether or not multiple SSIDs are configured.
- CSCeb39541—The default EAP client timeout (the length of time that the access point waits for a client to respond to the access point's EAP request) has changed from 10 seconds to 30 seconds.
- CSCeb47892—You can now use the web-browser interface to disable the access point radio after setting the role in radio network to **Access Point Root (Fallback to Radio Shutdown)**.

- CSCeb48645—Client devices in power-save mode no longer lock up when associated to an access point running Cisco IOS software.
- CSCeb52239, CSCec20465—The access point now correctly assigns VLANs to devices connected to a workgroup bridge.
- CSCeb60581—The access point now sends the correct username with RADIUS accounting packets.
- CSCeb69596—You can now enter the letters in MAC addresses using either upper-case or lower-case letters when using the web-browser interface to configure MAC-address filtering or authentication.
- CSCeb76171—The web-browser interface now displays pages correctly when a message-of-the-day (MOTD) banner is configured on the CLI.
- CSCeb79465—The access point with a spectralink wireless phone now sends buffered data.
- CSCeb87628—Client devices using PEAP authentication now authenticate successfully through the access point.
- CSCeb87982—The access point now correctly displays hot standby status and event messages.
- CSCec00308—Efficient Speedstream DHCP server now responds to Cisco IOS DHCP discover packets.
- CSCec07703—Cisco 7920 IP Phones no longer drop calls when associated to 1100 and 1200 series access points.
- CSCec12813—Client devices in power-save mode no longer lose packets when they wake up.
- CSCec15572—You can now use the **[no] boot upgrade** global configuration command to configure the access point to boot without loading a configuration.
- CSCec21082—The access point now reports accurate statistics for ifOutUcastPkts on radio interfaces.
- CSCec29293—The access point no longer immediately drops all client associations when you enter the **reload in minutes** command.
- CSCec39405—The following combination of radio settings no longer reduces throughput on the 802.11a radio in 1200 series access points:
 - Fragmentation threshold set to 500
 - RTS threshold set to 256
 - WPA enabled
- CSCec43028—The access point CLI no longer displays 40-bit WEP keys as 128-bit WEP keys.
- CSCin44512—If 8 or more VLANs are configured on your access point, you can now apply filters using the Apply Filters page in the web-browser interface.
- CSCin44591—PSPF now works when you use the web-browser interface to enable PSPF on a non-native VLAN.

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**.

Related Documentation

This section lists documents related to Cisco IOS Release 12.2(13)JA1 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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and 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 © 2004 Cisco Systems, Inc. All rights reserved.