



Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 12.4(3g)JA1

July 23, 2007

These release notes describe features, enhancements, and caveats for special technology early deployment release Cisco IOS Release 12.4(3g)JA1. This release supports 32-Mb Cisco autonomous access points, including Cisco Aironet 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 10](#)
- [Caveats, page 16](#)
- [Troubleshooting, page 20](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 20](#)

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



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

© 2007 Cisco Systems, Inc. All rights reserved.

System Requirements

You can install Cisco IOS Release 12.4(3g)JA1 on all 1130, 1240 series access points, 1300 series outdoor access point/bridges, and 1400 series bridges.

Finding the Cisco IOS Software Version

To find the version of Cisco 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 Cisco 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 Cisco IOS software, the software version appears at the top left of most pages in the web-browser interface.

Upgrading to a New Software Release

Follow these steps for instructions on upgrading your access point or bridge software:

-
- 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 that 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/cisco/software/navigator.html>

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

Cisco IOS Release 12.4(3g)JA1 has the following new features:

- Access Point mode support for 1400 series bridges
- Multiple SSID support for 1400 series bridges
- EAP-TLS supplicant support for 1300 series outdoor access point/bridge

Access Point Mode Support for 1400 Series Bridges

In this release, you can configure the 1400 series bridge as a root access point. The feature allows for basic access point support as shown in [Table 1](#).

Table 1 **1400 Series Access Point Functionality**

Access Point Feature	Supported	Access Point Feature	Supported
Basic functionality	Yes	Radio	Yes
Filtering security	Yes	Wireless security encryption authentication	Yes
Wireless security RADIUS server	No	Wireless security WPA	Only WPA v1 (TKIP)
Wireless security CCKM WDS	No	Wireless security IDS	No
VLAN	No	Access point management	Yes
QoS	No	Voice	No
SSID globalization	No	User interface	Yes
Hot standby	No	DFS/802.11h	No
Location based services	No	Workgroup bridge	Yes
Link role flexibility	No	Wireless NAC	No

[Figure 2](#) shows the Express Setup screen for this feature.

Figure 2 1400 Series Bridge Express Setup Page

Cisco Aironet 1400 Series Wireless Bridge

Hostname: root-bridge-3 root-bridge-3 uptime is 6 days, 9 hours, 21 minutes

Express Set-Up

Host Name:

MAC Address:

Configuration Server Protocol: ☐ DHCP ☒ Static IP

IP Address:

IP Subnet Mask:

Default Gateway:

SNMP Community:

☒ Read-Only ☐ Read-Write

Radio0/802.11A

Role in Radio Network: ☒ Access Point ☐ Root Bridge ☐ Non-Root Bridge ☐ Install-Mode
☐ Workgroup Bridge ☐ Universal Workgroup Bridge Client MAC:

Optimize Radio Network for: ☐ Throughput ☐ Range ☒ Default ☐ Custom

Aironet Extensions: ☒ Enable ☐ Disable

Apply Cancel

Detailed information and configuration procedures are in Chapter 6 of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(3g)JA & 12.3(8)JEB*, which is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/docs/wireless/access_point/12.4_3g_JA/configuration/guide/s43rf.html

Multiple SSID Support for 1400 Series Bridges

In this release, you can configure up to 16 SSIDs on the bridge. This feature is significant because bridges configured as a workgroup bridge can associate to a bridge configured as a root access point provided their SSIDs are properly configured.

Detailed information and configuration procedures are contained in Chapter 7 of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(3g)JA & 12.3(8)JEB*, which is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/docs/wireless/access_point/12.4_3g_JA/configuration/guide/s43ssid.html

EAP-TLS Supplicant Support for 1300 Series Outdoor Access Point/Bridge

This feature supports an 802.1X supplicant for EAP-TLS that provides a secure method for enabling 802.1X authentication on the switch ports that are connected to access points. This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It uses a client certificate for authentication.

RADIUS servers that support EAP-TLS include Cisco Secure ACS release 3.0 or later and Cisco Access Registrar release 1.8 or later.

Detailed information and configuration procedures are in Chapter 11 of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(3g)JA & 12.3(8)JEB*, which is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/docs/wireless/access_point/12.4_3g_JA/configuration/guide/s43auth.html

Installation Notes

This section contains information that you should keep in mind when installing 1130, 1240 series access points, 1300 series outdoor access point/bridges, and 1400 series bridges.

Access Points

This section contains installation notes for access points.

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 that you should consider before applying power to an access point.



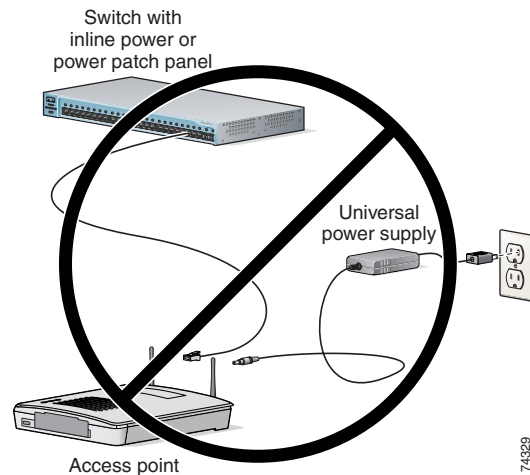
Caution

Cisco Aironet power injectors are designed only for use with Cisco Aironet access points and bridges. 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 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 3](#) shows the power configuration that can shut down the port on the patch panel or powered switch.

Figure 3 *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 4](#) shows the System Power Settings section of the System Configuration page.

Figure 4 *Power Options on the System Software: System Configuration Page*

System Power Settings	
Power State:	FULL POWER
Power Source:	AC_ADAPTOR
Power Settings:	<input type="radio"/> Power Negotiation <input checked="" type="radio"/> Pre-standard Compatibility
Power Injector:	<input type="checkbox"/> Installed on Port with MAC Address: <input type="text" value="DISABLED"/> (HHHH.HHHH.HHHH)
<input type="button" value="Apply"/>	

121655

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 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.

1400 Series Bridge

This section contains installation information for the 1400 series bridge.

Default SSID and Distance Settings Change When You Change Role in Radio Network

If the bridge's SSID has not been changed from the default setting and you select **Install Automatic Mode** as the bridge's role in radio network setting, the SSID automatically changes from *tsunami* to *autoinstall*. When you change the role in radio network from Install Automatic Mode to Root or Non-Root, the SSID changes automatically from *autoinstall* back to *tsunami*. However, if you change the SSID from its default setting, changing the role in radio network setting does not change the SSID.

In Install Automatic Mode, the default distance setting is 61.5 mi. (99 km). When you change the role in radio network from Install Automatic Mode to Root or Non-Root, the distance setting changes automatically from 61.5 mi. (99 km) to 0 mi. (0 km).

Default Encryption Key 2 Is Set by Bridge

The encryption key in slot 2 is the transmit key by default. If you enable WEP with MIC, use the same WEP key as the transmit key in the same key slot on both root and non root bridges.

Limitation to PAgP Redundancy on Switches Connected by Bridge Links

When two switches configured for Port Aggregation Protocol (PAgP) are connected by redundant wireless bridge links, the PAgP chang-over takes at least 30 seconds, which is too slow to maintain TCP sessions from one port to another.

CLI Command `power client n` Is Not Supported

The bridge does not support the `power client n` configuration interface command in the web-browser or CLI interfaces. The bridge does not perform any action when you enter this command.

Default Infrastructure SSID

When a VLAN is enabled, the WEP encryption mode and the WEP key are applicable only to a native VLAN. Any SSID configured should have the Infrastructure-SSID parameter enabled for that SSID. With the Infrastructure-SSID parameter enabled, the bridge ensures that a non-native VLAN cannot be assigned to that SSID.

ARP Table Is Corrupted When Multiple BVIs Are Configured

The bridge supports only one bridge virtual interface (BVI). Multiple BVIs should not be configured because the ARP table can be corrupted.

Bridge Power Up LED Colors

During power up, the bridge LEDs display the following color sequences:

1. The Install LED is initially turned off.
2. The Install LED turns amber.
3. The Status LED turns amber during the boot loader process.
4. The Ethernet, Status, and Radio LEDs turn green during the loading of the operating system.
5. The Ethernet, Status, and Radio LEDs turn amber during the loop-back test.
6. The Status LED starts to blink green, and then the Ethernet LED starts to blink green.
7. The Ethernet, Status, and Radio LEDs blink amber twice to show that the auto-install process has started.
8. During the auto-install process, the Ethernet, Status, and Radio LEDs turn off for a short time period, and then go through a blinking sequence twice. Each LED sequentially blinks at the following rates before becoming continuously amber:
 - a. Slow blinking rate of 1 blink per second.
 - b. Medium blinking rate of 2 blinks per second.
 - c. Fast blinking rate of 4 blinks per second.
9. The Install LED starts to blink amber to show that the bridge is searching for a root bridge.
10. When the bridge associates to a root bridge, the Install LED turns amber.

11. When the bridge becomes a root bridge and is waiting for a nonroot bridge to associate, the Install LED blinks green.
12. When the root bridge has a nonroot bridge associated, the Install LED turns green.

Bridge Cannot Detect Simultaneous Image Downloads

Do not attempt to load software images into the bridge from both a Telnet session and a console session simultaneously. The bridge cannot detect that two images are being loaded at the same time. For best results, use the **archive download** command in the CLI.

Bridge Cannot Detect Invalid Software When Using copy Command

The bridge sometimes cannot detect invalid software images when you load software using the copy command. For best results, use the **archive download** command in the CLI to load new software.

Telnet Session Sometimes Hangs or Will Not Start During Heavy Traffic

When the bridge is transmitting and receiving heavy traffic, you sometimes cannot start a Telnet session and some existing Telnet sessions halt. However, this behavior is expected because the bridge gives top priority to data traffic and a lower priority to Telnet traffic.

Important Notes

This section describes important information about the access points and bridge.

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
```

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 allows 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 can 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 can 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 a 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 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 that 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 to 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 resetting 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

We recommend 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 memory after the upgrade, the pages in the web-browser interface might not reflect the upgrade. This example shows how to upgrade system software by 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 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 this message.

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. CCKM supports only Spectralink and Cisco 7920 Version 2.0 Wireless Phones. Other voice clients 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)JA1:

- CSCse41589—Workgroup bridge fails to get a DHCP IP address after a successful EAP-FAST authentication to the root access point. The workgroup bridge can ping the root access point and wired host if BVI1 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 workgroup bridge uses LEAP authentication.
- CSCse42464—Access point fails to retrieve certificate from certificate authority server when 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 this 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 Cisco Aironet IOS access points.
The access point does not recognize the specified time-range. Either the ACL becomes active as specified, and the access point does not recognize when the ACL becomes inactive, thus continuing to apply the ACL; or the ACL is applied immediately when 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.
- 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 disauthenticating.

- CSCsi02700—TKIP group key contains a 0 length key field with simultaneous AES and TKIP SSIDs.

Establishment of an EAP-FAST WPA/TKIP connection fails and retries repeatedly due to the WPA/TKIP group key packet coming from the access point does not contain a key. A packet trace shows the EAP-FAST authentication succeeding, followed by the pairwise key handshake, and then two key packets for the group keys, which contains a 0 length key field. The access point times out and attempts reauthentication, causing the cycle to repeat.

This problem occurs when the 1231 series access point is configured with multiple SSIDs and VLANs, with some SSIDs using AES and others TKIP ciphers.

Workaround—Make all the SSIDs either AES or TKIP. In an Intel NAC environment with Multiple SSIDs and 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.

- CSCsi24761—The 802.11a radio in 1130 series access points sometimes remains in a reset state.

Workaround—Reset the access point.

- 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.

- CSCsj30069—Nonroot bridge fails to associate if native VLAN is not 1

This caveat affects Cisco IOS release 12.4(3g)JA and 12.3(8)JEB only and only the root bridge. The only platforms affected are the 1100, 1131, 1230, 1242, 1310, and 1410 series. The client trying to associate is either a repeater or nonroot bridge.

Workaround—Use VLAN 1 as the native VLAN.

- CSCse34644—Shared authentication with non-native vlan is not working.

Workaround—Save the configuration, and reload the access point. When the access point comes up, both clients authenticate. Edit the authentication SSID as follows:

Add open authentication; remove shared authentication. Then remove open and add shared authentication, and the client will associate. Save the configuration, and reload the access point.

- CSCsj03461—1310 series cannot authenticate to root 1310 using EAP-TLS when certificate is downloaded using SCEP method.

EAP-TLS authentication fails only if the certificate is downloaded using SCEP method.

Workaround—Download the certificate using cut-and-paste method.

- CSCsc94510—GE: GUI can set illegal combination of low latency rates.

The GUI can set an illegal combination of low latency rates on the access point. It is possible to see 48 and 54 Mbps set as both nominal and non-nominal values. When in this mode, you can not disable the 48 and 54 rates, which stay set as non-nominal.

Workaround—None.

- CSCsg71997—Hostname not assigned to access point when IP address obtained from DHCP server.

After setting up the DHCP server to provide IP address, hostname and DNS, the hostname is shown as *ap* after rebooting.

- CSCsj22047—User is unable to modify or disable Key Management for a configured SSID.

Key Management for a configured SSID cannot be disabled and in some instances attempts to modify from mandatory to optional failures.

Workaround—To disable key management, clear the WPA-PSK keys, select key-management as NONE, and click **apply**. The WPA-PSK keys are removed. Then select key-management as NONE, and click **apply**.

Configure an SSID with encryption AES-CCM and key management mandatory with WPA-PSK. Then attempt to disable the key management. After clicking **apply** and **OK**, select the SSID again, and key management is still mandatory.

If the correct encryption is not selected for optional key management, an error message only appears if the user selects optional and then clicks the WPA drop-down list. If the user does not click the drop-down and simply clicks **apply** at the bottom of the page, it appears as if the change is being made, but the key management remains mandatory.
- CSCsj17603—dot11ARP cache does not use client MAC address when sending ARP response.

When the **dot11 arp-cache** feature is enabled and if a given ARP entry is cached, the access point responds to an ARP request with its own MAC address. However, the source MAC address in the ARP payload is correct.

Conditions—This caveat affects all autonomous access points in root AP mode.

Workaround—None.
- CSCsj25335—IP Redirect feature towards DNS packet is not documented.

However, the *IP Redirection Application Note* mentions that BOOTP/DHCP, DNS, and broadcast data should not be redirected.

When the IP Redirect feature is configured under the dot11 radio interface, the destination MAC address of the DNS Packet is rewritten with the host Mac Address specified under the **ip redirect host <IP address>** command.
- CSCsj20308—SNMP object not available for RSSI

A bridge running Cisco IOS release 12.3(8)JA2 or 12.3(11)JA1 code fails to return a value for Object cDot11ClientSignalStrength, OID 1.3.6.1.4.1.9.9.273.1.3.1.1.3 while there is a value in the CLI for signal strength in the output of the **show dot11 associations all-client** command.

Workaround—None, except to use the CLI value.
- CSCsj03312—Low on memory and traceback message appears on workgroup bridge for EAP-TLS authentication.

Workaround—Make sure that correct user name and password is entered correctly, and make sure that certificate entered is valid.
- CSCsi97928—NAC clients with WPA not working on non-native VLAN when using dynamic VLAN assignment.

Workaround—Do not use dynamic VLAN assignment.
- CSCsj08967—1242 access point rebooted with unknown reload cause - reason ptr 0xF, PC 0x135EF0, address 0x0.

Workaround—None.

- CSCsj38156—CLI command **show controllers** displays AIR-AP1131G radio type.
The output of the **show controllers** command shows the type of the radio as AIR-AP1131G, which is incorrect.
Workaround—None.
- CSCsi98692—1230B-K9 access point reloads for unknown reason.
Workaround—None.
- CSCsd99067—AVVID priority map incorrectly maps COS 5 to COS 7 within same VLAN.
The AVVID priority mapping in the CoS advanced parameters is incorrectly mapping the CoS value to 7 when making a call to a wired phone in same VLAN. This situation occurs in an 802.11g network running one 7921 and one access point.
Workaround—None.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.4(3g)JA1:

- CSCek46661—VLAN assignment no longer fails when using local radius server.
- CSCse02766—Repeater clients are now able to connect hosts on the DS.
- CSCsf95975—Access point no longer crashes when AeroScout server address is misconfigured.
- CSCsg30911—IEEE802dot11-MIB objects are no longer showing out of range values.
- CSCsg59063—Control Plane Policing is no longer available.
- CSCsh43635—Frequent tracebacks on WDS process no longer occur.
- CSCsi04754—EAP-FAST now operates correctly with Local RADIUS server if LEAP is disabled.
- CSCsi08181—A valid interface is available when reloading a root bridge on a point-to-multipoint configuration.
- CSCsi23996—Access point no longer fails when issuing a **dot11_arp_cache_zero_remove** command.
- CSCsi25620—Bridge timers now operate normally for workgroup bridge.
- CSCsi32429—Radio Scan job no longer fails on scanning access points.
- CSCsi34566—Calls can now be made with CAC/TSPEC enabled.
- CSCsi35780—LRS-EAP-FAST operates normally when a workgroup bridge is used as the supplicant.
- CSCsi35908—Workgroup bridge no longer fails while deleting CAC calls.
- CSCsi35911—Channel list for least congested frequency can now be restricted.
- CSCsi68728—Traceback is no longer observed while clearing wlccp wds statistics.
- CSCsi73614—CB21AG 5-GHz client now obtains IP address after roaming back to repeater.

- CSCsi80169—SSH can now be disabled using the GUI.
- CSCsi80249—CKIP SEQ replay is no longer detected on root and repeater access points when mic-key-hash is enabled.
- CSCsi82424—Control-plane config item no longer shows error on boot.
- CSCsi86433—1230 series access point now reads reg Domain from its radio.
- CSCsi90721—Access point no longer fails while printing **s dot11 ass all** command.
- CSCsi92058—HTTPS access to AP functions normally after upgrading to 12.3(11)JA.
- CSCsi99890—LSS on a workgroup bridge is now configurable on the GUI.
- CSCsj03443—Authenticate, enroll, and certificate configuration is now available using the GUI.
- CSCsj10551—WGB now sends IAPP message for static bridge entries.
- CSCsj44081—Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures. This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

Details: The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp: May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error. The error message is then followed by a traceback.

If You Need More Information

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

<http://tools.cisco.com/Support/BugToolKit/>

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

Troubleshooting

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

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>

CCVP, the Cisco logo, and the Cisco Square Bridge logo 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, BPX, 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, Networking Academy, Network Registrar, *Packet*, 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. (0705R)

© 2007 Cisco Systems, Inc. All rights reserved.