Release Notes for Cisco Aironet 802 Access Points for Cisco IOS Releases 12.4(25d)JAX and 12.4(25d)JAX1

September 2012

These release notes describe features, enhancements, and caveats for two special technology deployment releases, Cisco IOS Releases 12.4(25d)JAX and 12.4(25d)JAX1. These releases supports Cisco 802 Access Points (AP802). The AP802 is an integrated access point on the Next Generation Cisco 880 Series Integrated Services Routers (ISRs).

Contents

These release notes contain the following sections:

- Introduction, page 1
- System Requirements, page 2
- New Features, page 3
- Important Notes, page 3
- Caveats, page 9
- Troubleshooting, page 10
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 10

Introduction

The 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 access points using the command-line interface (CLI), the web-browser interface, or Simple Network Management Protocol (SNMP).

System Requirements

You can install these releases on all 802 access points in Cisco 880 Series ISRs.

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 a portion of the command output from an access point running Cisco IOS Release 12.4(25d)JAX:

```
ap#show version
Cisco IOS Software, AP802 Software (AP802-K9W7-M), Version 12.4(25d)JAX, RELEASE SOFTWARE
(fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2011 by Cisco
Systems, Inc.
Compiled Mon 25-Jul-11 22:10 by prod_rel_team

ROM: Bootstrap program is AP802 boot loader
BOOTLDR: AP802 Boot Loader (AP802-BOOT-M) Version 12.4(23c)JA2, RELEASE SOFTWARE (fc3)
```

You can also find the software release on the System Software Version page in the access point's web-browser interface.

Upgrading to a New Software Release

Follow these steps for instructions on upgrading your access point 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.

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

New Features

Cisco IOS Release 12.4(25d)JAX has the following new features:

- Support for an autonomous (standalone) Cisco 802 Access Points

You can find detailed information and configuration procedures for 802 access points in 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

Cisco IOS Release 12.4(25d)JAX1 has these new features:

- Support for Autonomous (standalone) dual-radio(2.4 GHz and 5 GHz) Cisco 802 Access Points
- Dynamic Frquency Selection (DFS)

Note DFS functionality is disabled for FCC SKUs pending FCC certification.

Important Notes

This section describes important information about access points and bridges.

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 this 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.

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 an access point 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.

Caveats

This section lists Open Caveats and Resolved Caveats for access points in Cisco IOS Release 12.4(25d)JAX and 12.4(25d)JAX1.

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

These caveats are open in Cisco IOS Release 12.4(25d)JAX1:

Table 1 Open Caveats

Identifier	Headline
CSCtz39097	Enable DFS channels for FCC SKUs after FCC Cerification is done
CSCub24955	Traceback process_lock_semaphore seen during regression

Resolved Caveats

There are no resolved cavetas in these releases.

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