



Release Notes for Cisco Aironet 350, 1100, and 1200 Series Access Points for Cisco IOS Release 12.2(15)JA

April 15, 2004

These release notes describe features, enhancements, and caveats for Cisco IOS Release 12.2(15)JA. They also provide important information about Cisco Aironet 350, 1100, and 1200 series access points.

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Installation Notes, page 6](#)
- [Important Notes, page 8](#)
- [Caveats, page 14](#)
- [Troubleshooting, page 19](#)
- [Related Documentation, page 19](#)
- [Obtaining Documentation and Submitting a Service Request, page 19](#)



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

Copyright © 2004 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 12.2(15)JA 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 IOS software.



Note

Software upgrades fail when you use the web-browser interface to install Cisco IOS Release 12.2(15)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 *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* on Cisco.com:

http://www.cisco.com/en/US/docs/wireless/access_point/12.2_15_JA/configuration/guide/s15mfw.html

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(13)JA2:

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(13)JA2
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.

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

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

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

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

Some Fields Not Updated During Upgrade to IOS Software

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

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

New Features

This section lists new features in Cisco IOS Release 12.2(15)JA. [Table 1](#) lists the features that are supported on the devices that support this release.

Table 1 *New Features Introduced for Access Points in Cisco IOS Release 12.2(15)JA*

Feature	350 Series ¹	1100 Series	1200 Series
Access Point Scanning-Only Mode	X	X	X
Client tracking	X	X	X
IEEE 802.11d World Mode Support	X	X	X
Cisco Compatible Extensions information element	X	X	X
MAC address local authentication	X	X	X
IEEE 802.1X Support for EAP-FAST	X	X	X

1. Cisco Aironet 350 Series Access Points support the same feature set as an 1100 series access point, except that a 350 series access point cannot serve as a WDS access point.

Access Point Scanning-Only Mode

This Cisco SWAN feature allows the access point to be set in a scanning-only mode where it scans the RF environment for other access points and unassociated 802.11 clients. In this mode, the access point does not transmit beacons, respond to probe requests, or support client device association. This mode allows the access point to function as an intrusion detection device to detect rogue (unauthorized) access points and unassociated 802.11 clients. Refer to the WLSE user documentation for instructions on enabling this feature. Click this link to browse to the WLSE user documentation:

<http://www.cisco.com/en/US/products/sw/cscowork/ps3915/index.html>

Client Tracking

This new WDS feature expands the radio management information gathered from Cisco Aironet access points to include information on client authentication and roaming events. This feature expands Cisco SWAN capabilities by providing near-real-time tracking of client associations with the CiscoWorks Wireless LAN Solution Engine (WLSE). Click this link to browse to the WLSE user documentation:

<http://www.cisco.com/en/US/products/sw/cscowork/ps3915/index.html>

IEEE 802.11d World Mode Support

The 802.11d standard for world mode is supported by Cisco Aironet access points in this release. World mode enables the access point to inform an 802.11d client device which radio setting the device should use to conform to local regulations. For instructions on enabling 802.11d World Mode, refer to *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* on Cisco.com:

http://www.cisco.com/en/US/docs/wireless/access_point/12.2_15_JA/configuration/guide/s15rf.html

This information element allows a Cisco Aironet access point to inform Cisco Compatible Extensions client devices about the Cisco Compatible release version that it supports.

MAC Address Local Authentication

With this new feature, you can configure the access point's local authenticator to allow MAC authentication for users on the access point. Up to 50 users can be supported with this release. For instructions on configuring your local authenticator for MAC authentication, refer to *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* on Cisco.com:

http://www.cisco.com/en/US/docs/wireless/access_point/12.2_15_JA/configuration/guide/s15rf.html

IEEE 802.1X Support for EAP-FAST

This Cisco Wireless Security Suite feature supports the IEEE 802.1X standard port-based authentication Extensible Authentication Protocol (EAP) type EAP-Flexible Authentication through Secure Tunneling (EAP-FAST). EAP-FAST can also be supported by access points running Cisco IOS Release 12.2(11)JA or later. For instructions on configuring your access points for EAP authentication, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* on Cisco.com:

http://www.cisco.com/en/US/docs/wireless/access_point/12.2_15_JA/configuration/guide/s15rf.html

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 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.

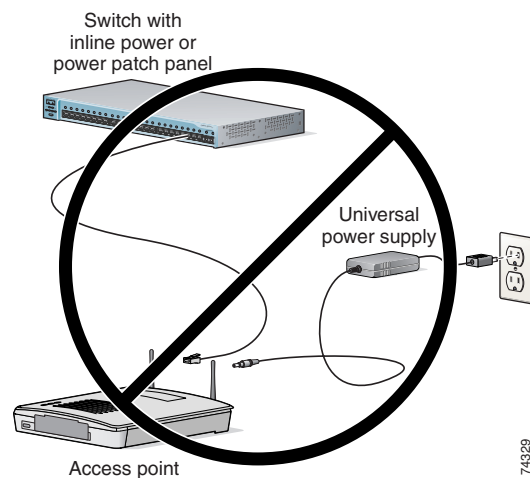
**Caution**

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 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.

TFTP Required to Upgrade 1200 Series Access Points to this Release

Software upgrades fail when you use the web-browser interface to install Cisco IOS Release 12.2(15)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 *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* on Cisco.com:

http://www.cisco.com/en/US/docs/wireless/access_point/12.2_15_JA/configuration/guide/s15mfw.html

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.

New Express Security Page Simplifies Security Setup

The new Express Security page in the access point web-browser interface makes it easier to create SSIDs and assign security settings to them. [Figure 2](#) shows the Express Security page.

Limitations of the Express Security page include:

- You cannot edit SSIDs. However, you can delete SSIDs and re-create them.
- You cannot assign SSIDs to specific radio interfaces. The SSIDs that you create are enabled on all radio interfaces. To assign SSIDs to specific radio interfaces, use the Security SSID Manager page.

- You cannot configure multiple authentication servers. To configure multiple authentication servers, use the Security Server Manager page.
- You cannot configure multiple WEP keys. To configure multiple WEP keys, use the Security Encryption Manager page.
- You cannot assign an SSID to a VLAN that is already configured on the access point. To assign an SSID to an existing VLAN, use the Security SSID Manager page.
- You cannot configure combinations of authentication types on the same SSID (such as MAC address authentication and EAP authentication). To configure combinations of authentication types, use the Security SSID Manager page.

For complete instructions on using the Express Security page, see the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* on Cisco.com:

http://www.cisco.com/en/US/docs/wireless/access_point/12.2_15_JA/configuration/guide/s15mfw.html

Figure 2 Express Security Page

Express Security Set-Up

SSID Configuration

1. SSID Broadcast SSID in Beacon

2. VLAN

No VLAN Enable VLAN ID: (1-4095) Native VLAN

3. Security

No Security

Static WEP Key

Key 1 128 bit

EAP Authentication

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

WPA

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

SSID Table

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input checked="" type="radio"/>	tsunami	none	none	open	none		<input checked="" type="checkbox"/>

111856

Access Points Do Not Support Loopback Interface

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



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 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**.

Microsoft Patch Fixes WPA Authentication Delay

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. A patch from Microsoft resolves this issue. The patch is described in Microsoft Knowledge Base Article 826942.

Caveats

This section lists [Open Caveats](#) and [Resolved Caveats](#) in Cisco IOS Release 12.2(15)JA.

Open Caveats

These caveats are open in Cisco IOS Release 12.2(15)JA:

- 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.
- 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.
- 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.
- 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.

- 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.

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

- 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.
- CSCec73044—When WPA is configured on the access point, associated client devices occasionally report MIC failures on packets from the access point.
- CSCed02220—When you upgrade an access point from 12.2(13)JAx to 12.2(15)JA, this command becomes invalid:

```
wlccp wds ipaddr 228 interface BVI1
```

- CSCed42897—The access point sends a **get tlv** command when the MAC is enabled. However, the access point should send the **get tlv** command only when the MAC is disabled.
- CSCed60301—When you enable shared key authentication and TKIP on an SSID on a 1200 series access point, some client devices cannot associate using the SSID.
- CSCed63953—The access point information element always transmits the default QoS CWMin value for best effort regardless of the value that you enter for that setting.
- CSCed66461—Some dual-mode client devices (clients with both 802.11b and 802.11g radios) cannot associate to the access point when you change the access point's 802.11g radio from Best Throughput to Best Range.
- CSCed67615—When you configure filtering on the GUI, MAC address filtering sometimes fails when you allow all addresses except a range of specific MAC addresses.

Workaround: Use the CLI to configure multicast MAC address filtering on the bridge groups.

- CSCed75292—The access point radio sometimes reboots when a client device attempts to authenticate at the same time that you enter this command on the access point CLI:

```
show aaa user all
```

Workaround: Disable the access point radio before you enter the **show aaa user all** command.

- CSCed79096—The 1200 series access point reports its power need to a switch with power over Ethernet as 15.4 W instead of 7 W.
- CSCed83246—Access points do not send IGMP queries through the radio interface when a client device reassociates.
- CSCed84527—The access point sometimes deauthenticates roaming client devices when the 1 and 2 Mbps data rates are disabled on the access point.
- CSCed87190—When you click the **Best Throughput** button on the access point web-browser interface for 802.11g radios the access point sets all data rates to **Require**. This setting blocks association by 802.11b client radios and, because ERP protection is still enabled, does not provide the best throughput.

Workaround:

- For the best throughput on the 802.11g interface, set the CCK rates (1, 2, 5.5, and 11 Mbps) to **Disable**, and set the OFDM rates (6, 9, 12, 18, 24, 36, 48, and 54 Mbps) to **Require**. These settings block association from 802.11b clients but provide the best throughput.
 - For the best possible throughput while allowing association from 802.11b clients, set the CCK rates (1, 2, 5.5, and 11 Mbps) to **Require** and set the OFDM rates (6, 9, 12, 18, 24, 36, 48, and 54 Mbps) to **Enable**.
- CSCee16473—When the WDS access point sends an oversized radio management packet to the WLSE device, an entry similar to this example appears in the WLSE event log:

```
com.cisco.swan.lib.wlccp.WlccpParseException: truncated message: buffer
length=8000, encoded length=8390
```

You can ignore these messages.

- CSCee18627—If the access point is not configured as a local authenticator, the access point reboots when you enter the **clear radius local-server user user** command.
- CSCin62683—Client devices sometimes fail to report a potential rogue access point. When a client fails to authenticate through a potential rogue access point and then successfully authenticates through a non-rogue access point, the client sometimes fails to report the potential rogue access point.
- CSCin69971—You cannot use the web-browser interface to upgrade 1200 series access points to Cisco IOS Release 12.2(15)JA because of the access point's image-size restriction.

Workaround: Use TFTP to upgrade your 1200 series access points to this release. For complete instructions on using TFTP to upgrade access point software, see the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* on Cisco.com:

http://www.cisco.com/en/US/docs/wireless/access_point/12.2_15_JA/configuration/guide/s15mfw.html

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.2(15)JA:

- CSCec16481—A Cisco device running Cisco Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

The vulnerability is only present in Cisco IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all Cisco IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.

Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml>.

- CSCdz29724—The access point no longer displays an invalid login message when an administrator enters a username that is not in the user list; the access point now waits for the user to enter a password before displaying a message that the login is invalid.
- CSCdz32659—Memory allocation failure (MALLOCFAIL) messages no longer occur for Cisco Discovery Protocol (CDP) processes.
- CSCeb10400—Client devices no longer make multiple attempts to reauthenticate using an incorrect password. The problem was caused by an access point queueing error that has been corrected.
- CSCeb15588, CSCec33519—Administrative users assigned the **admin-capability** attribute can now log into the access point using Telnet.
- CSCeb49869—Access points are no longer vulnerable to malformed GET requests that cause the unit to reboot.
- CSCeb50339—Access points are no longer vulnerable to a malformed HTTP GET request which contains 2 GB of data.
- CSCec28612—ACL logging is not supported on access point bridging interfaces (for example, BVI1). When applied on a bridging interface, ACL logging works as if it were configured without the log option, and logging does not take effect. However, ACL logging works well for BVI interfaces when you use a separate ACL for the BVI interface.
- CSCec43008—When you update a WEP key using SNMP, the access point radio restarts automatically and uses the updated WEP key.
- CSCec43849—When you configure your access point for MAC address authentication for a large number of MAC addresses, client devices no longer experience long delays when they roam from one access point to another at the same time. You can enable MAC authentication caching to prevent the delay.
- CSCec47635—Logging into the access point CLI or GUI through the Ethernet port no longer causes a drop in access point radio throughput.
- CSCec55720—Client devices using 802.11b radios no longer lose connectivity unexpectedly when associated to a 1200 series access point.
- CSCec55763—The 802.11a radio no longer hangs when both the radios in a 1200 series access point are operating under heavy data loads.
- CSCec59848—The access point no longer uses only multiples of 8 for the Max Data Retries setting on the 802.11g radio.
- CSCec60868—Changing the TKIP MIC failure holdoff time to a non-default value no longer triggers the holdoff timeout.

- CSCec72841—The ARP cache feature is now supported on repeater access points.
- CSCec79193—The access point now correctly labels the priority field in 802.1q headers when VLANs are configured and you use policy maps.
- CSCec79626—The access point no longer runs out of memory when used as a local authenticator on the wireless LAN.
- CSCec86837—When a standby access point comes online, it now shuts down the radio ports on the access point that it replaces.
- CSCec88829—The access point no longer executes the **do** command for virtual interfaces.
- CSCec89492—Access points now return the correct number of associated clients when you poll the CDot11ActiveWirelessClients MIB object.
- CSCed00171—You can now configure up to 50 users on an access point acting as a local authenticator.
- CSCed16401—Access points no longer flap between switch ports.
- 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>.

- CSCed28709—The access point ARP-cache feature now works correctly on VLANs for which an extended ACL is enabled.
- CSCed33428—The CLI help and the output for the **show dot11 adjacent-ap** command now indicate that the list of adjacent access points is generated from information provided by Cisco Aironet client devices that are configured for fast, secure roaming.
- CSCed35718—NAS shared keys are now stored correctly on access points configured as local authenticators.
- CSCed37061—The access point now sends the correct username in accounting records for EAP-FAST clients.
- 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>.

- CSCed39237—The access point GUI no longer identifies a root access point as a repeater when you configure VLANs and set the fallback role to **Shutdown**.
- CSCed40563—Problems with the CDP protocol have been resolved.
- CSCed41790—The access point now includes the SSID VSA in RADIUS authentication messages as well as in RADIUS accounting messages.
- CSCed51325—The access point now forwards reverse-ARP requests from client devices to the wired LAN.
- CSCed56428—The 802.11g radio in the access point now sends 10 short training symbols instead of 12.
- CSCed56493—The WDS access point no longer reboots when there is a mismatch between the Cisco IOS Release running on the WDS access point and other access points on the network, or when you enable LEAP + MAC authentication or EAP + MAC authentication.
- CSCed63936—You can now enter QoS fixed-slot times higher than 15.
- CSCed65634—The access point 2.4-GHz radio no longer reaches the maximum quota for its transmit queue when wireless phones are associated.
- CSCed69756—By default, the access point sends reauthentication requests to the authentication server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers do not support the authenticate-only service-type attribute. Changing the service-type attribute to login-only ensures that Microsoft IAS servers recognize reauthentication requests from the access point. Use the **dot11 aaa authentication attributes service-type login-only** global configuration command to set the service-type attribute in reauthentication requests to login-only.
- CSCed72780—You can now use the GUI to configure WPA and Network-EAP for an SSID without also configuring open authentication.
- CSCed75714—A combination of settings (WPA or WPA-PSK key management, IP Phone QoS element, and transmit power less than 100 mW) on the access point's 802.11g radio no longer causes association delays for Cisco Aironet 802.11b client devices. The problem is resolved by Cisco Aironet Client Installation Wizard Package 1.3.10 and client firmware version 5.41.
- CSCed81399—You can now use the **no short-slot-time** command to disable short slot time on the 802.11g radio interface.
- CSCin51169—The access point Ethernet port now operates correctly with all valid speed and duplex configurations.

- CSCin60014—These invalid configurations no longer cause radio errors:
 - WPA optional with the TKIP cipher
 - WPA mandatory with TKIP+WEP40
 - WPA mandatory with TKIP+WEP128
- CSCsa12593—When you convert an access point that runs VxWorks to Cisco IOS software and administrator authentication is enabled on the access point, administrators are no longer locked out of the access point after the conversion to Cisco IOS software.

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(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. 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.