Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(11)JA1

January 18, 2007

This release is a maintenance release and contains no new features. These release notes list open and resolved caveats for Cisco IOS Release 12.3(11)JA1. They also provide important information about the Cisco Aironet 1130 and 1240 Series Access Points and 1300 Series Outdoor Access Point/Bridges.

Cisco IOS Release 12.3(11)JA1 supports autonomous 32 Mb platforms. 16 Mb platforms and platforms supported by Cisco IOS Release 12.3(8)JA and earlier (350, 1100, 1130, 1200, and 1230 series access points and 1300 series access point/bridge) are supported by Cisco IOS Release 12.3(8)JEA1.

Contents

These release notes contain the following sections:

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

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, and the 1300 series outdoor access point/bridge using the command-line interface (CLI), the web-browser interface, or Simple Network Management Protocol (SNMP).

System Requirements

You can install Cisco IOS Release 12.3(11)JA1 on all 1130, 1240 series access points, and 1300 series outdoor access point/bridges.

Finding the IOS Software Version

To find the version of IOS software running on your access point, use a Telnet session to log into the access point and enter the **show version** EXEC command. This example shows command output from an access point running Cisco IOS Release 12.3(8)JA:

```
ap1240AG>show version
Cisco Internetwork Operating System Software
IOS (tm) C1240 Software (C1240-K9W7-M), Version 12.3(8)JA
Copyright (c) 1986-2006 by Cisco Systems, Inc.
```

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

Upgrading to a New Software Release

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

Step 1 Follow this link to the Cisco home page:

http://www.cisco.com

Step 2 Click **Support**. Then click **Documentation** from the drop-down window. The Support Documentation page appears.

Step 3 Click **Wireless**. The Wireless Support Resources page appears.

Step 4 Scroll down to the Access Points section.

Step 5 Select the access point you are upgrading. The Introduction page for that access point appears.

Step 6 Under the Configure section, click **Install and Upgrade Guides**. A list of configuration documents appears.

Step 7 Select the appropriate **Software Configuration Guide.**

Step 8 Navigate to the Managing Firmware and Configurations 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

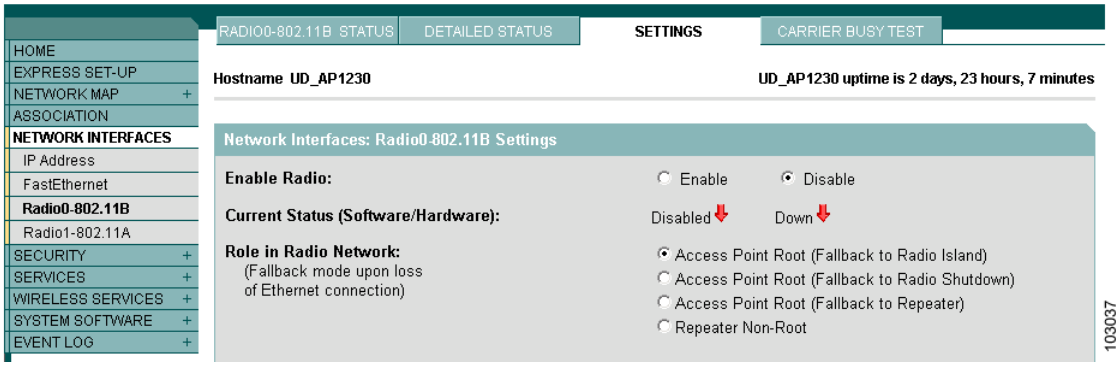
Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

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

No new features are introduced in Cisco IOS Release 12.3(11)JA1.

Installation Notes

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

Installation in Environmental Air Space

Cisco Aironet 1130 and 1240 Series Access Points provide adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the *National Electrical Code* (NEC) and Sections 2-128, 12-010(3) and 12-100 of the *Canadian Electrical Code*, Part 1, C22.1.

Caution The power injector does not provide fire resistance and low smoke-producing characteristics and is not intended for use in extremely high or low temperatures or in environmental air spaces such as above suspended ceilings.

Power Considerations

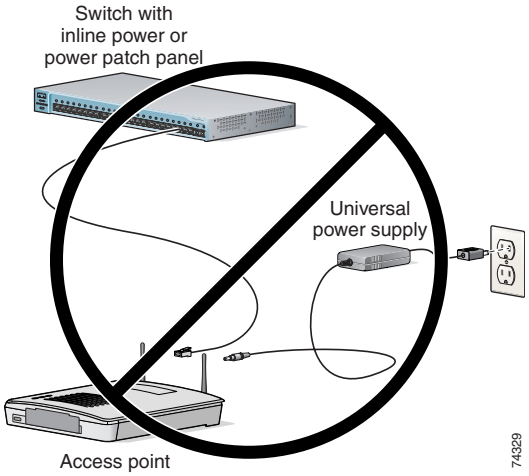
This section describes issues you should consider before applying power to an access point.

Caution Cisco Aironet power injectors are designed for use with Cisco Aironet access points and bridges only. *Do not use the power injector with any other Ethernet-ready device.* Using the power injector with other Ethernet-ready devices can damage the equipment.

Use Only One Power Option

You cannot provide redundant power to 1130 series access points with both DC power to its power port and inline power from a patch panel or powered switch to the access point's Ethernet port. If you apply power to the access point from both sources, the switch or power patch panel might shut down the port to which the access point is connected. Figure 2 shows the power configuration that can shut down the port on the patch panel or powered switch.

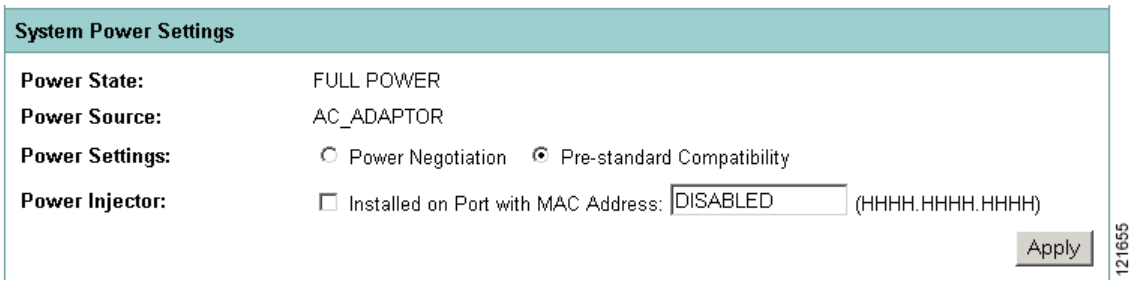
Figure 2 Improper Power Configuration Using Two Power Sources



Configuring Power for 1130 and 1240 Series Access Points

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

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



Using the AC Power Adapter

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

Using a Switch Capable of IEEE 802.3af Power Negotiation

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

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

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

Using a Power Injector

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

Antenna Installation

For instructions on the proper installation and grounding of external antennas for 1240 series access points, refer to the National Fire Protection Association's *NFPA 70, National Electrical Code*, Article 810, and the Canadian Standards Association's *Canadian Electrical Code*, Section 54.

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

Important Notes

This section describes important information about the access point.

CCKM and Fast Roaming on Cisco 7921/7925 IP Phones

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

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

DFS Not Supported on Certain 1130 Series Access Points

Due to FCC regulations, existing Cisco Aironet 1130AG Access Points with the FCC Identification Number LDK102054 are not able to software-upgrade to support Dynamic Frequency Selection (DFS) for the FCC. Even if these access points are upgraded to Cisco IOS Software Release 12.3(11)JA1, DFS for the FCC will not be enabled on the access point. New Cisco Aironet 1130AG Access Points that ship from the factory with Cisco IOS Software Release 12.3(11)JA1 and the FCC Identification Number LDK102054E will support Dynamic Frequency Selection (DFS) for the FCC.

Layer 3 Not supported with NAC for MBSSID

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

DFS Enabled by Default on 5-GHz Radios in North America

In this release, Dynamic Frequency Selection (DFS) is automatically enabled on 5-GHz radios configured for use in North America. The 5-GHz radios use DFS to detect radar signals and avoid interfering with them. Radios configured for use in Europe and Singapore also use DFS. Other regulatory domains do not use DFS. Refer to the "DFS Automatically Enabled on Some 5-GHz Radio Channels in North America" section on page 17 for detailed information.

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.

Save Interface Level Configuration Before Upgrading to Releases 12.3(11)JA1 or Later

If the access points have SSIDs configured at the interface level (rather than at the global level), before upgrading to Cisco IOS Release 12.3(7)JA and above, upgrade to Cisco IOS Release 12.3(4)JA, save the configurations and then upgrade to Release 12.3(11)JA1. This procedure must be followed to make sure that the SSID configurations are converted from the interface level to global level.

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

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

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

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

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

Default Username and Password Are *Cisco*

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

Some Client Devices Cannot Associate When QoS Is Configured

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

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

Some Devices Disassociate When Multiple BSSIDs Are Added or Deleted

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

Enabling MBSSIDs Without VLANs Disables Radio Interface

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

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

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

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

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

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

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

GRE Tunnelling Through WLSM Sometimes Requires MTU Setting Adjustments

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

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

TACACS+ and DHCP IP Address Sometimes Locks Out Administrators

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

Access Points Do Not Support Loopback Interface

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

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

Non-Cisco Aironet 802.11g Clients Might Require Firmware Upgrade

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

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

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

Use Auto for Ethernet Duplex and Speed Settings

Cisco recommends that you use **auto**, the default setting, for both the speed and duplex settings on the access point Ethernet port. When your access point receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link reboots the access point. If the switch port to which the access point is connected is not set to **auto**, you can change the access point port to **half** or **full** to correct a duplex mismatch and the Ethernet link is not reset. However, if you change from **half** or **full** back to **auto**, the link is reset and, if your access point receives inline power from a switch, the access point reboots.

Note The speed and duplex settings on the access point Ethernet port must match the Ethernet settings on the port to which the access point is connected. If you change the settings on the port to which the access point is connected, change the settings on the access point Ethernet port to match.

Use force-reload Option with archive download-sw Command

When you upgrade access point or bridge system software by entering the **archive download-sw** command on the CLI, you must use the **force-reload** option. If the access point or bridge does not reload the Flash after the upgrade, the pages in the web-browser interface might not reflect the upgrade. This example shows how to upgrade system software successfully using the **archive download-sw** command:

```
AP# archive download-sw /force-reload /overwrite tftp://10.0.0.1/image-name
```

Radio MAC Address Appears in ACU

When a Cisco Aironet client device associates to an access point running IOS software, the access point MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Radio MAC Address Appears in Access Point Event Log

When a client device roams from an access point (such as access point *alpha*) to another access point (access point *bravo*), a message appears in the event log on access point alpha stating that the client roamed to access point bravo. The MAC address that appears in the event message is the MAC address for the radio in access point bravo. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Mask Field on IP Filters Page Behaves the Same As in CLI

In Cisco IOS Release 12.2(8)JA and later, the mask that you enter in the Mask field on the IP Filters page in the access point GUI behaves the same way as a mask that you enter in the CLI. If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address that you entered in the IP Address field.

Repeater Access Points Cannot Be Configured as WDS Access Points

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

Cannot Perform Link Tests on Non-Cisco Aironet Client Devices and on Cisco Aironet 802.11g Client Devices

The link test feature on the web-browser interface does not support non-Cisco Aironet client devices nor Cisco Aironet 802.11g client devices.

System Software Upgrade Sometimes Fails Using Microsoft Internet Explorer 5.01 SP2

A system software upgrade sometimes fails when you use Microsoft Internet Explorer 5.01 SP2 to upgrade system software using the TFTP Upgrade page in the web-browser interface. Use a later version of Microsoft Internet Explorer to perform HTTP system software upgrades, or use TFTP to upgrade system software. Click this URL to browse to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for complete instructions on performing software upgrades:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/tsd_products_support_configure.html

Corrupt EAP Packet Sometimes Causes Error Message

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

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

You can ignore these messages.

When Cipher Is TKIP Only, Key Management Must Be Enabled

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

Cisco CKM Supports Spectralink Phones

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

Non-Cisco Aironet Clients Sometimes Fail 802.1x Authentication

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

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

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

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

Layer 3 Mobility Not Supported on Repeaters and Workgroup Bridges

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

WLSM Required for Layer 3 Mobility

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

Caveats

This section lists open and resolved caveats for access points.

Open Caveats

These caveats are open in Cisco IOS Release JA12.3(11)JA1:

- CSCsd99125— WDS may report an incorrect new channel to WLSE after a RADAR event

  During DFS event testing, it was discovered that if a DFS event was triggered on a non-root device, the WLSE sometimes received an erroneous new channel report.

- CSCsd90308—Large default beacon size causes blue screen on Conexant Wi-Fi station

  The very large default beacon size on the 802.11a band with 12.3(11)JA firmware is causing a Conexant ISL39200C with the Wi-Fi test bed driver to blue screen under Windows XP.

  The 802.11a beacon size of with TKIP, AES, and WMM enabled is approximately 285 bytes, depending on the size of the SSID. This is an enormous jump in size since Cisco's last version of firmware due to the Country IE 7 and the Power Constraint IE now being advertised by default.

  The Conexant radio seems to blue screen at 235 bytes and larger. Conexant has reproduced the problem.

- CSCse49342—DHCP_SERVER_FAILURE observed in 1300 series in WGB mode
- CSCse48137—Nested repeater does not work

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

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

- CSCse36333—Workgroup bridge client fails to get a DHCP IP address when root link is configured for WPA v2 LEAP authentication

  A root access point and workgroup bridge access point configured for WPAv2 LEAP authentication properly associate and authenticate, but the workgroup bridge client does not get an IP address from the DHCP server. The root access point does not show the workgroup bridge client details.

- CSCse40389—Dot1x(LEAP) reauthentication occurs even though it is not enabled

  A 3550 or 2950 switch continuously re-authenticates an access point on a specific interval though re-authentication is disabled on the switch side when the dot1x method is LEAP.

  Continuous re-authentication does occur when the dot1x authentication method is FAST.

- CSCse41589—Workgroup bridge fails to get a DHCP IP address after a successful EAP-FAST authentication to the root access point

  The workgroup bridge is able to ping the root access point and wired host if BVI1 is assigned with a static IP address. Occasionally, the workgroup bridge is assigned a DHCP IP address after a long period of time (about 15 to 20 minutes).

  The failure to obtain a DHCP IP address is not observed when the the workgroup bridge uses LEAP authentication.

- CSCse42464—Access point fails to retrieve certificate from certificate authority server using GUI

  Certificate is obtained correctly when using the CLI.

- CSCse48448—Workgroup bridge non-native VLAN configuration blocks switch native VLAN port

  The workgroup bridge are associated to the root access point but the switch port (VLAN1) is blocked by spanning-tree with the following error message:

```
3750Switch#
3w2d: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 2 on
GigabitEthernet1/0/1 VLAN1.
3w2d: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet1/0/1 on VLAN0001.
Inconsistent local vlan.
3750Switch#
```

- CSCse09744—SSID config page for NAC for MBSSID on the GUI does not have the ability to tie a VLAN name to the VLAN in the SSID configuration page

  On the SSID page, the VLAN fields exists but no fields exist to link the VLAN name. To add a VLAN name associated with the VLAN requires navigating to the Services VLAN page.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.3(11)JA1:

- CSCsb12598

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto.

- CSCsb40304

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto.

- CSCsd92405

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto.

- CSCsd92405—Router no longer crashes when receiving a multiple malformed TLS/SSL3 finished message.
- CSCse85200—Validation of the TLV fields in a CDP packet no longer fail to detect lengths less than the TLV header size.
- CSCsf07847—CDP no longer fails to discover neighbor information.
- CSCsd02001—AES-CCMP Replay errors no longer periodically occur on 1300 series bridges running Cisco IOS Release 12.3(7)JA configured with AES encryption.
- CSCsd54914—802.1x reauthentication interval for a 1300 series access point/bridge in non-root bridge mode now functions correctly.
- CSCek46852—EAP-FAST now works with open source client and local RADIUS server.
- CSCsg91315—WDS do return report to WLSE without a problem.

- CSCse70031—Access points running Cisco IOS Release 12.3(8)JA2 and configured for WPAv2 no longer sends its MAC address as the username in the ACS accounting records.
- CSCsg48579— The **no led display alternate** command has been removed from the access point's running configuration.
- CSCse29487—Repeater-to-repeater roaming now occurs correctly.
- CSCsg05807—7920 phones roam correctly between MBSSID-enabled access points.
- CSCsg26708—Access points running Cisco IOS Release 12.3(8)JA2 no longer stop passing broadcast traffic from the wired to wireless side.
- CSCsg79644—1240 and 1230 access points in workgroup bridge and associated to a 1300 series bridge no longer stop broadcast and multicast traffic.
- CSCsd62772—Radius accounting start/stop records are not sent, for associated client
- CSCse84920—Access point no longer reloads with unknown system cause.
- CSCse95836—Access point no longer forwards invalid ethernet frame, length=0 over wireless link.
- CSCsf08775—EAP-FAST supplicant now authenticates correctly to a Steel Belt RADIUS server
- CSCsg16033—A workgroup bridge associated to a root access point now appear when polling the Dot11 Client Configuration Info Table and Dot11 Client Statistics Table of the CISCO-DOT11-ASSOCIATION-MIB.
- CSCsg20744—Disable MBSSID message now appears when configuring the access point in scanner mode.
- CSCse72925—SNMP **mib community-map** command no longer causes a traceback and access point reload.
- CSCsf95975—Access points no longer crash when AeroScout server address is misconfigured.
- CSCsg44483—LEAPCL-3-TIMEOUT messages no longer appear on reauthentication/rekey.
- CSCsg73790—Wired clients on a workgroup bridge now receive multicast traffic from an LWAPP access point.
- CSCsg99358—1240 series no longer crashes in unconfigured VLAN on automated regression.

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**.

Documentation Updates

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

Changes

This section describes changes to access point and bridge documentation for this release.

DFS Automatically Enabled on Some 5-GHz Radio Channels in North America

Access points with 5-GHz radios configured at the factory for use in North America now comply with regulations that require radio devices to use Dynamic Frequency Selection (DFS) to detect radar signals and avoid interfering with them.

By default, the access point automatically uses DFS to set the operating frequency on 5-GHz radios. The access point randomly selects a frequency from among these frequencies:

- Frequencies 5.150 to 5.250 GHz (also known as the UNII-1 band)
- Frequencies 5.250 to 5.350 GHz (also known as the UNII-2 band)
- Frequencies 5.470 to 5.725 GHz (also known as the UNII-3 band)
- Frequencies 5.725 to 5.825 GHz (also known as the UNII-4 band)

Note By default, Band 3 (5.470 to 5.725 GHz) is disabled to allow backward compatibility with older clients. You must explicitly enable it in the Radio Settings page of the GUI or by using the **dfs band block** radio interface CLI command.

When DFS is enabled, the access point monitors its operating frequency for radar signals. If it detects radar signals on the channel, the access point takes these steps:

- Blocks new transmissions on the channel.
- Flushes the power-save client queues.
- Broadcasts an 802.11h channel-switch announcement.
- Disassociates remaining client devices.
- If participating in WDS, sends a DFS notification to the active WDS device that it is leaving the frequency.
- Randomly selects a different 5-GHz channel.
- Scans the new channel for radar signals for 60 seconds.
- If there are no radar signals on the new channel, enables beacons and accepts client associations.
- If participating in WDS, sends a DFS notification of its new operating frequency to the active WDS device.

Blocking Channels from DFS Selection

You can block groups of channels to prevent the access point from selecting them when DFS is enabled. Use this configuration interface command to block groups of channels from DFS selection:

[**no**] **dfs band** [**1**] [**2**] [**3**] [**4**] **block**

The 1, 2, 3, and 4 options designate blocks of channels:

- **1**—Specifies frequencies 5.150 to 5.250 GHz. This group of frequencies is also known as the UNII-1 band.
- **2**—Specifies frequencies 5.250 to 5.350 GHz. This group of frequencies is also known as the UNII-2 band.
- **3**—Specifies frequencies 5.470 to 5.725 GHz. By default, this group of channels is blocked from DFS selection.
- **4**—Specifies frequencies 5.725 to 5.825 GHz. This group of frequencies is also known as the UNII-3 band.

This is the command that appears in a default configuration:

```
ap(config-if)# dfs band 3 block
```

This example shows how to prevent the access point from selecting frequencies 5.150 to 5.350 GHz during DFS:

```
ap(config-if)# dfs band 1 2 block
```

This example shows how to unblock frequencies 5.150 to 5.350 for DFS:

```
ap(config-if)# no dfs band 1 2 block
```

This example shows how to unblock all frequencies for DFS:

```
ap(config-if)# no dfs band block
```

NAC Support for MBSSID

Networks must be protected from security threats, such as viruses, worms, and spyware. These security threats disrupt business, causing downtime and continual patching. Endpoint visibility and control is needed to help ensure that all wired and wireless devices attempting to access a network meet corporate security policies. Infected or vulnerable endpoints need to be automatically detected, isolated, and cleaned.

NAC is designed specifically to help ensure that all wired and wireless endpoint devices (such as PCs, laptops, servers, and PDAs) accessing network resources are adequately protected from security threats. NAC allows organizations to analyze and control all devices coming into the network. By ensuring that every endpoint device complies with corporate security policy and is running the latest and most relevant security protections, organizations can significantly reduce or eliminate endpoint devices as a common source of infection or network compromise.

WLANs need to be protected from security threats such as viruses, worms, and spyware. Both the NAC Appliance and the NAC Framework provide security threat protection for WLANs by enforcing device security policy compliance when WLAN clients attempt to access the network. These solutions quarantine non-compliant WLAN clients and provide remediation services to help ensure compliance.

Release 12.3(11)JA1 provides NAC support for MBSSID. A client, based on its health (software version, virus version, and so on) is placed on a separate VLAN that is specified to download the required software to upgrade the client to the software versions required to access the network. Four VLANs are specified for NAC support, one of which is the normal VLAN where clients having the correct software version are placed. The other VLANs are reserved for specific quarantine action and all infected clients are placed on one of these VLANs until the client is upgraded.

Each SSID has up to 3 additional VLANs configured as “unhealthy” VLANs. Infected clients are placed on one of these VLANs, based on how the client is infected. When a client sends an association request, it includes its infected status in the request to the RADIUS server. The policy to place the client on a specific VLAN is provisioned on the RADIUS server.

When an infected client associates with an access point and sends its state to the RADIUS server, the RADIUS server puts it into one of the quarantine VLANs based on its health. This VLAN is sent in the RADIUS server Access Accept response during the dot1x client authentication process. If the client is healthy and NAC compliant, the RADIUS server returns a normal VLAN assignment for the SSID and the client is placed in the correct VLAN and BSSID.

Each SSID is assigned a normal VLAN, which is the VLAN on which healthy clients are placed. The SSID can also be configured to have up to 3 backup VLANs that correspond to the quarantine VLANs on which clients are placed based on their state of health. These VLANs for the SSID use the same BSSID as assigned by the MBSSID for the SSID.

The configured VLANs are different and no VLAN overlap within an SSID is allowed. Therefore, a VLAN can be specified once and cannot be part of 2 different SSIDs per interface.

Quarantine VLANs are automatically configured under the interface on which the normal VLAN is configured. A quarantine VLAN inherits the same encryption properties as that of the normal VLAN. VLANs have the same key/authentication type and the keys for the quarantine VLANs are derived automatically.

Dot11 sub-interfaces are generated and configured automatically along with the dot1q encapsulation VLAN (equal to the number of configured VLANs). The sub-interfaces on the wired side is also configured automatically along with the bridge-group configurations under the FastEthernet0 sub-interface.

When a client associates and the RADIUS server determines that it is unhealthy, the server returns one of the quarantine NAC VLANs in its RADIUS authentication response for dot1x authentication. This VLAN should be one of the configured backup VLANs under the client’s SSID. If the VLAN is not one of the configured backup VLANs, the client is disassociated.

Data corresponding to the all the backup VLANs are sent and received using the BSSID that is assigned to the SSID. Therefore, all clients (healthy and unhealthy) listening to the BSSID corresponding the the SSID wake up. Based on the multicast key being used corresponding to the VLAN (healthy or unhealthy), packet decrypting takes place on the client. Wired side traffic is segregated because different VLANs are used, thereby ensuring that traffic from infected and uninfected clients do not mix.

A new keyword, **backup**, is added to the existing **vlan** <*name*> | <*id*> under **dot11 ssid** <*ssid*> as described below:

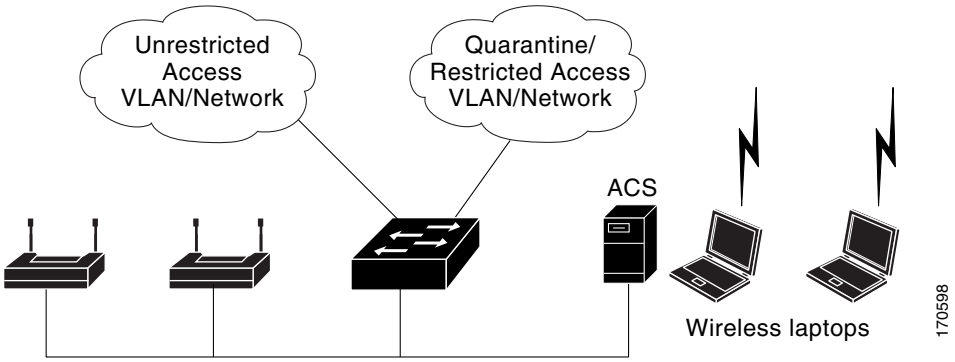
```
vlan <name>|<id> [backup <name>|<id>, <name>|<id>, <name>|<id>
```

Configuring NAC for MBSSID

Note This feature supports only Layer 2 mobility within VLANs. Layer 3 mobility using network ID is not supported in this feature.

Note Before you attempt to enable NAC for MBSSID on your access points, you should first have NAC working properly. Figure 4 shows a typical network setup.

Figure 4 Typical NAC Network Setup



For additional information, see the documentation for deploying NAC for Cisco wireless networks.

Follow these steps to configure NAC for MBSSID on your access point:

Step 1 Configure your network as shown in Figure 4.

Step 2 Configure standalone access points and NAC-enabled client-EAP authentication.

Step 3 Configure the local profiles on the ACS server for posture validation.

Step 4 Configure the client and access point to allow the client to successful authenticate using EAP-FAST.

Step 5 Ensure that the client posture is valid.

Step 6 Verify that the client associates to the access point and that the client is placed on the unrestricted VLAN after successful authentication and posture validation.

A sample configuration is shown below.

```
dot11 mbssid
dot11 vlan-name engg-normal vlan 100
dot11 vlan-name engg-infected vlan 102
dot11 vlan-name mktg-normal vlan 101
dot11 vlan-name mktg-infected1 vlan 103
dot11 vlan-name mktg-infected2 vlan 104
dot11 vlan-name mktg-infected3 vlan 105
!
dot11 ssid engg
    vlan engg-normal backup engg-infected
    authentication open
    authentication network-eap eap_methods
!
dot11 ssid mktg
    vlan mktg-normal backup mktg-infected1, mktg-infected2, mktg-infected3
    authentication open
    authentication network-eap eap_methods
!
interface Dot11Radio0
!
encryption vlan engg-normal key 1 size 40bit 7 482CC74122FD transmit-key
encryption vlan engg-normal mode ciphers wep40
!
encryption vlan mktg-normal key 1 size 40bit 7 9C3A6F2CBFBC transmit-key
encryption vlan mktg-normal mode ciphers wep40
!
ssid engg
```

```
!
ssid mktg
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio0.100
encapsulation dot1Q 100 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
bridge-group 102 subscriber-loop-control
bridge-group 102 block-unknown-source
no bridge-group 102 source-learning
no bridge-group 102 unicast-flooding
bridge-group 102 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.100
encapsulation dot1Q 100 native
no ip route-cache
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface FastEthernet0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
no bridge-group 102 source-learning
bridge-group 102 spanning-disabled
!
```

New IOS CLI Commands

No new IOS CLI commands are introduced in this release.

Omissions

The command **dot11 extension power native** was omitted from the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points 12.3(8)JA* and *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges 12.3(8)JA*.

When enabled, the **dot11 extension power native** shifts the power tables the radio uses from the IEEE 802.11 tables to the native power tables. The radio derives the values for this table from the NativePowerTable and NativePowerSupportedTable of the CISCO-DOT11-1F-MIB. The Native Power tables were designed specifically to configure powers as low as -1dBm for Cisco Aironet radios that support these levels.

Related Documentation

This section lists documents related to Cisco IOS Release 12.3(11)JA and to 1130AG, 1240AG series access points, and 1300 series outdoor access point/bridges.

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.