Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 12.4(10b)JA

October 26, 2007

These release notes describe features, enhancements, and caveats for special technology early deployment release Cisco IOS Release 12.4(10b)JA. This release supports 32-MB Cisco autonomous access points, including Cisco Aironet 1130, 1240, and 1250 series access points, 1300 series access point/bridges, and 1400 series bridges.

Contents

These release notes contain the following sections:

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, 1240, 1250 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

System Requirements

You can install Cisco IOS Release 12.4(10b)JA on all 1130, 1240, 1250 series access points, 1300 series outdoor access point/bridges, and 1400 series bridges.

Finding the Cisco IOS Software Release

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 release 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 release 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

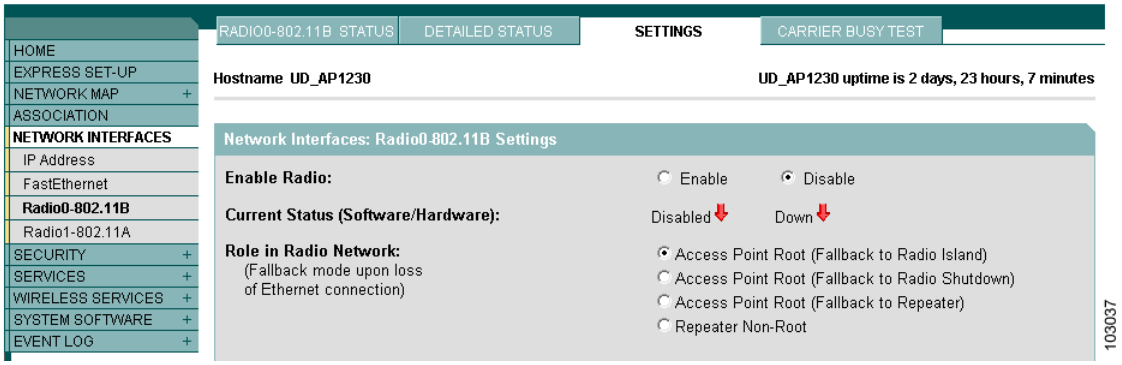
Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

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(10b)JA has the following new features:

- Support for Cisco Aironet 1250 Series Access Points
- Regulatory update for Japan

Support for Cisco Aironet 1250 Series Access Points

The Cisco Aironet 1250 Series Access Point is the industry's first business-class access point based on the IEEE 802.11n draft 2.0 standard. It provides reliable WLAN coverage to improve the end-user experience for both existing 802.11a/b/g clients and new 802.11n clients. The access point offers combined data rates of up to 600 Mb/s to meet the most rigorous bandwidth requirements. Users can now rely on wireless networks to deliver a similar experience to wired networks, providing mobile access to high-bandwidth data, voice, and video applications, irrespective of their location.

The Cisco Aironet 1250 Series Access Point is a next-generation wireless solution with unparalleled throughput and improved reliability and predictability for wireless connectivity. The robust Cisco Aironet 1250 series is a modular platform designed to be easily field-upgradable to support a variety of wireless capabilities. This modularity allows businesses to deploy existing wireless technologies today with the confidence that their network investment will extend to support emerging and future wireless technologies.

Detailed information and configuration procedures for the 1250 series access point are in Chapter 6 of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(10b)JA & 12.3(8)JEC*, which is available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps6973/tsd_products_support_series_home.html

Note The 802.11n HT rates apply only to no encryption or WPA2/AES encryption. They do not apply to WEP or WPA encryption. If WEP or TKIP encryption is used, the 1250 series access points and any 802.11n Draft 2.0 clients will not transmit at the HT rates. Legacy rates (802.11a/b/g) will be used for any clients using WEP or TKIP encryption.

Note For 1250 series access points, the maximum throughput for encrypted downstream traffic is lower than expected at higher data rates. (CSCsk07386)

Regulatory Update for Japan

This release supports the U regulatory domain for the W52 frequency set (channels 36, 40, 44, and 48) in Japan for the Cisco Aironet 1200 and 1230 Series. This support was added for the Cisco Aironet 1130 and 1240 series in Cisco IOS Software Release 12.4(3G)JA, which shipped previously. 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 this URL:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

Installation Notes

This section contains information that you should keep in mind when installing 1130, 1240, 1250 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, 1240, and 1250 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

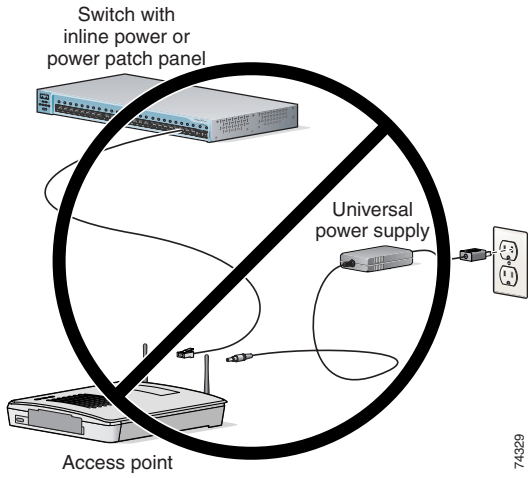
This section describes issues that you should consider before applying power to an access point.

Caution Cisco Aironet power injectors are designed for use only 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 2 shows the power configuration that can shut down the port on the patch panel or powered switch.

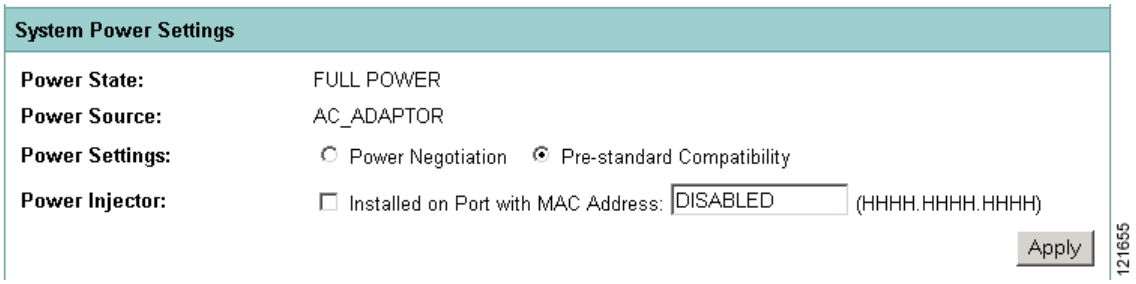
Figure 2 Improper Power Configuration Using Two Power Sources



Configuring Power for 1130 , 1240, and 1250 Series Access Points

The 1130, 1240, and 1250 series access points disable the radio interfaces when the connected power source 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 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 access points and bridges.

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
```

Bridge Configuration Not Tested on 1250 Series Access Point

Bridging functions have not been tested on the 1250 series access point even though bridge configuration commands are available.

Access Points Send Multicast and Management Frames at Highest Basic Rate

Access points running recent Cisco IOS versions are transmitting multicast and management frames at the highest configured basic rate, and is a situation that could causes reliability problems.

Access points running LWAPP or autonomous IOS should transmit multicast and management frames at the lowest configured basic rate. This is necessary in order to provide for good coverage at the cell's edge, especially for unacknowledged multicast transmissions where multicast wireless transmissions may fail to be received.

Since multicast frames are not retransmitted at the MAC layer, stations at the edge of the cell may fail to receive them successfully. If reliable reception is a goal, then multicasts should be transmitted at a low data rate. If support for high data rate multicasts is required, then it may be useful to shrink the cell size and to disable all lower data rates.

Depending on your specific requirements, you can take the following action:

- If you need to transmit the multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, one that is low enough to reach the edges of the wireless cells.
- If you need to transmit the multicast data at a certain data rate in order to achieve a certain throughput, then configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of non-multicast clients.

Low Throughput Seen on 1250 Series Access Points with 16 BSSIDs Configured

If your network uses 16 BSSIDs with 1- and 2-Mbps data rates, 1250 series access points might experience very low throughput due to high management traffic.

802.11n HT Rates Apply Only to No Encryption or WPA2/AES Encryption

The 802.11n HT rates apply only to no encryption or WPA2/AES encryption. They do not apply to WEP or WPA encryption. If WEP or TKIP encryption is used, the 1250 series access points and any 802.11n Draft 2.0 clients will not transmit at the HT rates. Legacy rates (802.11a/b/g) will be used for any clients using WEP or TKIP encryption.

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 Caveats, Resolved Caveats, and Closed Caveats for access points and bridges in Cisco IOS Release 12.4(10b)JA.

Open Caveats

These caveats are open in Cisco IOS Release 12.4(10b)JA:

- 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.

- 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.

- 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
```

- CSCsf06407—Packets from Cisco 7920 phones always fall into the COS 6 queue. This problem occurs when the stream feature is enabled.

  Workaround: None.

- CSCsf14351—Medium time restriction affects built-in bridge functionality on Theseus.
- CSCsf27222—Unable to maintain more than 7 voice calls.

  Workaround: None.

- 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).

- CSCsg80305—When 16 SSIDs are configured, client devices sometimes fail to associate to the 16th SSID.

  Workaround: Save the configuration and reload the UC520.

- CSCsg88872—Client devices can sometimes associate to an access point when WEP is set to optional on the client but set to required on the access point.

  Workaround: None.

- 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.

- CSCsh44876—The access point incorrectly lists client wired interface IP addresses in *show dot11 assoc* command output and in the association table.

  Workaround: None.

- 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.

- CSCsi10705—The trhoughput on dual-radio 1200 series access points is sometimes lower than the throughput on a single-radio 1200 series access points.

  Workaround: None.

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

  Workaround—Reset the access point.

- CSCsi70230—Tracebacks and a memory allocation error sometimes occur on 1310 series bridges during a software upgrade.

  Workaround: None.

- 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.

- 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.

- CSCsj53216—Supplicants sometimes fail to receive DHCP addresses when the access point changes the VLAN at logon.

  Conditions: EAP authentication with access point in VLAN x and client device in VLAN y.

  Workaround: If possible, put the access point and the client device in the same VLAN.

- CSCsj68025—Wireless clients correctly roam between access point 1 and access point 2 but after a few roaming events, roaming fails.

  Conditions: Two autonomous 1242 access points configured for bridging between them using interface dot11radio 1 and WPA-PSK. The interface dot 1 of access point 1 is configured as station-role root bridge while the same interface on access point 2 is configured as station-role non-root bridge. They correctly associate using SSID1 and traffic can pass. Both access points also are configured with the interface dot11radio 0 as station-role root offering connectivity to wireless clients using SSID2 with WPA-PSK. The interfaces dot 0 and dot 1 of each access point are bridged using the same bridge-group so that traffic can flow from wireless clients to one access point and through the bridge to the other access point.

  Workaround: None.

  Further Problem Description: The reason for this failure is that the IAPP disassociation info sent from one access point to the other is not correctly sent over the bridge; therefore both access points report the wireless client as “locally associated” and the WPA authentication fails.

- CSCsj86643—When you use the a workgroup bridge (WGB) to simulate a WMM/TSPEC client, the WGB/pagent-sourced UP 6 traffic (followed by a TSPEC) is downgraded to best effort when ACM is enabled. This downgrade occurs because the access point and WGB shared driver code assumes that the workgroup bridge is an access point and the uplink traffic is invalid, and thus downgrades all packets.

  Workaround: None.

- CSCsj88333—When Dot11 ARP cache is enabled on an access point, the access point puts 0 in the VLAN field of the 802.1q header when it sends out ARP responses on behalf of associated wireless clients. Thus, the ethernet switch considers the ARP response is for the native VLAN. As a result, the device sending ARPs for the wireless client may not receive the ARP response.

  Conditions: The problem first appeared in Cisco IOS Release 12.3(8)JA. Dot11 ARP cache is enabled and the associated wireless clients are on the non-native VLAN. An output ACL is configured on the radio interface.

  Workaround: Configure the SSID on the native VLAN; or disable dot11 ARP cache; or remove the output ACL from the dot11radio interface.

- CSCsk05871—Sometimes packets are not marked as voice to 7921 phones.

  Condition: A 7921 phone talking to a non-WMM client (a 7920 phone, for example), a wired client, or another 7921 client with WMM disabled.

  Workaround: None.

- CSCsk13961—The following MIB objects display incorrect values for 802.11n radios in 1250 series access points:
  - cd11IfAssignedSta
  - cd11IfPhyMacSpecification
  - cd11IfPhyDsssMaxCompatibleRate
  - cd11IfErpOfdmTxPowerLevel5
  - cd11IfClientCurrentTxPowerLeve1

  Workaround: None.

- CSCsk23262—A change in WDS units sometimes triggers shutdown of the radios in an access point in hot standby mode.

  The backup Hot Standby unit takes over as the primary Hot Standby unit when the WDS changes from primary to backup.

  Workaround: Adjust cell coverage so that Hot Standby unit can hear only its parent access point. When the WDS change happens, all the clients attached to access point receive a deauthentication message, and they are forced to reassociate. When the backup Hot Standby unit receives the deauthentication message, it can join any access point with matching credentials.

- CSCsk28551—A root bridge sometimes fails to update its bridge table for clients that are connected to an access point behind a workgroup bridge when these clients reload.

  Workaround: Perform a shut and no-shut radio interface operation on the root bridge.

- CSCsk35829—On 1410 series bridges, you can select WPAv2 as a WPA setting even though AES encryption is not supported on 1410 series bridges.

  Workaround: None.

- CSCsk40578—When the access point radio interface is reset, the access point sends a deauthentication message to the associated wireless clients and removes the client entries from its association table. The existing PMK cache is not cleared for the WPAv2 clients. However, the access point should clear the PMK cache because clients do a full re-authentication.

  Workaround: None.

- CSCsk44106—SNMP returns incorrect cipher values for some clients when multiple ciphers are defined on an interface. This condition only affects some of the clients when there are multiple ciphers on the interface.

  Workaround: None.

- CSCsk58820—Station roles have different possible RTS threshold values (some 4000 some 2347).

  Workaround: None.

- CSCsk63453—Tracebacks occur on 1200 series access points when the Taiwan carrier set is enabled.

  Workaround: None.

- CSCsk65207—1310 series bridges sometimes ignore a fixed channel under the dot11radio0 interface even when it is the least congested channel.

  Workaround: None.

- CSCsk78264—A change in the RF domain name takes effect only after a reboot.

  Workaround: Reboot the controller after changing the RF domain name.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.4(10b)JA:

- 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 is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6

- CSCsc04907—Resetting the access point to factory defaults does not clear the static IP address.
- CSCse49342—DHCP_SERVER_FAILURE observed in 1300 series in WGB mode.
- CSCsg69625—The access point does not mark the DSCP on the IP GRE header.
- CSCsg71454—System sometimes restarts because of unknown reload cause.
- CSCsg71997—Hostname not assigned to access point when IP address obtained from DHCP server.
- CSCsh17037—In rare circumstances, a memory leak may develop in the SSH process.
- CSCsi10234—An access point in HREAP mode sometimes gets out of sync with the controller on which WLANS are active if the access point loses connection with the controller and the WLAN configuration on the controller is changed.
- CSCsi18135—Add dynamic WLAN functionality for Diagnostic WLAN.

- CSCsi23423—Radio restart occurs 1131 series access points connected to a 4402-50 controller running software release 4.0.206.0.
- CSCsi55490—The controller does not support IGMP snooping and access point group VLANs.
- CSCsi60004—Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager.
- CSCsi73614—A CB21AG 5GHz client adapter sometimes fails to receive an IP address after roaming back to a repeater access point.
- CSCsi90532—The Supported Features Advertisement Information Element (SFA IE) is not transmitted in association responses.
- CSCsi92058—HTTPS access to the access point does not work after upgrading to Cisco IOS Release 12.3(11)JA.
- CSCsi97928—NAC clients with WPA not working on non-native VLAN when using dynamic VLAN assignment.
- CSCsj17603—dot11ARP cache does not use client MAC address when sending ARP response.
- CSCsj22047—User is unable to modify or disable Key Management for a configured SSID.
- CSCsj30069—Nonroot bridge fails to associate if native VLAN is not 1.
- CSCsj38156—CLI command **show controllers** displays AIR-AP1131G radio type.
- CSCsj52519—You cannot set the access point primary trustpoint on the access point GUI.
- CSCsj63868—The **fallback shutdown** command does not configure the specified channel.
- CSCsj73804—Idle timeout may take up to three times as long as the configured period when the last frame received from a client had the powersave bit set.
- CSCsj76233—The 802.11n MIBs require improvements.
- CSCsk19943—An access point in HREAP mode initally forwards packets to the controller before dropping data locally.
- CSCsk42419—The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

  The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

  The Security Advisory for this issue is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080521-ssh
- CSCsk60020—The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

  The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

The Security Advisory for this issue is posted at

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080521-ssh

- CSCsl22707—A 1250 series access point using Power over Ethernet (PoE) continually resets when connected to a Catalyst 3550 series switch. This problem is resolved by a new bootloader. New 1250 series access points shipped from the factory contain the new bootloader image [12.4(18a)JA1]. Do not, however, attempt to replace the bootloader in 1250 series access points in the field. Instead, follow the instructions in the workaround below.

  Workaround: For 1250 series access points in the field, use either a power injector or an AC power supply to provide power to the access point, or upgrade the switch to IOS Release 12.1(19)EA1 or later and enter this CLI command to configure the switch to continue providing power during initialization:

  power inline delay shutdown *seconds* **initial** *seconds*

  where **shutdown** *seconds* is the amount of time that the switch continues to provide power to the device after linkdown (between 0 and 20 seconds) and **initial** *seconds* is the initial time that the power shutdown delay is in effect (between 0 and 300 seconds).

  Without this command, the switch removes power immediately when a linkdown occurs on the connected device.

Closed Caveats

These caveats have been closed and will not be addressed:

- CSCse47224—If wireless clients attempt to authenticate at a very high rate (more than three to five authentication attempts per second) using PEAP through an autonomous IOS access point that uses WPA2 for key management and AES encryption, some of the authentication attempts might fail.

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