



Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.4(3g)JA

April 26, 2007

These release notes describe features, enhancements, and caveats for special technology early deployment release Cisco IOS Release 12.4(3g)JA. Release 12.4(3g)JA supports 32 Mb Cisco autonomous access points including Cisco Aironet 1100, 1130, and 1240 series access points, 1300 series access point/bridges, and 1400 series bridges.

Contents

These release notes contain the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Important Notes, page 8](#)
- [Caveats, page 14](#)
- [Troubleshooting, page 21](#)
- [Documentation Updates, page 21](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 22](#)

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.



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

© 2007 Cisco Systems, Inc. All rights reserved.

You can configure and monitor 1130 and 1240 series access points, 1300 series outdoor access point/bridges, and 1400 series bridges using the command-line interface (CLI), the web-browser interface, or Simple Network Management Protocol (SNMP).

System Requirements

You can install Cisco IOS Release 12.4(3g)JA on all 1130, 1240 series access points, 1300 series outdoor access point/bridges, and 1400 series bridges.

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 12.4(3g)JA:

```
ap1240AG>show version
Cisco Internetwork Operating System Software
IOS (tm) C1240 Software (C1240-K9W7-M), Version 12.4(3g)JA
Copyright (c) 1986-2007 by Cisco Systems, Inc.
```

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

Upgrading to a New Software Release

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

-
- Step 1** Follow this link to the Cisco home page:
<http://www.cisco.com>
 - Step 2** Click **Support**. The Support page appears.
 - Step 3** Click **See Documentation**. The Documentation page appears.
 - Step 4** Click **Wireless**. The Wireless Support Resources page appears.
 - Step 5** Scroll down to the Access Points section.
 - Step 6** Select the access point model for which you need the information. The Introduction page for the model you selected appears.
 - Step 7** Under the Configure section, click **Configuration Guides**. A list of configuration documents appears.
 - Step 8** Click **Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(3g)JA**.
 - Step 9** Navigate to the Managing Firmware and Software chapter.
-

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

<http://www.cisco.com/public/sw-center/sw-ios.shtml>

Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

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

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

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

Figure 1 Network Interfaces: Radio Settings Page



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

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

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

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

New Features

Table 1 lists the new features in Cisco IOS Release 12.4(3g)JA and the supported platforms.

Table 1 New Cisco IOS Software Features for Cisco IOS Release 12.4(3g)JA

Feature	1100 Series Access Points	1130AG Series Access Points	1200 Series Access Points	1230 Series Access Points	1240AG and 1130G Series Access Points	1300 Series Outdoor Access Point/Bridge	Cisco Aironet 1400 Series Wireless Bridge
Cisco Aironet 1240G and 1130G Series Access Points	–	x	–	–	x	–	–
Regulatory domain update for Japan	–	–	–	–	x	–	–
Multiple VLAN and rate limiting support for point-to-multipoint bridging	–	x	–	–	x	x	–
Universal workgroup bridge	–	x	–	–	x	x	–
Client MFP support	–	x	–	–	x	x	–
Channel scan limitation for workgroup bridge	–	x	–	–	x	x	–

Feature Descriptions

Cisco Aironet 1240G and 1130G Series Access Points

The Cisco Aironet flagship access points—the Cisco Aironet 1240AG Series and the Cisco Aironet 1130AG Series—are now available in single-band 802.11g versions for use in regulatory domains that do not allow 802.11a (5-GHz) operation.

The Cisco Aironet 1240G Series Access Points provide single-band 802.11g wireless connectivity for challenging RF environments such as factories, warehouses, and large retail establishments.

The Cisco Aironet 1130G Series is a single-band, low-profile, business-class access point with integrated antennas for easy deployment in offices and similar RF environments.

Japan Upgrade Utility

This release supports the U regulatory domain for the W52 frequency set (channels 36, 40, 44, and 48) in Japan. Cisco access points specified for this new domain ship with a U domain radio. Installed J domain access points are automatically upgraded to U domain status with this release. For the latest Cisco WLAN compliance status, please visit:

http://www.cisco.com/application/pdf/en/us/guest/products/ps5861/c1650/cdcont_0900aecd80537b6a.pdf.

Japan allows three different frequency sets organized into regulatory domains as shown in [Table 2](#)

Table 2 *Japan Frequency Sets*

Frequency Set	Channel (Freq)	Channel (Freq)	Channel (Freq)	Channel (Freq)
J52	34 (5170 MHz)	38 (5190 MHz)	42 (5210 MHz)	46 (5230 MHz)
W52	36 (5180 MHz)	40 (5200 MHz)	44 (5220 MHz)	48 (5240 MHz)
W53	52 (5260 MHz)	56 (5280 MHz)	60 (5300 MHz)	64 (5320 MHz)

These frequency sets have 3 legal combinations in which Cisco has organized into regulatory domains:

- J regulatory domain = J52
- P regulatory domain = W52+W53
- U regulatory domain = W52

The upgrade utility allows users to migrate their 802.11a radios from J52 to W52. The utility operates on the following devices:

- 1130 series access points
- 1240 series access points

Users must migrate all 802.11a radios in their wireless network from J52 to W52. There cannot be a mix of radios in the network operating in the J52 and W52 bands because of overlap.

Multiple VLAN and Rate Limiting Support for Point-to-Multipoint Bridging

This feature provides the Cisco Aironet wireless LAN bridges the ability to provision each non-root under one VLAN. This could be supported by simply adding the 802.1Q tag with the configured VLAN ID to all the uplink packets coming from the Ethernet side of the non-root bridge. Cisco Aironet wireless bridges provide control in limiting the data traffic pumped through the air. This feature makes it possible to control the maximum rate of traffic transmitted or received on an interface. The actual action of limiting the data rate is done at Layer 3 before the traffic data is provided to the radio.

In order to implement rate limiting, the Cisco IOS Class-based Policing feature is used. You can find more details about this feature at the following link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a00801b23f8.htm

Client MFP Support

Wireless Intrusion Detection System (IDS)-Management Frame Protection (MFP), which provides for the authentication of 802.11 management frames by the wireless network infrastructure, was introduced with Cisco IOS Software Release 12.3(8)JA. This release enhances MFP support and is now available for Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapters, Wireless PCI Adapters, and Autonomous Access Points running in root, repeater, workgroup bridge, and non-root bridge mode. MFP adds security to the MAC management layer of 802.11 connectivity by cryptographically hashing the management frames and generating a Message Integrity Check (MIC) during network connection. This release allows a Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapter or Wireless PCI Adapter to detect a spoofed management frame at the first instance of an attack and generate an intrusion detection system (IDS) alert to the device interface. Autonomous access points that detect a spoofed management frame from a client or another access point will also generate an IDS alert that is sent to the Cisco Wireless LAN Solution Engine (WLSE), as shown in Figure 2. In order to take advantage of

the MFP, the clients must support Cisco Compatible Extensions Version 5 devices. For more details, see the Cisco Compatible Extensions program Webpage at: <http://www.cisco.com/go/ciscocompatible/wireless>.

Universal Workgroup Bridge

This feature allows one Ethernet client to connect through a Cisco autonomous access point configured as a workgroup bridge to non-Cisco access points. When configured for universal workgroups bridge support, the access point uses the MAC address of the Ethernet client to associate with the non-Cisco access points. All probe and association requests will be sent and received using the MAC address of the Ethernet client instead of the dot11 MAC. As a result, the root (non-Cisco) access point will not be able to use telnet to manage the workgroup bridge, because it can only read the single MAC address of the connected Ethernet client, and it uses this MAC address to forward any traffic to the workgroup bridge.

Channel Scan Limitation For Workgroup Bridge

This feature reduces the total scanning time and hand-off delay as a workgroup bridge roams from one access point to another. With this feature, the workgroup bridge can be configured to scan only one or a limited subset of channels instead of scanning all possible channels.

Installation Notes

This section contains information you should keep in mind when installing 1130, 1240 series access points, and 1300 series outdoor access point/bridges.

Installation in Environmental Air Space

Cisco Aironet 1130 and 1240 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.

Power Considerations

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



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 1130 series access points with both DC power to its power port and inline power from a patch panel or powered switch to the access point's Ethernet port. If you apply power to the access point from both sources, the switch or power patch panel might shut down the port to which the access point is connected. [Figure 2](#) shows the power configuration that can shut down the port on the patch panel or powered switch.

Figure 2 *Improper Power Configuration Using Two Power Sources*



Configuring Power for 1130 and 1240 Series Access Points

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

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



Using the AC Power Adapter

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

Using a Switch Capable of IEEE 802.3af Power Negotiation

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

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

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

Using a Power Injector

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

Antenna Installation

For instructions on the proper installation and grounding of external antennas for 1240 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.

CCKM and Fast Roaming on Cisco 7921/7925 IP Phones

When a 7921 or 7925 wireless associates to an access point in a WDS with CCKM, it cannot fast roam because call admission control is not enabled. To work around this issue you must enable admission control by issuing the **admit-traffic** command in the access point SSID configuration as shown in the following example:

```
dot11 ssid voice
vlan 21
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-managemenet wpa cckm
admit-traffic
```

Unable to Make Calls Using the 7921 Phone with CAC/TSPEC Enabled on the Access Point

With CAC/TSPEC enabled on the access point, a call cannot be made from a 7921 wireless phone associated to the access point to another IP phone using basic voice setup. Calls from the 7921 fail only on 32-MB platform images; the problem is not observed with the 16-MB platform image. The workaround for this problem is to use Cisco IOS Release 12.3(11) JA1.

This issue is tracked through open caveats CSCsi34566.

Layer 3 Not supported with NAC for MBSSID

Layer 3 is not supported with NAC for MBSSID in this release.

Change to Default IP Address Behavior

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

- When you connect a 1130 or 1240 series access point or a 1300 series outdoor access point/bridge with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an address, continues to send requests indefinitely.

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

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

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

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

A hidden configure level command, **dot11 wpa handshake timeout**, can be used to increase the timeout between sending the WPA key packets from the default value (100 ms) to a value between 101 and 2000 ms. The command stores its value in the configuration across device reloads.

Default Username and Password Are *Cisco*

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

Some Client Devices Cannot Associate When QoS Is Configured

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

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

Some Devices Disassociate When Multiple BSSIDs Are Added or Deleted

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

Enabling MBSSIDs Without VLANs Disables Radio Interface

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

This example shows the commands you use to re-enable the radio:

```
AP1242AG(config)# interface d1
AP1242AG(config-if)# shut
AP1242AG(config-if)# no mbssid
AP1242AG(config-if)# no shut
```

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

Cannot Set Channel on DFS-Enabled Radios in Some Regulatory Domains

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

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

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

GRE Tunnelling Through WLSM Sometimes Requires MTU Setting Adjustments

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

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

TACACS+ and DHCP IP Address Sometimes Locks Out Administrators

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

Access Points Do Not Support Loopback Interface

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



Caution

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

Non-Cisco Aironet 802.11g Clients Might Require Firmware Upgrade

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

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

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

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 Cannot Be Configured as WDS Access Points

Repeater access points can participate in WDS but they cannot provide WDS. You cannot configure a repeater access point as a main WDS access point, and if a root access point becomes a repeater in fallback mode, it cannot provide WDS.

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.

Corrupt EAP Packet Sometimes Causes Error Message

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

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

You can ignore these messages.

When Cipher Is TKIP Only, Key Management Must Be Enabled

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

Cisco CKM Supports Spectralink Phones

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

Non-Cisco Aironet Clients Sometimes Fail 802.1x Authentication

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

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

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

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

Layer 3 Mobility Not Supported on Repeaters and Workgroup Bridges

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

WLSM Required for Layer 3 Mobility

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

Caveats

This section lists open and resolved caveats for access points.

Open Caveats

These caveats are open in Cisco IOS Release 12.4(3g)JA:

- CSCek46661—VLAN assignment fails when using local radius server.
After passing EAP-FAST authentication, the client is not placed into the VLAN defined by the group configured in the local RADIUS server. Instead, the client remains in the VLAN assigned by the SSID.
- CSCsd90308—Large default beacon size causes blue screen on Conexant Wi-Fi station
The very large default beacon size on the 802.11a band with 12.3(11)JA firmware is causing a Conexant ISL39200C with the Wi-Fi test bed driver to blue screen under Windows XP.
The 802.11a beacon size of with TKIP, AES, and WMM enabled is approximately 285 bytes, depending on the size of the SSID. This is an enormous jump in size since Cisco's last version of firmware due to the Country IE 7 and the Power Constraint IE now being advertised by default.
The Conexant radio seems to blue screen at 235 bytes and larger. Conexant has reproduced the problem.
- CSCsd99125— WDS may report an incorrect new channel to WLSE after a RADAR event
During DFS event testing, it was discovered that if a DFS event was triggered on a non-root device, the WLSE sometimes received an erroneous new channel report.
- CSCse41589—Workgroup bridge fails to get a DHCP IP address after a successful EAP-FAST authentication to the root access point. The workgroup bridge is able to ping the root access point and wired host if BV11 is assigned with a static IP address. Occasionally, the workgroup bridge is assigned a DHCP IP address after a long period of time (about 15 to 20 minutes).
The failure to obtain a DHCP IP address is not observed when the the workgroup bridge uses LEAP authentication.
- CSCse42464—Access point fails to retrieve certificate from certificate authority server using GUI
Certificate is obtained correctly when using the CLI.

- CSCse48137—Nested repeater does not work

A nested 1130 access point configured for open authentication and root mode station role fails to associate with a repeater and displays the following console message:

```
*Mar 1 00:01:34.822: %DOT11-4-CANT_ASSOC: Interface Dot11Radio1, cannot associate: No
Response
*Mar 1 00:02:17.603: %DOT11-6-DFS_SCAN_COMPLETE: DFS scan complete on frequency 5560
MHz
*Mar 1 00:02:31.821: %DOT11-4-CANT_ASSOC: Interface Dot11Radio1, cannot associate:
Rcvd response from 0014.6956.5cda channel 149 801
```

- CSCse49342—DHCP_SERVER_FAILURE observed in 1300 series in WGB mode.
- CSCsg74791—Time-based ACLs do not work properly on IOS access points.

The access point does not appear to recognize the specified time-range. Either the ACL becomes active as specified, and the access point will not recognize when the ACL becomes inactive, thus continuing to enforce/apply the ACL; or the ACL will be applied immediately once it is enabled on an interface (radio or fa0).

- CSCsg90606—When an SSID is configured with WPA version 2+CCKM and encryption is set to TKIP, wireless clients fail to authenticate to the access point.

Workaround: None.

- CSCsh17037—In rare circumstances a memory leak may develop in the SSH process.

Workaround—Reboot the access point.

- CSCsh40248—1310 bridges in access point mode sometimes display this message: “Warning: Dot11Radio Temperature has reached ‘SHUTDOWN’level at -2(C).” However, -2 celsius is within the 1310 bridge operating range.

Workaround: None.

- CSCsh43635—Frequent tracebacks occur on WDS Process = WLCCP WDS Traceback= 0x5BEB4

On a AP/WDS, the WDS is generating frequent tracebacks on the WLCCP WDS process. The tracebacks appear to be occurring about every 3 minutes. The WDS is running radio management. It appears that normal system activity causes this to occur. This issue may be caused by the radio management context switching that occurs between normal radio management and access point radio scan jobs.

- CSCsh84949—Wireless client fails to receive multicast data stream.

Workaround—Configure no ip igmp snooping on the access point.

- CSCsh86675—1310 Bridge continuously authenticates and deauthenticates with LEAP enabled.

Occurs when 1310 configured as an access point and associating with an Intel 2915 802.11g radio. Client running LEAP associates and disassociates with the client de authenticating.

- CSCsi02700—TKIP group key 0 length with simultaneous AES and TKIP SSIDS

In an Intel NAC environment with Multiple SSIDs/VLANs, including SSIDs using AES and TKIP ciphers, the AES SSID works, but the TKIP SSIDs fail. The API log showed repeated failures of the same form. The group key was rejected by the Intel 2200 driver. The packet trace showed that the group key packets contained no key, listed the key length as 0, and index of 0.

- CSCsi04754—EAP-FAST does work with local RADIUS server if LEAP is disabled.
If LEAP is disabled on the local radius server, local RADIUS server fails to authenticate EAP-FAST clients. This condition applies to the 1100, 1131, 1200, 1242 access points, and the 1310 outdoor access point/bridge. LEAP is disabled on the local RADIUS server.
Workaround—enable LEAP on the local RADIUS server or use an external RADIUS server.
- CSCsi16928—Online SCEP enrollment request rejected by certificate authority.
Workaround—none.
- CSCsi23996—An access point may crash and restart citing an error in dot11_arp_cache_zero_remove.
This may occur under normal operating conditions. The following tracebacks or messages may be observed in the logs or SHOW TECH:
Unexpected exception to CPUvector 1100, PC = 0x49F39C, LR = 0x49FA68 -Traceback= 49F39C 49FA68 450D94 452274 4291DC 42E2E8 411500 2411
Workaround—none.
- CSCsi24761—The 802.11a radio in 1130 series access points sometimes remains in a reset state. Resetting the access point returns the radio to normal operation.
- CSCsi25404—1240 access point reloads due to “ROM by unknown reload cause - reason ptr 0xF, PC 0x6C33B0, address 0x0.”
Tracebacks point to Dot11 driver.
Workaround—none.
- CSCsi32429—Radio scan job fails on scanning access points.
When an access point radio scan job is run on scanning access points, the radio scan job fails with the error shown below.
WLSE Scan Job Log Error Message:
ERROR: Removing interface 00-12-43-f5-00-60(10.91.102.52) from AP Radio Scan participation because of SnmpResponseGenErr on 10.91.102.52 while performing SnmpSet at index = 0
- CSCsi34566—Unable to make a call with CAC/TSPEC enabled on the access point.
With CAC/TSPEC enabled on the access point, a call cannot be made from a 7921 wireless phone associated to the access point to another IP phone using basic voice setup. It should be noted that calls from the 7921 fail only on 32MB platform images. The problem is not observed with the 16MB platform image.
Workaround: Use Cisco IOS Release 12.3(11) JA1.
- CSCsi35780—LRS EAP-FAST does not work when a workgroup bridge is used as supplicant.
- CSCsi35911—Cannot restrict channel list for Least Congested Frequency
The ability to restrict the channel list for Least Congested Frequency does not work. Using the GUI interface, if you select the desired channels and then apply when the screen refreshes all channels are highlighted as though all channels are selected. Using the CLI the command is accepted and is part of the running-config but the access point has been observed to use a channel outside of the selected channels.
- CSCsi46919—LRS EAP-FAST user is rejected initially.
When using LRS for EAP-FAST the PAC provisioning fails the first time for automatic PAC provisioning and prompts for the username & password, then passes after reentering the user credentials.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.4(3g)JA:

- CSCed45578—Console no longer locks after booting with system accounting.
- CSCsb08590—BR1410 no longer fails to flash radio firmware on IOS upgrade to 12.3(4)JA.
- CSCsb12598

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.



Note

Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCsb70864—BR1410 no longer fails to flash radio firmware on IOS upgrade to version 12.3(7)JA.
- CSCek46852—EAP-FAST works with open source client and local radius.
- CSCsb78160—Access point system error messages updated in documentation.
- CSCsb58098—MBSSID enabled hot standby access point now not EAP associates to a primary access point.
- CSCsc60071—ImportAP Authorization List into the doc has been clarified.
- CSCsc83142—1310 non-root bridge no longer shuts down its radio if SWAN participation is disabled.
- CSCsc88186—Non-root to non-root association for BR1310 now documented.
- CSCsc95298—Deauthentication reassociation messages now appear on event log.
- CSCsd02001—AES-CCMP no longer replays on 1310 access point/bridge.
- CSCsd17187—BR1310 default value of rts threshold operates normally.

- CSCsd54914—802.1x reauthentication interval behavior is now correct for non-root bridge.
- CSCsd62772—Radius accounting start/stop records are now sent for associated client.
- CSCsd85587

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

The vulnerable cryptographic library is used in the following Cisco products:

- Cisco IOS, documented as Cisco bug ID CSCsd85587
- Cisco IOS XR, documented as Cisco bug ID CSCsg41084
- Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM)

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.


Note

Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml> and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.

- CSCsd92405
- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.
- Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.
- Cisco IOS is affected by the following vulnerabilities:
- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
 - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
 - Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.



Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCse16085—Wi-Fi WMM test failure no longer occurs.
- CSCse29487—Repeater to Repeater roaming no longer fails.
- CSCse35087—1240 access point clock no longer loses time without NTP.
- CSCse56501

A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml>

- CSCse70031—Accounting record no longer uses MAC address for username with WPAv2.
- CSCse72925—SNMP mib community-map engineID command no longer causes traceback on access points.
- CSCse84920—Access point no longer reloads to ROM with unknown system cause.
- CSCse95836—Access point no longer forwards invalid Ethernet frame length=0 over wireless.

- CSCsf04754

Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080609-snmpv3.shtml>

- CSCsf07847—CDP no longer fails to discover neighbor information in releases.
- CSCsf08775—EAP-FAST supplicant now operates properly with Steel Belt RADIUS server.
- CSCsf18528—Unexpected SNMP traffic no longer causes 1200 series access point restart.
- CSCsf22409—Fastethernet interface no longer stops processing entries on rx ring.
- CSCsf95975—Access point no longer crashes when AeroScout server address is misconfigured.
- CSCsg05807—7020 phone roaming now operates correctly with MBSSID enabled.
- CSCsg16033—cDot11ClientStatistics & cDot11ClientConfiguration messages are now consistent with workgroup bridges.
- CSCsg20744—Turn off MBSSID now appears when configuring access point to sensor mode.
- CSCsg26708—Access point no longer stops passing broadcast traffic from wired to wireless side.
- CSCsg4448—%LEAPCL-3-TIMEOUT messages no longer occur with 1242 to WDS.
- CSCsg48579—**no led display alternate** CLI is now removed from the running configuration.
- CSCsg56375—BR1410 radio no longer resets when over temperature detected.
- CSCeg62070—Tracebacks no longer occur during HTTP transactions with long URLs.
- CSCsg68227—QoS class parameters for CWmax are no longer reset after radio interface shut down.
- CSCsg71594—CLI no longer permits configuring both EAP and WPA-PSK on the same SSID.
- CSCsg79644—1240 and 1230 in workgroup bridge mode no longer stop broadcast and multicast traffic with 1310 access point/bridge.
- CSCsg80960—Access point no longer reloads when receiving multicast from an unconfigured dot1q VLAN.
- CSCsg91315—WDS does now returns reports to WLSE
- CSCsg99358—Traceback/crashes no longer occur in unconfigured VLAN.
- CSCsh22776—Wireless clients now associate in WDS environment if EAP is optional.
- CSCsh33598— Access point now conforms with mainstream IOS behavior.
- CSCsh47853—**show dot11 associations** command now shows correct output bytes.
- CSCsh52582—Association table in GUI and CLI will displays proper amount of characters.
- CSCsh53511—1131 access point no longer loses connection with an Intel 3945 Wireless NIC.

- CSCsh62835—EAP-FAST no longer fails with local authentication & open source cards.
- CSCsh71209—Disabling Aironet extensions on root now prevents repeater to join.
- CSCsh71226—Using a repeater it is no longer possible to jump VLAN configuration on SSID.
- CSCsh80023—Apostrophe in hostname no longer causes GUI to malfunction.
- CSCsh83796—Repeater access point no longer loses association after re-configuring the association mac-list.
- CSCsh85001—Access point GUI now displays timezone name as an offset of GMT.

If You Need More Information

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

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

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

Troubleshooting

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

Documentation Updates

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

Related Documentation

This section lists documents related to Cisco IOS Release 12.4(3g)JA and to 1130AG, 1240AG series access points, and 1300 series outdoor access point/bridges.

- *Quick Start Guide: Cisco Aironet 1130AG Series Access Points*
- *Quick Start Guide: Cisco Aironet 1240AG Series Access Points*
- *Quick Start Guide: Cisco Aironet 1300 Series Outdoor Access Point/Bridge*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *Cisco Aironet 1130AG Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1300 Series Outdoor Access Point/Bridge Hardware Installation Guide*
- *Installation Instructions for Cisco Aironet Power Injectors*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

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

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.