



# Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 12.4(10b)JDA and 12.4(10b)JDA2

---

**November 30, 2008**

These release notes describe caveats and features for this maintenance release of Cisco IOS Release 12.4(10b)JDA and 12.4(10b)JDA2. Cisco IOS Release 12.4(10b)JDA supports 32-Mb Cisco autonomous access points, including Cisco Aironet 1130, 1240, and 1250 series access points. Cisco IOS Release 12.4(10b)JDA2 supports 1300 series access point/bridges and 1400 series bridges.



**Caution**

---

Cisco IOS Releases 12.4(10b)JDA and 12.4(10b)JDA2 are not interchangeable. Use Release 12.4(10b)JDA only for 32-Mb access points. Use Release 12.4(10b)JDA2 only for 1300 and 1400 series bridges.

---

## Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Important Notes, page 12](#)
- [Caveats, page 20](#)
- [Troubleshooting, page 26](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 26](#)



---

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

© 2008 Cisco Systems, Inc. All rights reserved.

# Introduction

The Cisco Aironet Access Point is a wireless LAN transceiver that acts as the connection point between wireless and wired networks or as the center point of a standalone wireless network. In large installations, the roaming functionality provided by multiple access points enables wireless users to move freely throughout the facility while maintaining uninterrupted access to the network.

You can configure and monitor 1130, 1240, 1250 series access points, 1300 series outdoor access point/bridges, and 1400 series bridges by using the command-line interface (CLI), the web-browser interface, or Simple Network Management Protocol (SNMP).

## System Requirements

You can install Cisco IOS Release 12.4(10B)JDA on all 1130, 1240, 1250 series access points. You can install Cisco IOS Release 12.4(10b)JDA2 on 1300 series outdoor access point/bridges, and 1400 series bridges. The releases are not interchangeable.

## Finding the Cisco IOS Software Release

To find the version of Cisco IOS software running on your access point, use a Telnet session to log into the access point, and enter the **show version EXEC** command. This example shows command output from an access point running Cisco IOS Release 12.4(10b)JDA:

```
ap1240AG> show version
Cisco Internetwork Operating System Software
IOS (tm) C1240 Software (C1240-K9W7-M), Version 12.4(10B)JDA
Copyright (c) 1986-2008 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

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 **Product & Services**. A drop-down menu appears.
  - Step 3** Click **Wireless**. The Wireless Introduction page appears.
  - Step 4** Scroll down to the Product Portfolio section.
  - Step 5** In the Access Point section, select the access point model for which you need the information. The Introduction page for the model you selected appears.
  - Step 6** Under the Support section, click **Configure**. A list of configuration documents appears.
  - Step 7** Click **Configuration Guides**. The Configuration Guides page appears.

- Step 8** Click **Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(10b)JA and 12.3(8)JEC**.

For information on Cisco IOS software, click this link to browse to the Cisco IOS Software Center on Cisco.com:

<http://www.cisco.com/public/sw-center/sw-ios.shtml>

## 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	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio {0   1}</code>	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	<code>shutdown</code>	Disable the radio port.
Step 4	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>copy running-config startup-config</code>	(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

The following new feature is included in Cisco IOS Release 12.4(10B)JDA:

- System log message enhancement

### System Log Message Enhancement

With this release, system logging functions are enhanced with the addition of the following new system messages:

**Error Message** %DOT11-4-LOADING\_RADIO: Interface [chars], loading the radio firmware ([chars])

**Explanation** The radio has been stopped to load new firmware.

**Recommended Action** Recommended Action: No action is required.

**Error Message** %LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]

**Explanation** The data link level line protocol has changed state.

**Recommended Action** No action is required.

**Error Message** %SYS-5-RESTART: System restarted --[chars]

**Explanation** A reload or restart was requested.

**Recommended Action** Notification message only. No action is required.

**Error Message** %SYS-5-CONFIG\_I: Configured from [chars] by [chars]

**Explanation** The router configuration has been changed.

**Recommended Action** This is a notification message only. No action is required.

**Error Message** %LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]

**Explanation** The data link level line protocol has changed state on the interface shown.

**Recommended Action** No action is required.

**Error Message** %SNMP-5-COLDSTART: SNMP agent on host [chars] is undergoing a cold start

**Explanation** The SNMP server completed a coldstart.

**Recommended Action** Notification message only. No action is required.

**Error Message** %SYS-6-CLOCKUPDATE: System clock has been updated from [chars] to [chars], configured from [chars] by [chars].

**Explanation** The system clock has been modified.

**Recommended Action** This is an informational message only. No action is required.

**Error Message** %SYS-6-LOGGERSTART: Logger process started

**Explanation** The logger process has been initialized and started.

**Recommended Action** Recommended Action: No action is required.

**Error Message** DHCP-6-ADDRESS\_ASSIGN

**Explanation** The interface has been allocated an address by means of DHCP.

**Recommended Action** None

**Error Message** NO\_SSID\_OR\_NO\_VLAN

**Explanation** No SSID or VLAN is configured. (Example:%DOT11-1-NO\_SSID\_OR\_NO\_VLAN: No SSID configured. Dot11Radio0 not started.)

**Recommended Action** Use the CLI to assign an SSID, and VLAN if required, to the affected interface.

Use the IOS command **logging facility** is available that allows users to customize the severity level of system error messages by determining the severity levels of system error messages that are reported or discarded. The command is supported on 1100, 1130, 1200, 1240, 1250, and 1300 series access points and 1400 series bridges. The events covered by this command are:

- Interfaces up/down (includes all interfaces)
- Interface link change
- Radius down/up
- Access point going down (rebooting)
- Uplink down
- Uplink failed
- Radio failed
- Rogue access point found.

The command syntax is as follows:

**logging facility <facility name> event <event name> severity <severity level>**

The **facility name** option has 4 options:

- 1. system
- 2. dot11
- 3. radius
- 4. link

The command is available only if one of the facility names is selected.

The **event name** selections depends on the facility name selected. Supported events and subevents for the respective facilities are shown in the following table:

Facility Name	Event	Subevent
system	clock config logger (12.3(8)JEC2 only) reload restart	–
dot11	uplink radio rogue ap ssid	failed, down load no-ssid-or-no-vlan
rogue ap	–	–
radius	down up	–
link	interface	up-down, link-changed
DHCP	address-assign	
SNMP	cold-start	–
LINE	up-down	–

The severity level specifies the maximum severity level to report and print a system logging message. There are 8 severity levels available, which are shown in the following table:

Severity Level	Logging Severity Level Description
0. emergencies	System is unusable
1 alerts	Immediate action needed
2. critical	Critical conditions
3. errors	Error conditions
4. warnings	Warning conditions
5. notifications	Normal but significant conditions
6. informational	Informational messages
7. debugging	Debugging messages

The following example configures severity level 3 (error conditions) for the facility *system*, event *reload* error messages:

```
ap(config)# logging facility system event reload severity errors
```

The following example configures severity level 1 (*immediate action needed*) for the facility *dot11*, event *radio failed* error messages:

```
ap(config)# logging facility dot11 radio failed severity alerts
```

Using the **no** form of the command removes the configured severity level from the configuration and reverts to the default severity for the event.

## Installation Notes

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

## Access Points

This section contains installation notes for access points.

### Installation in Environmental Air Space

Cisco Aironet 1130, 1240, and 1250 Series Access Points provide adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the *National Electrical Code (NEC)* and Sections 2-128, 12-010(3) and 12-100 of the *Canadian Electrical Code, Part 1, C22.1*.



#### Caution

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

## Power Considerations

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



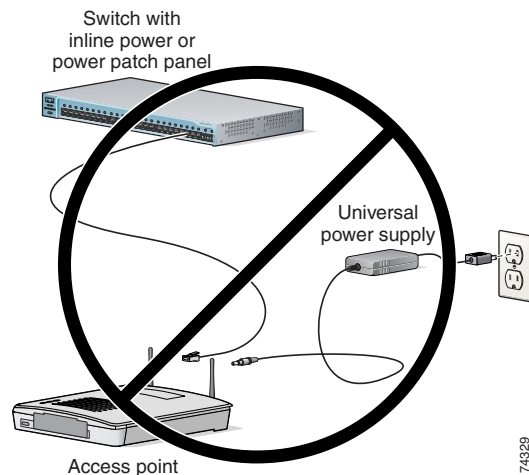
**Caution**

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

### Use Only One Power Option

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

**Figure 2** *Improper Power Configuration Using Two Power Sources*



### Configuring Power for 1250 Series Access Points

The 1250 series access point disables the radio interfaces when the connected power source does not provide enough power. Depending on your power source, you might need to enter the power source type in the access point configuration. Use the System Software: System Configuration page on the web-browser interface to select a power option. [Figure 3](#) shows the System Power Settings section of the System Configuration page.

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

System Power Settings	
Power State:	FULL POWER
Power Source:	AC_ADAPTOR
Power Settings:	<input type="radio"/> Power Negotiation <input checked="" type="radio"/> Pre-standard Compatibility
Power Injector:	<input type="checkbox"/> Installed on Port with MAC Address: <input type="text" value="DISABLED"/> (HHHH.HHHH.HHHH)
<input type="button" value="Apply"/>	

The PoE power status can also be found in the PoE Status section on the network interfaces>network status page on the access point GUI. The status statements can include any of the following:

- Normal (full power)
- Low (radio disabled)
- Lower than 15.4 W
- Lower than 16.8 W

### Using the AC Power Adapter

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

### Using a Switch Capable of IEEE 802.3af Power Negotiation

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

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

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

### Using a Power Injector

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

## 1250 Series Power Modes

The 1250 series access point can be powered by either inline power or by an optional AC/DC power adapter. Certain radio configurations may require more power than can be provided by the inline power source. When insufficient inline power is available, you can select several options (based upon your access point radio configuration) as shown in the following table:

Radio Band	Data Rate	Number of Transmitters	Cyclic Shift Diversity (CSD)	Maximum Transmit Power (dBm) <sup>1</sup>		
				802.3af Mode (15.4W)	Enhanced PoE Power Optimized Mode (16.8 W)	Enhanced PoE Mode (20 W)
2.4-GHz	802.11b	1	N/A	20	20	20
	802.11g	1	N/A	17	17	17
	802.11n (MCS 0-7)	1	Disabled	17	17	17
		2	Enabled (default)	Disabled	14 (11 per Tx) <sup>2</sup>	20 (17 per Tx)
802.11n (MCS 8-15)	2	N/A	Disabled	14 (11 per Tx)	20 (17 per Tx)	
5-GHz	802.11a	1	N/A	17	17	17
	802.11n (MCS 0-7)	1	Disabled	17	17	17
		2	Enabled (default)	Disabled	20 (17 per Tx)	20 (17 per Tx)
802.11n (MCS 8-15)	2	N/A	Disabled	20 (17 per Tx)	20 (17 per Tx)	

1. Maximum transmit power will vary by channel and according to individual country regulations. Refer to the product documentation for specific details.
2. Tx—Transmitter

## Antenna Installation

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



### Warning

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

## 1400 Series Bridges

This section contains installation information for the 1400 series bridges.

### Default SSID and Distance Settings Change When You Change Role in Radio Network

If the bridge's SSID has not been changed from the default setting and you select **Install Automatic Mode** as the bridge's role in radio network setting, the SSID automatically changes from *tsunami* to *autoinstall*. When you change the role in radio network from Install Automatic Mode to Root or Non-Root, the SSID changes automatically from *autoinstall* back to *tsunami*. However, if you change the SSID from its default setting, changing the role in radio network setting does not change the SSID.

In Install Automatic Mode, the default distance setting is 61.5 mi. (99 km). When you change the role in radio network from Install Automatic Mode to Root or Non-Root, the distance setting changes automatically from 61.5 mi. (99 km) to 0 mi. (0 km).

## Default Encryption Key 2 Is Set by Bridge

The encryption key in slot 2 is the transmit key by default. If you enable WEP with MIC, use the same WEP key as the transmit key in the same key slot on both root and non root bridges.

## Limitation to PAgP Redundancy on Switches Connected by Bridge Links

When two switches configured for Port Aggregation Protocol (PAgP) are connected by redundant wireless bridge links, the PAgP change-over takes at least 30 seconds, which is too slow to maintain TCP sessions from one port to another.

## CLI Command `power client n` Is Not Supported

The bridge does not support the `power client n` configuration interface command in the web-browser or CLI interfaces. The bridge does not perform any action when you enter this command.

## Default Infrastructure SSID

When a VLAN is enabled, the WEP encryption mode and the WEP key are applicable only to a native VLAN. Any SSID configured should have the Infrastructure-SSID parameter enabled for that SSID. With the Infrastructure-SSID parameter enabled, the bridge ensures that a non-native VLAN cannot be assigned to that SSID.

## ARP Table Is Corrupted When Multiple BVIs Are Configured

The bridge supports only one bridge virtual interface (BVI). Multiple BVIs should not be configured because the ARP table can be corrupted.

## Bridge Power Up LED Colors

During power up, the bridge LEDs display the following color sequences:

1. The Install LED is initially turned off.
2. The Install LED turns amber.
3. The Status LED turns amber during the boot loader process.
4. The Ethernet, Status, and Radio LEDs turn green during the loading of the operating system.
5. The Ethernet, Status, and Radio LEDs turn amber during the loop-back test.
6. The Status LED starts to blink green, and then the Ethernet LED starts to blink green.
7. The Ethernet, Status, and Radio LEDs blink amber twice to show that the auto-install process has started.
8. During the auto-install process, the Ethernet, Status, and Radio LEDs turn off for a short time period, and then go through a blinking sequence twice. Each LED sequentially blinks at the following rates before becoming continuously amber:
  - a. Slow blinking rate of 1 blink per second.
  - b. Medium blinking rate of 2 blinks per second.
  - c. Fast blinking rate of 4 blinks per second.

9. The Install LED starts to blink amber to show that the bridge is searching for a root bridge.
10. When the bridge associates to a root bridge, the Install LED turns amber.
11. When the bridge becomes a root bridge and is waiting for a nonroot bridge to associate, the Install LED blinks green.
12. When the root bridge has a nonroot bridge associated, the Install LED turns green.

## Bridge Cannot Detect Simultaneous Image Downloads

Do not attempt to load software images into the bridge from both a Telnet session and a console session simultaneously. The bridge cannot detect that two images are being loaded at the same time. For best results, use the **archive download** command in the CLI.

## Bridge Cannot Detect Invalid Software When Using copy Command

The bridge sometimes cannot detect invalid software images when you load software using the copy command. For best results, use the **archive download** command in the CLI to load new software.

## Telnet Session Sometimes Hangs or Will Not Start During Heavy Traffic

When the bridge is transmitting and receiving heavy traffic, you sometimes cannot start a Telnet session and some existing Telnet sessions halt. However, this behavior is expected because the bridge gives top priority to data traffic and a lower priority to Telnet traffic.

# Important Notes

This section describes important information about access points and bridges.

## CCKM and Fast Roaming on Cisco 7921/7925 IP Phones

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

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

## Access Point Creates File When Radar is Detected on a DFS Channel

When an access point detects a radar on a DFS channel, the access point creates a file in its flash memory. The file is based on the 802.11a radio serial number and contains the channel numbers on which the radar is detected. This is an expected behavior and you should not remove this file. See the caveat CSCsv36602 in the [“Open Caveats” section on page 20](#).

## Only 8 SSIDs Supported on Bridge Devices

In order to rectify concatenation issues in previous releases, this release supports only 8 SSIDs on all Cisco Aironet bridge devices.

## Access Points Send Multicast and Management Frames at Highest Basic Rate

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

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

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

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

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

## Interpreting the Show Controller Dot11Radio Active Power Level Output

A portion of the output of the `show controller dot11radio` CLI command displays the active power levels by rate as shown in the example below:

```
1.0 to 11.0, 20 dBm, changed due to regulatory maximum
6.0 to m15., 17 dBm, changed due to regulatory maximum
m0.-4 to m15.-4, 14 dBm, changed due to regulatory maximum
```

The -4 in the third line indicates 40-MHz.

## Enabling a Crash File for 1250 Series Access Points

A 1250 series access point that is running a Cisco IOS Release prior to 12.4(10b)JDA and greater do not generate a crash log when it crashes. The crash log is disabled so that a crash does not corrupt the flash file system.

New 1250 series access points shipped from the factory contain the new bootloader image. Previous versions do not support that fixes the flash file system after it is corrupted during a crash (without losing files). This new bootloader automatically sets a new CRASH\_LOG environment variable to “yes,” which enables a crash log to be generated following a crash. Therefore, no user configuration is needed to enable a crash log on new 1250 series access points shipped from the factory.

To enable 1250 series access points in the field to generate a crash log following a crash, install Cisco IOS Release (insert Krypton release number here) or later and enter this case-sensitive bootloader CLI command on the access point: **set CRASH\_LOG yes**. When you set this CLI, the access point does not immediately generate a crash log. The log is generated after a crash occurs. After the crash log is generated, enter this command to disable the CRASH\_LOG environment variable to minimize the risk of corrupting the flash file system: **set CRASH\_LOG no**.

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

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

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

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

## Layer 3 Not Supported with NAC for MBSSID

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

## Change to Default IP Address Behavior

Cisco IOS Releases 12.3(2)JA and later change the default behavior of access points requesting an IP address from a DHCP server:

When you connect a 1130 or 1240 series access point or a 1300 series outdoor access point/bridge with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an address, continues to send requests indefinitely.

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

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

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

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

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

## Default Username and Password Are *Cisco*

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

## Some Client Devices Cannot Associate When QoS Is Configured

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

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

## Some Devices Disassociate When Multiple BSSIDs Are Added or Deleted

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

## Enabling MBSSIDs Without VLANs Disables Radio Interface

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

This example shows the commands that you use to re-enable the radio:

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

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

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

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

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

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

## TKIP and Cisco 7920 IP Phones

When a 7920 phone is associated to a 1250 series access point using Temporal Key Integrity Protocol (TKIP) encryption, the access point might report “TKIP TSC replay detected” and discard the packets transmitted by the phone (CSCsj35039). To work around this issue, perform one of the following:

- Use static or dynamic WEP with 802.1X key management for the 7920 SSID.
- Disable long preambles.

## 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](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 and resolved caveats for access points and bridges in Cisco IOS Releases 12.4(10B)JDA, and 12.4(10b)JDA2

## Open Caveats

These caveats are open in Cisco IOS Release 12.4(10B)JDA and 12.4(10b)JDA2.

- CSCsv36602—Files appearing on access point flash with 5-GHz serial number as filename

These files are created when radar is detected on a DFS channel. The files are created with the filename consisting of the serial number of the radio that detected the radar and include the DFS channel on which the radar was detected. The file is used is used when the access point is reset to ensure that the radar detected channels are not immediately selected after the reset.

Conditions: When radar is detected on a DFS channel.

Workaround: None. This is an expected behavior. The file should not be removed.
- CSCsl22707—A 1250 series access point using Power over Ethernet (PoE) continually resets when connected to a Catalyst 3550 series switch.

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

**power inline delay shutdown** (*seconds*) **initial** (*seconds*)

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

Without this command, the switch removes power immediately when a linkdown occurs on the connected device.
- CSCsv82129—**dot11\_mgmt: bad cookie** error msg appears in workgroup bridge mode running open authentication.
- CSCsv71726—1300 series root bridge with CCKM+CMIC show authentication fails.
- CSCsw17396—Root and nonroot 1300 series bridges associate with mismatched WEP key.
- CSCsw17391—1300 series group key update operation aborts.
- CSCsw15978—1400 series bridge displays incorrect encryption warning messages.

Even though AES-CCM encryption is not supported on 1400 series, the following warning message appears when user selects unsupported encryption for WPA key management: “WPA key mgmt cipher requires one or more WPA ciphers (TKIP or AES-CCMP)”.

Workaround: None
- CSCsv75779—1300 series bridge GUI association ping link test page displays a loading error.
- CSCsv97205—Infrastructure client information is invisible on 1300 series bridge GUI.
- CSCsw17385—1300 series GUI Station Information page displays incorrect class value.

When a root bridge and non-root bridge is configured, the station information status table on the non-root association activity page shows “Bridge” but the root bridge class shows as “Unknown” when it should be “Bridge”.

- CSCsv97588—1310 GUI network interfaces page on Radio0 802.11g status page displays “Transmitter power cck/ofdm” error message in the Configured Radio Channel line.
- CSCsw14082—Root parent timeout warning message does not appear on 1300 series bridge GUI.
- CSCsw15976—Carrier busy test option is missing on 1400 series bridge GUI.
- CSCsw16204—ARP caching option is missing in services summary on 1400 series bridge GUI.
- CSCsw16488—Locate access point radio buttons are not enabled on 1400 series GUI.
- CSCsu99415—Crash and traceback observed in non-root 1300 series bridge with shared authentication.
- CSCsu52611—Linktest uses incorrect data rate for transmission.

When a linktest is initiated on a 1250 series access point running Cisco IOS release 12.4(10b) JA4, the linktest is not performed on MCS rates by default.

The linktest is performed by the the command **dot11 dot11Radio 0 /linktest** in privileged exec mode. When executed, the linktest results indicate that the test has occurred on some legacy rate as opposed to MCS rates.

Workaround: Explicitly choose the MCS rate for which you desire the test to be performed.

- CSCso60782—1240 access point fails on process **aprm scan**.

There are no core files as the access point does not generate a traceback and coredump when it fails. The access point silently fails.

- CSCsq92434—**show processes cpu** command displays invalid information.

When displaying **show processes cpu** command, the five second slot shows two numbers but the the one min and five min only shows one number. In addition, the cpu utilization% may not be accurate.

- CSCsq99702—Radio preamble setting is missing from 1250 series access point GUI.

There is no radio preamble setting on the GUI of the 1250 series access point. Previous access points included a way to set the radio preamble using the GUI. However, the setting can be changed on the CLI using the **no preamble-short** command under the d0 radio interface.

Workaround: Set the radio preamble using the CLI.

- CSCsr30708—1250 access point may crash after removing guest-mode using the CLI.

The access point may crash after configuring guest mode with open authentication, assigning an SSID, and enabling the radio interface. If guest mode is removed using the CLI, the access point may crash. If this occurs, a traceback similar to the one below prints:

```
22:53:32 UTC Tue Mar 5 2002: Unexpected exception to CPUvector 300, PC = 0x5383D4, LR
= 0x538030
-Traceback= 0x5383D4 0x53C210 0x1CE8D0 0x1D0654
CPU Register Context:
MSR = 0x00009030 CR = 0x24002024 CTR = 0x0031005C XER = 0x20000000
R0 = 0x00000004 R1 = 0x015BDC08 R2 = 0x00000000 R3 = 0x015D0AA8
R4 = 0x015A8160 R5 = 0x00009030 R6 = 0x01320000 R7 = 0x01320000
R8 = 0x00000001 R9 = 0x00000000 R10 = 0x00000000 R11 = 0x00000000
R12 = 0x1982F398 R13 = 0x4FCA0C63 R14 = 0x01180000 R15 = 0x01180000
R16 = 0x012C0000 R17 = 0x015BDCF8 R18 = 0x015BDCF0 R19 = 0x01370000
R20 = 0x015BDC68 R21 = 0x01763F44 R22 = 0x00000002 R23 = 0x00000004
R24 = 0x017640EC R25 = 0x017540EC R26 = 0x00000000 R27 = 0x015D0AA8
R28 = 0x017440EC R29 = 0x015A81C4 R30 = 0x015A7FE0 R31 = 0x015A8160
```

- CSCsr41089—Side menu bar missing on 1240 access point GUI when accessing the wireless service option.
- CSCsr43516—Cannot configure dot1x using GUI on a 1240 series access point.

Problem occurs with one access point configured as a WDS with one infrastructure access point with WDS associated, and dot1x authentication configured on the infrastructure access point. Using the GUI, if key management is selected an error message prints after clicking **Apply**. In addition, the key management checkbox is in a disabled state after deselecting it.

- CSCsr79628—Number of supported BSSIDs not shown in access point GUI.  
The **show controllers** command report the number of BSSIDs supported, but is not shown on the GUI.
- CSCsr79832—No option available to configure guard-interval using the GUI.  
Workaround: Use the **guard-interval** CLI command.
- CSCsr81316—MALLOCFAIL and tracebacks occur in SSH process.  
During normal operations, the access point's memory becomes fragmented. The access point eventually reloads, triggering a MALLOCFAIL and tracebacks in the system logs
- CSCsr97839—1130 series access point incorrectly buffers frames destined for 7921 phone.  
After some time on a call the 1130 appears to incorrectly buffer frames destined for a 7921 causing 1-way audio for the conversation. The 7921 continues to send audio and the other party can still hear but the RTP back to the 7921 is seen hitting the access point port but not over the air. The 1130 appears to be sending QoS null packets to the 7921 thinking that the 7921 is in power save mode and therefore buffers the frames. If the user presses a button on the 7921 when 1-way audio is occurring, the audio works again in both directions for a few seconds then fails again reverting to 1-way audio. 7920s talking to the same access point do not experience the 1-way audio but they do not use U-APSD.  
Workaround: None other than rebooting the 7921 to start a fresh authentication with the access point.
- CSCsu11294—Ethernet driver issue.  
WMIC uses f0 interface to connect to C3250 f0/0 interface (or other router Ethernet interface). When the WMIC f0 interface is shutting down, the C3250 f0/0 interface line protocol status still shows as up. This scenario is also seen on 1310, Releases 12.4(3G)JA, JA1, 12.4(10b)JA images. The issue is not observed on Release 12.3(8) images.
- CSCsu43113—A 1250 series access point in WGB mode associated to a 1140 series root access point with WPA2/PSK configured deauthenticates and will not reassociate.  
The WGB associates and clients can pass traffic for about 20 minutes, after which the root access point deauthenticates the WGB. Eventually the WGB reassociates, but could take 20 minutes or more. Usually if the WGB radio interface is reset, the WGB can associate and begin passing traffic again.  
Workaround: Try toggling the WGB radio interface.
- CSCsu51305—Get TSPEC refusal when attempting to make an SRTP call with an autonomous access point.  
TSPEC refusal occurs when user tries to make an SRTP call from a 7921 phone with an autonomous access point. Problem occurs when using SRTP with CAC enabled or trying to barge into a 7921 phone.  
Workaround: Disable CAC.
- CSCsu79203—Few objects of ENTITY-MIB give wrong values during SNMP query.
- CSCsu79245—ceAssetMfgAssyNumber object shows incorrect assembly number.  
When **show version** command is issued, the output prints the value of *Top Assembly Serial Number* instead of expected value *Top Assembly Part Number*.

- CSCsu79234—Few objects of CISCO-ENTITY-EXT-MIB showing wrong values.
- CSCsk80813—Vista's anonymous provisioning does not work with access point local AAA server
- CSCsk05871—Sometimes packets are not marked as voice to 7921 phones.

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

Workaround: None.

- CSCsr58019—Bridge link fluctuating with concatenation (Duplicate of CSCsr19482).

While performing FTP data transfer the bridge link fluctuates with concatenation configured. Without concatenation the FTP data transfer operates normally.

- CSCsq90480—Access point accepts TSPEC in reassociation for non-CCXv4 client.

Workaround: None.

- CSCso10119—1231 access point reboots.

The 1231 crashes at random and gives the following tracebacks and reboots:

```
68E024 68E970 68EDF4 4E48F0 495AD0 497EE8 4979C8 4922B0 4FDAB4 4FF85C 50262C 158AA0
```

Workaround: None.

- CSCsq03411—Periodic reauthentication fails with CCKM enabled.

Workaround: None

- CSCsq64212—Clock save interval doesn't save date with access point.

When an access point is configured with the **clock save interval** command and is rebooted, the clock reverts back to the default 2002 date. The issue occurs when the access point is configured to authenticate to another access point configured as a bridge or workgroup bridge and the authentication type is EAP-TLS. After the access point reboots, the certificates are considered invalid because of the dates.

Workaround: Manually set the clock on the access point after each reboot.

- CSCsr53764—Some wired workgroup bridge clients get stuck randomly while roaming.

The workgroup bridges are installed on a train with its clients running customer-specific applications. The workgroup bridge roams very fast between access points due to the speed of the train. When the the train moves through a tunnel, some workgroup bridges often remain associated to a specific access point. For example, when the train travels toward access point 020, the workgroup bridge associates with it and wired clients associate with this workgroup bridge. After the workgroup bridge roams to the next access point (for example 021, 022, or 023), some wired clients still show up under access point 020 even though the workgroup bridge has moved to a new access point. As a result, the wired clients associated with the workgroup bridge lose their connection with the outside network.

Workaround: None.

- CSCsg90480—Access point accepts TSPEC in Re-assoc for non-CCXv4 client.

Workaround: None.

- CSCsv48416—Suppress debug logs on 1100 series access point.  
Debug messages appear even though debug is not enabled.

## Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.4(10b)JDA and 12.4(10b)JDA2:

- CSCsg00102—SSLVPN service stops accepting any new SSLVPN connections.  
Symptoms— SSLVPN service stops accepting any new SSLVPN connections.  
Conditions—A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.
- CSCsv29382—Bridge throughput is degrading with concatenation.
- CSCso97733— Concatenation causes radio failure on 1300 series bridge link.
- CSCsr19482—TKIP\_MIC\_Failure observed on the root-bridge when WPA-PSK is configured on the root bridge and nonroot bridge.
- CSCso02086— Unable to apply QoS settings on the standalone access point using the GUI.
- CSCsl28924—Authentication server caching fails.
- CSCsq45790—Wrong dynamic VLAN assigned.
- CSCso12541—Root access point frequently authenticates and deauthenticates with repeater access point.
- CSCsm34905—Wrong dynamic VLAN assigned after re-authentication.
- CSCsk93026—1230 series access point sometimes loses certificate while upgrading.
- CSCsi97733—Concatenation causes radio to fail on 1310 series bridge link.
- CSCsl00363—Changing 802.1x credentials on WGB for EAP-FAST requires a reboot
- CSCso70124—failing to populate SNMP instance for non-vlan(cd11IfVlanSecurityTable)
- CSCsl22194—**show dot11 association** shows negative values
- CSCsm34905—Wrong dynamic VLAN assigned after re-authentication
- CSCso65304—1250 series access point signal to noise in dBm
- CSCsm78141—Access point never sends authenticate-fail trap
- CSCso62119—WLAN encryption mode always returns WEP mode even encryption AES
- CSCso02086—Unable to apply QoS settings on the standalone access point through GUI
- CSCsq29310—Javascript error in file ap\_contextmgr\_ap.shtml
- CSCso81756—A print warning message if apply unsupported encryption on 802.11n radio.
- CSCsq19104—A 1250 GUI displays warning pop up screens at each page when using inline power.
- CSCsm73025—WGB dependent CLI not cleared after unconfiguring WGB
- CSCso57659—More events in syslog logging levels severity feature support
- CSCsk42319— No error message is generated when key management WPAv1 with AES-CCM
- CSCso44446—Closed dot11 priority-map avvid causes dropping RTP on IOS access point

- CSCek69256—A dot11\_mgr\_disp.c: coding error
- CSCso07662—WPA/TKIP downstream throughput degraded when compared to previous versions
- CSCsk78264—A change in the RF domain name takes effect only after a reboot.
- CSCsm38303—Coverage display on WLSE cannot be displayed correctly.
- CSCsq66991—Client cannot reconnect to a 1250 series access point with authentication request.
- CSCsr82508—Upgrade tool sees LWAPP image for 1250 series access point as an invalid image.
- CSCsr44855—Memory leak in SSH process.
- CSCsr11909—Access point ARPing for non local WLSM tunnel loopback destination address.
- CSCsr94048—**privilege interface level xx speed** command crashes access point.
- CSCsr27699—Roaming operation does not work correctly.
- CSCsj56438—Crafted EAP response identity packet may cause device to reload.

This Cisco Bug ID identifies a vulnerability in Cisco's implementation of Extensible Authentication Protocol (EAP) that exists when processing a crafted EAP Response Identity packet. This vulnerability affects several Cisco products that have support for wired or wireless EAP implementations.

This vulnerability is documented in the following Cisco bug IDs:

Wireless EAP - CSCsj56438

Wired EAP - CSCsb45696 and CSCsc55249

This Cisco Security Response is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20071019-eap.shtml>.

- CSCsg74791—Time-based ACLs do not work properly on Cisco Aironet autonomous access points.
- CSCso65219—Autonomous 1250 series access point GUI displays incorrect Tx power.
- CSCsu41132—IP http timeout-policy does not log a user out.
- CSCsm80730—1240 series access point does not send a reassociation response to client.
- CSCir02221—CCKM issue with 1240 series access points.

These caveats are resolved in Cisco IOS Release 12.3(8)JEC3:

- CSCsh97579—Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsq31776—Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.
- CSCsv04836—Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being

accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml>.

## 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://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

(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/tac>. If you are a registered user, click **Registered users click here** to access the entire technical support site. If you are not a registered user, the public public portion of the technical support site displays. Choose a task or information and proceed.

## 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>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)