Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 15.2(4)JA

August 2013
OL-29224-01

These release notes describe features, enhancements, and caveats for Cisco IOS Release 15.2(4)JA. This release supports these Cisco Aironet autonomous access points:

- AP 1040
- AP 801
- AP 802
- AP 1140
- AP 1550
- AP 1600
- AP 2600
- AP 3500
- AP 3600
- AP 1260

Note You cannot use HTTPS file transfer to upgrade to Cisco IOS Release 15.2(2)JB from previous releases. Because of the image size for this release, you must use TFTP or FTP file transfer for the upgrade. Refer to the upgrade instructions at this URL: http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap20-firmware.html#wp1035507

Contents

These release notes contain these sections:

Cisco Systems, Inc.
www.cisco.com

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.

System Requirements

You can install the 32 MB Cisco IOS Release 15.2(4)JA on all 1260, 1040, 1140, 3500i, 3500e, 3600i, 3600e, 2600i, 2600e, 1600i, 1600e, and 1550 series access points.

Finding the Cisco IOS Software Release

To find the version of Cisco IOS software that is 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 that is running Cisco IOS Release 15.2(4)JA:

```
ap1260AG> show version
Cisco IOS Software, C1260 Software (AP3G1-K9W7-M), Version 15.2(4)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

Note You cannot use HTTPS file transfer to upgrade to Cisco IOS Release 15.2(2)JA from previous releases. Because of the image size for this release, you must use TFTP or FTP file transfer for the upgrade. Refer to the upgrade instructions at this URL:
http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap20-firmware.html#wp1035507

To upgrade your access point or bridge software, follow these steps:

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, 15.2(4)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

The new Cisco IOS software is supported only in these versions of 1550 series :

Version	First VID with 128MB
1552C	VID 07
1552CU	VID 01 (all)
1552E	VID 04
1552EU	VID 01 (all)
1552I	VID 03
1552H	VID 04
1552S	VID 01 (all)

Converting a Lightweight Access Point Back to Autonomous Mode

You can convert an access point from lightweight mode back to autonomous mode by loading a Cisco IOS Release that supports autonomous mode. If the access point is associated with a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated with a controller, you can load the Cisco IOS release using TFTP.

The image files and their supported access points are listed in Table 1.

Table 1 Image File Names

Image File	Supported Access Point
Ap3g2	2600i/2600E, 3600i/3600E
Ap3g1	3500i/3500e, 1260I/1260E
Ap1g2	1600i/1600E
1520	1552C, 1552CU, 1552E, 1552EU, 1552S, 1552I, 1552H
1140	1040 and c1140

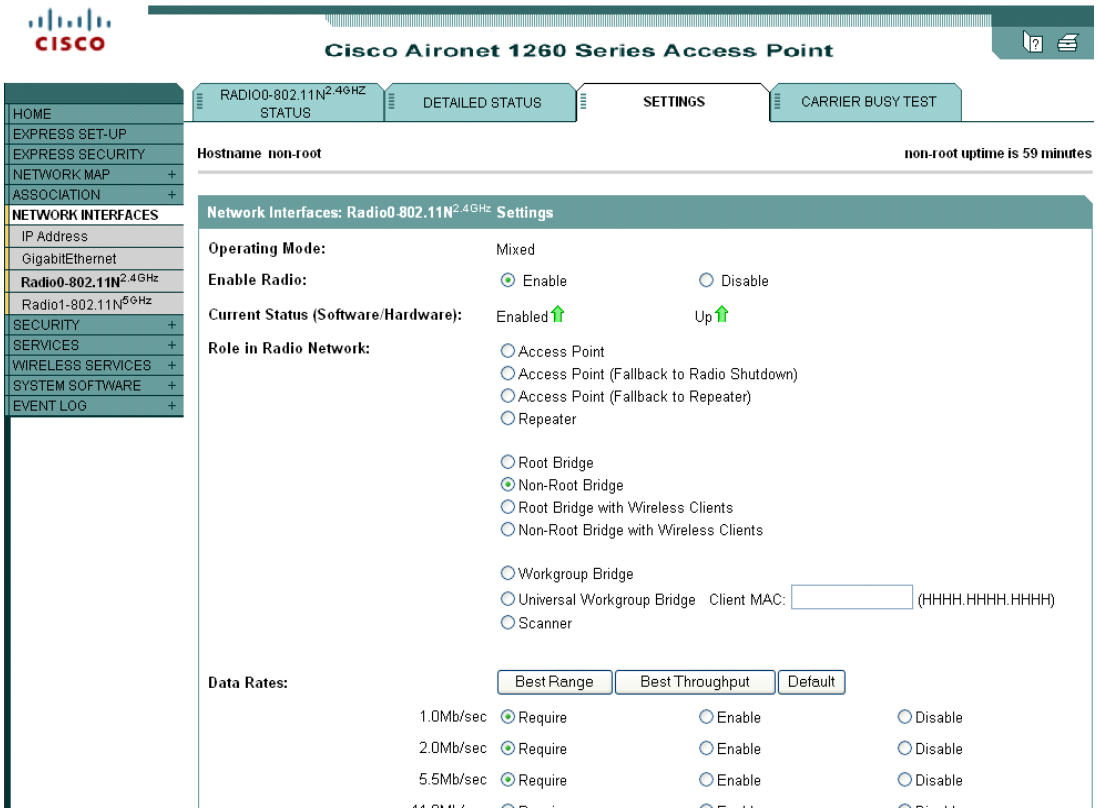
Disabling Radios to Prevent Unexpected Reboots When Upgrading the System Software

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 the software.

To disable the radio interfaces using the access point's web-browser interface, which you can access through the access point's Ethernet port, follow these steps:

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 Choose **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 access point CLI:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0** | **1**}	Enters 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**	Disables the radio port.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves 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.

Supported Browsers

These browsers are supported:

- Internet Explorer 8.x and later
- Firefox 3.x and later

New Features

Cisco IOS Release 15.2(4)JA has these new features:

- Support for IPv6, page 5
- Support for Guest Access, page 5
- Support for 802.11w, page 6

Support for IPv6

Cisco IOS Release 15.2(4)JA supports IPv6 protocols. IPv6 is the replacement internet protocol for IPv4. It uses 128 bit addresses as opposed to 32 bit addresses that are used in IPv4. Cisco IOS Release 15.2(4)JA supports these unicast addresses:

- Aggregatable Global Address: These addresses are globally routable and reachable on the IPv6 portion of the Internet. Global addresses are identified by the Format Prefix of 001.
- Link-Local Address: These addresses are automatically configured on interface using:
  - link-local prefix FE80::/10 (1111 1110 10)
  - interface identifier in the modified EUI-64 format

Support for Guest Access

Cisco IOS Release 15.2(4)JA supports guest access to the network. Guest networks provide access to the Internet and intranet without compromising the security of the host enterprise network.

Support for 802.11w

Cisco IOS Release 15.2(4)JA provides support for 802.11w protocol. Unlike encrypted data traffic, the management frames are sent in an unsecure manner while using the 802.11 protocol for data transfer. The standard 802.11w protocol ensures that the data transfer is secured by applying robust management frame protection protocols.

Installation Notes

This section contains information that you should keep in mind when installing 1260, 1040, 1140, 3500i, 3500e, 3600i, 3600e, 2600i, 2600e, 1600e, and 1550 series access points.

Access Points

This section contains installation notes for access points.

Installation in Environmental Air Space

Cisco Aironet 1040, 1140, 1250, 1260, and 2600 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 1550, 1260, 1600E, 2600, E3500E, and 3600E 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.

Use FTP or FTPS File Transfer to Upgrade to Cisco IOS Release 15.2(2)JB

You cannot use HTTPS file transfer to upgrade to Cisco IOS Release 15.2(2)JB from previous releases. Because of the image size for this release, you must use TFTP or FTP file transfer for the upgrade. Refer to the upgrade instructions at this URL:

http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap20-firmware.html#wp1035507

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

This 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 the Cisco 1040/1140 series access point and does not have any impact on functionality. Ignore the “watchdog timer expired” reason after an access point has been 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 1230 series. This support was added for the Cisco Aironet 1130 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 the U domain status with this release.

For the latest Cisco WLAN compliance status, 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, 1140, 1260, 1600, 2600, 3500 and 3600 series access points (802.11n platforms). The 5-GHz bands support 20 and 40-MHz channel widths, and the 2.4-GHz bands support only a 20-MHz channel width.

The following items are supported for AP1040, AP1140, AP1260, AP1600, AP2600, AP3500 and AP3600 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-1300/1400 or other bridge products.

The following items are not supported for AP1040, AP1140, AP1260, AP1600, AP2600, AP3500 and AP3600 bridging:

- The distance CLI command: long-range links over 1 km currently are not supported; therefore, 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 Transmit Multicast and Management Frames

Access points that are running recent Cisco IOS versions transmit multicast and management frames at the highest configured basic rate, which can cause reliability problems.

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

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

Depending on your specific requirements, these options are available:

- If you need to transmit multicast data with the greatest reliability and if there is no need for great multicast bandwidth, configure a single basic rate that is low enough to reach the edges of the wireless cells.
- If you need to transmit multicast data at a certain data rate in order to achieve a certain throughput, configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of nonmulticast 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 releases change the default behavior of access points that request an IP address from a DHCP server

When you connect a 1040, 1130, 1140, 1250, or 1260 series access point or a 1300 series outdoor access point/bridge with a default configuration to a LAN, the access point requests an IP address from a 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

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 that is defined to use authentication key-management WPA, together 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 multiple BSSIDs. When you add or delete multiple BSSIDs, check the association status of devices that are 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 reenable the radio, you must shut down the radio, disable multiple BSSIDs, and reenable the radio.

This example shows how to reenable the radio:

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

After you reenable 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 that are 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 versions.

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 you request for an IP address from the DHCP server, you might be locked out of the access point after it reboots if you do not have a local username and password configured on the access point. This issue does not affect access points that are configured with a static IP address. If you have been locked out, you 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 Upgrades

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.

Using the force-reload Option with archive download-sw Command

When you upgrade an 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 the 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 that runs Cisco 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 releases, 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 or Cisco Aironet 802.11g client devices.

Corrupt EAP Packet Sometimes Causes an 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 that is configured for Layer 3 mobility. Layer 3 mobility is not supported on repeaters and workgroup bridges.

Hardware Limitation in Cisco Aironet 1250 and 1140 Series Access Points

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 access 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 the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points.*

Autonomous AP Will Treat The Sub-interface Tied To Bridge-group1 As The Native Vlan

When using a configuration on an autonomous AP where there is no native VLAN defined, each interface is being dot1q tagged, communication will fail after upgrading to 15.2(2)JA or later. It appears that the configuration is still correct after the upgrade, but the AP sends the untagged frames for bridge-group 1, even though the encapsulation is not defined as native. The autonomous AP will treat the sub-interface tied to bridge-group 1 as the native VLAN, even if it is not defined with the native keyword: "encapsulation dot1 <vlan> native". The VLAN associated with bridge-group 1 must be set to native on the connecting switchport configuration

The workaround for this is to configure VLAN 100 as the native VLAN on the connected switchport trunk, even though the encapsulation is not specified as native on the AP.

IP Routing Enabled By Default

IP routing is enabled by default in 15.2(2)JB. This default configuration will render ip default-gateway statements inoperable. The workaround is to disable ip routing globally (config t, no ip routing), configure a default route instead of a default-gateway (e.g. config t, ip route 0.0.0.0 0.0.0.0 <default-gateway>), or disable IP routing using the following cli command:

no ip routing

DHCP Failure When Access Point Renewal Time Is Greater Than Rebind Time

An access point is unable to obtain IP through the same IOS DHCP server when the access point is running on 15.2x and the WLC has been upgraded from 7.2 to 7.3 or 7.4. The problem occurs because the Renewal (T1) time dhcp option 58 is larger than Rebinding (T2) time dhcp option 59.

Configuring the radius server using the old cli

This cli command was used in the previous releases to configure radius servers:

radius-server host {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Though this command can be still be used, we recommend that you use this new command:

radius server {server-name}[**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Caveats

This section lists Open Caveats and Resolved Caveats for access points and bridges in Cisco IOS Release 15.2(4)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:

https://tools.cisco.com/RPF/register/register.do

Open Caveats

Table 2 lists caveats that are open in Cisco IOS Release 15.2(4)JA.

Table 2 Open Caveats

Identifier	Headline
CSCud51131	CLI required to configure IPv6 SNTP server addresses.

Table 2 Open Caveats

Identifier	Headline
CSCue53185	The allowed frequencies are repeated in show controllers dot111 command for Japan regdomain.
CSCuf85579	Multicast downstream fails on a wlan client with security wpa2-tkip on enabling broadcast key rotation.

Resolved Caveats

Table 3 lists caveats that are resolved in Cisco IOS Release 15.2(4)JA.

Table 3 Resolved Caveats

Identifier	Headline
CSCud22555	WGB is unable to associate when configured for EAP with MFP disabled.
CSCud50794	On applying ACL, the Access Point either crashes, or traceback occurs.
CSCud51085	The AP GUI needs to be modified to enable IPv6 addresses to be configured.
CSCud66094	Client gets de-authenticated frequently.
CSCud73322	Cisco IOS software release upgrade fails after IPv6 collapse.
CSCud81067	WLAN client was connected as a web authenticated guest even after changing web authentication to web pass-through.
CSCud83443	Web authentication pass through does not work after reloading the software image.
CSCud83601	The dot11 radio interface is disabled due to PoE.
CSCud85688	Web authentication session timeout is not working for guest users.
CSCud86072	WGB wired client, connected as a guest access user, is unable to transfer TCP and UDP traffic.
CSCud90208	AP 1600 crashs due to failure of radio crypto FIPS self test.
CSCud92009	Data corruption and traceback error displayed in an Access Point while using the WLCCP show command.
CSCud93736	11n client does not connect to an AP with wpa2-aes.
CSCud95740	Unable to make TSPEC calls after the 802.11ac radio collapse.
CSCue02283	WGB is getting deauthenticated when 11w is enabled and deauthentication attack is done.
CSCue07764	WGB crashes after an upgrade.
CSCue08313	Access Point crashes and traces back due to low memory.
CSCue14936	WGB fails to roam on the on the second AP when two access points are configured using dot11r key management.
CSCue14942	Dot11Radio over air preauthentication does not work.
CSCue15779	IE 54 does not advertise overair or over DS-bit when modified.
CSCue32694	Workgroup bridge (WGB) and its clients cannot reach infra side via IPv6.
CSCue33102	QOS policy and class map are not supported on an Access Point.

Table 3 Resolved Caveats

Identifier	Headline
CSCue89182	The Access Point is unable to upgrade from previous software version to latest version through web-user interface.
CSCuf46502	Radio Resource Management (RRM) capabilities bit is set in autonomous Dot11 Radio1.
CSCuf46891	WGB does not get an IP on the native VLAN.
CSCuf84682	CPUHOG message followed by traceback is observed on booting up 1552EU.
CSCug30995	Upgrade to latest software image fails on the Cisco Aironet 3500 series access point as the access point gets stuck in the ROMMON mode.
CSCug43429	Layer 2 extended access list does not work on a non-native VLAN.
CSCue05062	The client devices that associate with the repeater can not associate with the root AP.
CSCue07208	GUI support for IPv6 ACL, Timers and Server Management for Autonomous AP must be provided.
CSCth42489	Multicast traffic stops on fast roaming. The number of access points is displayed incorrectly when an AP roams back within 20 seconds.

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