



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

July 1, 2004

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

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Installation Notes, page 5](#)
- [Important Notes, page 7](#)
- [Caveats, page 13](#)
- [Troubleshooting, page 15](#)
- [Related Documentation, page 15](#)
- [Obtaining Documentation, page 15](#)
- [Documentation Feedback, page 16](#)
- [Obtaining Technical Assistance, page 16](#)
- [Obtaining Additional Publications and Information, page 18](#)



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).

This release is based on Cisco IOS Release 12.2(15)JA.

System Requirements

You can install Cisco IOS Release 12.2(15)XR on all 1100 series access points and on model AP1230 access points. 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.



Note

Software upgrades fail when you use the web-browser interface to install Cisco IOS Release 12.2(15)XR 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 on page 20-18 in the *Cisco IOS Software Configuration Guide for Cisco Aironet 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.

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.



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:

```
ap>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 documentation home page:
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>
2. Follow this path to the product, document, and chapter:
Aironet 1200 Series Wireless LAN Products > Cisco Aironet 1200 Series Access Points > Aironet 1200 Series Access Points, Cisco IOS Release 12.2(15)JA > Cisco IOS Software Configuration Guide for Cisco Aironet Access Points > Managing Firmware and Configurations > Working with Software Images
3. Click this link to browse to the Cisco IOS Software Center on Cisco.com:
<http://www.cisco.com/public/sw-center/sw-ios.shtml>
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



Note

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



Note

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

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

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_administration_guides_list.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/public/sw-center/sw-ios.shtml>

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)XR. [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)XR*

Feature	350 Series	1100 Series	1200 Series
IP-Based Wireless Domain Services	–	X	X
Layer 3 Mobility Service via Fast Secure Roaming Tunnels	–	X	X

IP-Based Wireless Domain Services

This feature enables the access point to be explicitly configured with the IP address of its WDS device. This allows the access point to use a Cisco network infrastructure device running WDS from anywhere in the network. For instructions on using this feature, refer to the “Configuring Access Points to use the WDS Device” section on page 11-12 in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*. Click this link to browse to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_guide_book09186a00801ea410.html

Layer 3 Mobility Service through Fast Secure Roaming Tunnels

This feature allows an access point to segregate WLAN clients into different mobility groups. Once a client is authenticated using its mobility group's security policy, all IP traffic from the client is encapsulated using Generic Routing Encapsulation (GRE) and sent to a specific multipoint generic routing encapsulation (mGRE) interface of a Cisco Structured Wireless-Aware Network (SWAN) infrastructure device that supports mobility groups. A Layer 3 mobility service capable access point provides clients within each mobility group with Layer 3 mobility when used with a Cisco SWAN infrastructure device supporting Layer 3 mobility. Support for Layer 3 roaming is provided for all Wi-Fi Certified client devices. Support for fast secure Layer 3 roaming is provided for Cisco or Cisco Compatible wireless client devices using the Cisco Centralized Key Management (CCKM) protocol.

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.

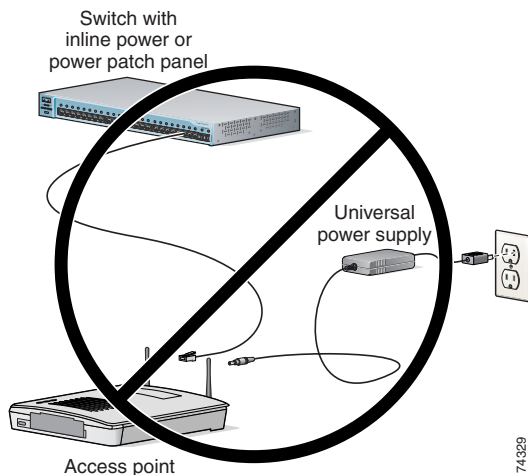
**Note**

The WS-F6K-PWR power over Ethernet (PoE) daughtercard in a Catalyst 6500 series switch cannot supply power to a 1200 series access point. Using a Catalyst 6500 series switch for inline power requires the WS-F6K-FE48-AF, WS-F6K-GE48-AF, or WS-F6K-VPWR-GE PoE daughtercard.

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)XR 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 on page 20-18 in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*. Click this link to browse to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_guide_book09186a00801ea410.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 “Configuring Basic Security Settings” section on page 2-11 in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

Figure 2 Express Security Page

HOME Hostname ap ap uptime is 1 minute

EXPRESS SETUP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY +

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

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

Access points do not support a loopback interface. Cisco recommends that you not configure a loopback interface on the access point.

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/prod_configuration_guides_list.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](#) for Cisco IOS Release 12.2(15)XR. This release is based on Cisco IOS Release 12.2(15)JA. All bugs resolved in Cisco IOS Release 12.2(15)JA are also resolved in this release.

Open Caveats

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

- 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.
- CSCec73044—When WPA is configured on the access point, associated client devices occasionally report MIC failures on packets from the access point.
- 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.
- 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.
- 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.

Resolved Caveats

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

- CSCeb02792—The 802.11a radio in 1200 series access points no longer reports 100% busy for all frequencies when you run the Carrier Busy test.
- CSCec02800—The access point web-browser interface no longer incorrectly displays cached information for the Associations page and now lists all associated client devices.
- CSCec25430—The access point no longer reboots when it receives a specific packet.
- CSCec25559, CSCed48488—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 does not decrease.
- CSCec55763—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 no longer hangs and the access point no longer reboots.
- 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 access point no longer reboots.
- CSCed02200—During EAP-SIM authentication, the access point now accepts client identities longer than 63 bytes.
- CSCed02220—When you upgrade an access point from 12.2(13)JAX to 12.2(15)XR, the **wlccp wds ipaddr 228 interface BVII** command remains valid.
- CSCed03154—The access point no longer indicates that a client device is associated when the client is not associated.
- CSCed25530—The Ethernet queue on 350 series access points no longer hangs, and input traffic is no longer dropped from the Ethernet interface.
- CSCed60301—When you enable shared key authentication and TKIP on an SSID on a 1200 series access point, most client devices can associate using the SSID.
- CSCed64393—A memory allocation failure no longer occurs on 350 series access points that have been upgraded to run Cisco IOS software.
- CSCed66461—Dual-mode client devices (clients with both 802.11b and 802.11g radios) can now associate to the access point when you change the access point's 802.11g radio from Best Throughput to Best Range.
- CSCed79096—The 1200 series access point now correctly reports its power need to a switch with power over Ethernet as 7 W.
- CSCed83246—Access points now send IGMP queries through the radio interface when a client device reassociates.
- CSCed84527—The access point no longer deauthenticates roaming client devices when the 1 and 2 Mbps datarates are disabled on the access point.
- CSCed87190—The **Best Throughput** button on the access point web-browser interface for 802.11g radios now provides the best throughput for the 802.11g radio.
- CSCee16473—When the WDS access point sends an oversized radio management packet to the WLSE device, this message no longer appears in the WLSE event log:

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

- CSCee18627, CSCee14096—If the access point is not configured as a local authenticator, the access point no longer reboots when you enter the **clear radius local-server user user** command.
- CSCee22037—When you convert an access point from VxWorks to Cisco IOS software and you have SNMP traps enabled before the conversion, the access point GUI now indicates as enabled only the SNMP traps that are enabled after the conversion.
- CSCee44666—Software upgrade no longer disables TACACS+.
- CSCee53647—Cisco legacy world mode remains enabled when you upgrade to Cisco IOS release 12.2(15)XR.
- CSCee55955—Client devices no longer fail LEAP authentication when IOS/PIX attributes are configured in Cisco Secure ACS.
- CSCee62247—Client devices in power-save mode no longer generate tracebacks when associated to 350 series access points.
- CSCee70393—The **debug dot11 mgmt tally** command now shows the incrementing and decrementing of association counters on the access point.
- CSCin62683—Client devices no longer fail to report a potential rogue access point.
- CSCin74956—Client devices that associate to the access point using an SSID with CKIP+CMIC encryption now receive IP addresses from the DHCP server.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac>. 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)XR and to 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 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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

<http://cisco.com/univercd/cc/td/doc/pcat/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the [Related Documentation](#) section.



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

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.