Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Releases 12.4(25d)JA and 12.3(8)JEE

December 2010

These release notes describe features, enhancements, and caveats for special technology deployment release Cisco IOS Release 12.4(25d)JA. This release supports 32-Mb autonomous Cisco Aironet 1040, 1130, 1140, 1240, 1250 and 1260 series access points, and 1300 and 1400 series access points/bridges. It also supports the Cisco IOS Release 12.3(8)JEE for the 16-Mb autonomous Cisco Aironet 1100, 1200, and 520 series access points..

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.

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

You can configure and monitor 520, 1040, 1100, 1130, 1140, 1200, 1240, 1250,1260 access points, and 1300 and 1400 series access points and bridges by using the command-line interface (CLI), the web-browser interface, or Simple Network Management Protocol (SNMP).

System Requirements

You can install the 32-Mb Cisco IOS Release 12.4(25d)JA on all 1040, 1130, 1140, 1240, 1250 and 1260 series access points. You can also install the16-Mb Cisco IOS Release 12.3(8)JEE on all 520, 1100, and 1200 series access points.

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(25d)JA:

```
ap1260AG> show version
Cisco IOS Software, C1260 Software (AP3G1-K9W7-M), Version 12.4(25d)JA
Copyright (c) 1986-2010 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 and Documentation page appears.

Step 3 Under the Select a Product Name, click **Wireless**. The Product/Technology Support page appears.

Step 4 Under the Make a Selection to Continue section, click **Access Point**. Products and Access Point are highlighted.

Step 5 Select the access point model for which you need the information. For example, click the **Cisco Aironet 1260 Series.** A list of documents appears.

Step 6 Click **Configure**. A list of configuration documents appears.

Step 7 Click **Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(25d)JA**.

Step 8 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

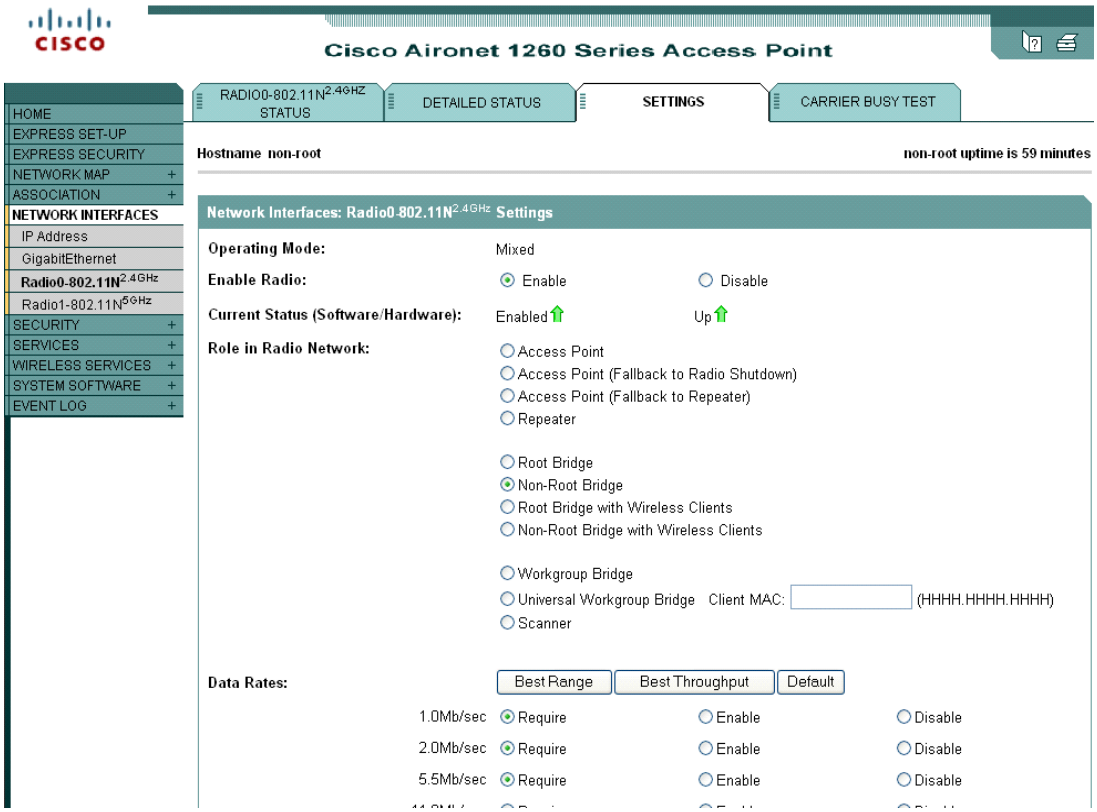
Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

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(25d)JA has the following new features:

- Support for an autonomous (standalone) Cisco Aironet 1040 and 1260 Series Access Points
- CLI for Framed Access Support
- Support a new -R Russian Federation AG Regulatory Domain
- WGB VLAN Tagging
- MAR Support
- WGB Wireless Client Support

Support for Cisco Aironet 1040 and 1260 Series Access Points

The Cisco Aironet 1040 and 1260 Series Access Points are business-class access points 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 approximately 444.2 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 1040 and 1260 Series Access Points are the next-generation wireless solution with unparalleled throughput and improved reliability and predictability for wireless connectivity. The robust Cisco Aironet 1260 series is aesthetically designed and provides enhanced power requirements as compared to previous 11n access point's (1250). This allows businesses to deploy existing wireless technologies today with the confidence that their network investment will extend to support emerging and future wireless technologies.

Note The c1260 access point uses the “ap3g1-k9w7-tar” image.

Note The c1040 access point uses the same image as the c1140 access point, which is the “c1140-k9w7-tar” image.

Detailed information and configuration procedures for the 1040 and 1260 series access point are in Chapter 6 of the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(25d)JA & 12.3(8)JEE*, 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 1040, 1140, 1250, and 1260 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.

CLI for Framed Access Support

Framed attribute is supported with the Autonomous 1040 and 1260 Series Access Points. A new option "framed" is added to the existing CLI "dot11 aaa authentication attributes service." This allows you to configure service types as "login" or "framed" depending on the user requirement. CLI syntax:

```
router(config-t) dot11 aaa authentication attribute service [login-user | framed-user]
```

By default the service type "login" will be sent in the access request.

Russian Federation AG Regulatory Domain

A new Russian Federation regulatory domain -R is defined for this release. This new regulatory domain is supported on the Cisco Aironet 1040 and 1260 Series Access Point platforms. The new -R domain is supported on 5G radios and has new power tables and channel selections. Because the channel selections change frequently, they are not included in this document. For up-to-date information on channel settings for your access point, see the *Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges* document. This document is available on cisco.com at the following URL:

http://www.cisco.com/en/US/docs/wireless/access_point/channels/ios/reference/guide/atonchp2.html

WGB VLAN Tagging

The Workgroup-Bridge (WGB) VLAN tagging feature enables segregation of VLAN traffic based on the VLAN numbers.

When this feature is enabled, the WGB removes the 802.1q header while sending the packet from a VLAN client to the wireless LAN controller (WLC). WGB gets the packet to a VLAN client without 802.1q header and WGB code has to be modified to add the 802.1q header while forwarding the frame to the switch behind WGB.

WGB updates the WLC with the wired-client VLAN information in the Internet Access Point Protocol (IAPP) Association message. WLC treats the WGB client as a VLAN-client and forwards the packet in the right VLAN interface based on the source-mac-address.

In the upstream direction, WGB removes the 802.1q header from the packet while sending to the WLC. In the downstream direction while forwarding the packet to the switch connecting the wired-client, the WLC sends the packet to WGB without the 802.1q tag and WGB adds a 4-byte 802.1q header based on the destination mac-address.

Enter this command to enable WGB VLAN tagging:

```
WGB(config)#workgroup-bridge unified-vlan-client ?
        -replicate  Enable WGB broadcast to all vlans
        <cr>
```

MAR Support

This release of IOS supports the Cisco 3201 Wireless Mobile Interface Card (WMIC) in the 3200 Series Mobile Access Router (MAR). It does not support the following WMIC modules:

- Cisco 3205 Wireless Mobile Interface Card (WMIC)
- Cisco 3202 Wireless Mobile Interface Card (WMIC)

Note Use the **c3201-k9w7-tar** autonomous image for 3201 WMIC.

WGB Wireless Client Support

The WGB wireless client support feature allows the WGB to retain the connectivity to wireless clients in the other radio even if it lost its uplink in the current radio.

Installation Notes

This section contains information that you should keep in mind when installing 1040, 1130, 1140, 1240, 1250 and 1260 series access points, and 1300 and 1400 access points/bridges.

Access Points

This section contains installation notes for access points.

Installation in Environmental Air Space

Cisco Aironet 1040, 1130, 1140, 1240, 1250 and 1260 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.

Antenna Installation

For instructions on the proper installation and grounding of external antennas for 1260 series access points, refer to the National Fire Protection Association's *NFPA 70, National Electrical Code*, Article 810, and the Canadian Standards Association's *Canadian Electrical Code*, Section 54.

Warning **Do not install the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death.**

Important Notes

This section describes important information about access points and bridges.

Cisco 1040/1140 Series Access Points May Record "watchdog timer expired" as Last Reset Reason

The following error message sometimes appears as the last reset reason when the access points are power cycled:

```
Watchdog timer expired
```

This symptom is observed only in Cisco 1040/1140 Series Access Point and does not have any impact on functionality. Ignore the watchdog timer expired after power cycled. You can also overwrite the reset reason to"reload" by rebooting with command operation.

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.

Point-to-point and Point-to-Multipoint bridging support for 802.11n platforms

The point-to-point and point-to-multipoint bridging is supported on the Cisco Aironet 1040, 1130, 1140, 1240, 1250 and 1260 Series Access Points (802.11n platforms). The 5 GHz bands support 20- and 40-MHz and the 2.4-GHz bands support 20 MHz.

The following items are supported for AP1040 and AP1260 bridging:

- MIMO, short-range bridging (on campus or inter-building bridge deployments), with dipole and MIMO antennas (line of sight and short range) under 1 Km.
- 20-MHz and 40-MHz 802.11n support.
- Workgroup bridge (WGB) short-range support.
- SISO (single-in, single-out), MCS 0-7 and legacy bridge rates (802.11 a/b/g and 802.11n) using one outdoor antenna.

Note This is only supported using short range links and is not a replacement for the AP-1240/1300/1400 or other Bridge products.

The following items are not supported for AP1040 and AP1260 bridging:

- The distance CLI command; long-range links over 1 Km currently are not supported, so the distance command is not supported.
- Outdoor MIMO bridging using external antennas has not been fully tested and is not fully supported with this release.

Access Points are Transmitting Multicast and Management Frames

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 1260 Series Access Points with 16 BSSIDs Configured

If your network uses 16 BSSIDs with 1- and 2-Mbps data rates, 1260 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 1040, 1130, 1140, 1240, 1250, or 1260 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:

```
AP1260AG(config)# interface d1
AP1260AG(config-if)# shut
AP1260AG(config-if)# no mbssid
AP1260AG(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.

The Cisco Aironet 1250 and 1140 Series Access Points Have a Hardware Limitation

The beacons on the Cisco Aironet 1250 and 1140 Access Points can only have output at intervals that are multiples of 17 milliseconds. When these access points are configured for a 100 millisecond beacon interval, they transmit beacons every 102 milliseconds. Similarly, when the beacon interval is configured for 20 milliseconds, these access points transmit beacons every 17 milliseconds.

Potential RFC 3748 Violation

When the following command is configured under the SSID settings (for LEAP authentication):

```
authentication client username <WORD> password [0 | 7] <LINE>
```

If the first access-challenge returned by the Radius server after the access-request from the access point is not for the LEAP method but for EAP-MD5, the acces point violates RFC 3748.

Instead of sending an EAP NAK requesting LEAP authentication, the access point sends the user's credentials with EAP-MD5 and drops the derived keys, since it cannot read the EAP-MD5 from the access-accept.

This violates RFC 3748.

The workaround for this is to use the commands `dot1x credentials` and `dot1x eap profile` for LEAP authentication.

For configuration procedures, see *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, x.x.*

Caveats

This section lists Open Caveats and Resolved Caveats for access points and bridges in Cisco IOS Release 12.4(25d)JA. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in boldface type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

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

To become a registered cisco.com user, go to the following website:

http://www.cisco.com/RPF/register/register.do

Open Caveats

Table 1 lists caveats that are open in Cisco IOS Release 12.4(25d)JA.

Table 1 Open Caveats

Identifier	Headline
CSCsv82129	Lithium: "dot11_mgmt: bad cookie" error msg appear in WGB with open auth
CSCsx21409	AP1252/AP1142 TKIP and CCMP replays generated on queued multicast frames
CSCsz81157	Security changes disable 11n capability
CSCta57157	Client MAC Spoofing generated because WDS username not captured.
CSCta75163	BR1310 - Leap to wpa-psk migration failed
CSCtb02087	Lithium:The 1140 thruput about 70% of H for 1400byte packets in dual mode
CSCtg54769	TKIP MIC failures observed in WGB and root during CCKM fast roam
CSCti98577	Mercury : configuring eap-tls on wgb crash and traceback observed.
CSCtk35949	WLSM based L3 CCKM roaming not working for WGB

Resolved Caveats

Table 2 lists caveats that are resolved in Cisco IOS Release 12.4(25d)JA.

Table 2 Resolved Caveats

Identifier	Headline
CSCso17545	1230 ios ap crash due to sys-2-MALLOCFAIL.
CSCtb42068	Autonomous: Remove 40MHz option for 2.4GHz band
CSCtb47581	WLSE 1030 tftpboot/public directory does not exist in HA enabled WLSEs.
CSCtd32301	J: TSF timestamp is out of sync with beacon.

Identifier	Headline
CSCtd10712	The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols: – NetMeeting Directory (Lightweight Directory Access Protocol, LDAP) – Session Initiation Protocol (Multiple vulnerabilities) – H.323 protocol All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation. Cisco has released free software updates that address these vulnerabilities. This advisory is posted at this URL: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.
CSCtd58904	AP crash on SNMP query
CSCte05605	WGB connectivity broken under de-auth attack when enabled client MFP
CSCte08161	Cannot get IP address from server if key-management is “wpa optional”
CSCte89125	Auth flood may lead to high CPU or complete availability impact
CSCtf11449	Leth-MR: Changing encryption abruptly cause infra-AP to crash
CSCtf17125	Follow up for CSCte43374, Root AP still passes EAP log off during CCKM
CSCtf39372	Le-mr0.5 : Running radio scan cause transmitter to be stopped on AP
CSCtf39826	AP 1131 stops responding to Polycom phone
CSCtg03203	1142/1252 APs recognize 802.11n HT enabled clients as legacy ones
CSCtg03918	WGB CCKM fast roaming failed in 5Ghz due to CCKMIE time difference
CSCtg08806	WGB Roaming: Multicast getting dropped for WGB client after roaming
CSCtg09159	Radio may get stuck in RESET or DOWN state
CSCtg22356	1130 constant radio resets
CSCtg25046	WGB: EAP frame dropped due to delay on dot1x init
CSCtg35493	Packets wedge in radio interface input queue on 1250 AP
CSCtg41297	[IOS-AP]-Disabling telnet for a Cisco IOS AP shows back Enabled in GUI
CSCtg43290	BR1310 “Station-role root bridge wireless-clients” causes tx lock up
CSCtg57607	WGB fails to send IAPP update
CSCtg63099	NAV in CTS-to-self frame while Radio Monitoring is set as 0 msec
CSCth28681	Voice loss observed between 7921 while roaming
CSCth29519	BR1410 radio interface down after upgrade to 12.4(21a)JA
CSCth31685	Q-Bridge-MIB doesn't provide output for dot1qTP and dot1qStatic
CSCth49688	Mercury : WGB lost association on auth flood attack
CSCth50530	WLSM based L3 CCKM roaming not working for Autonomous AP

Identifier	Headline
CSCth57171	Mobile station CLI on WGB causes DHCP IP issues
CSCth70360	Mercury : WGB not getting DHCP IP address with wpa optional
CSCti25197	Mercury: WGB not getting IP address for wpa optional on aes-wep40/wep128.
CSCti45441	Mercury: C1200 loses BVI interface IP (eth int stops passing traffic)
CSCti47730	WGB IOS AP connection flapping to root AP
CSCti67700	Mercury : WLSE Not able to add customize floor map in location Manager
CSCti70007	Mercury : WGB does not retain the ip while roaming with mobile station
CSCti78833	Multicast reflected on infrastructure comm. is used and one intf is down
CSCti92884	Mercury : WLSE Not able to manage 1140 AP
CSCtj15586	Mercury : Association rsp timeout while WGB roaming with mobile station.
CSCtj50370	Mercury: c1040 stops beaconing shortly after switchover to hsb-active mode

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