# Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 12.4(10b)JA3

**March 21, 2008**

These release notes describe caveats and features for maintenance release Cisco IOS Release 12.4(10b)JA3. This release supports 32-Mb Cisco autonomous access points, including Cisco Aironet 1130, 1240, and 1250 series access points, 1300 series access point/bridges, and 1400 series bridges.

## Contents

These release notes contain the following sections:



## Introduction

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

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).


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

# System Requirements

You can install Cisco IOS Release 12.4(10b)JA3 on all 1130, 1240, 1250 series access points, 1300 series outdoor access point/bridges, and 1400 series bridges.

## 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(3g)JA:

```
ap1240AG> show version
Cisco Internetwork Operating System Software
IOS (tm) C1240 Software (C1240-K9W7-M), Version 12.4(3g)JA
Copyright (c) 1986-2007 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/cisco/software/navigator.html

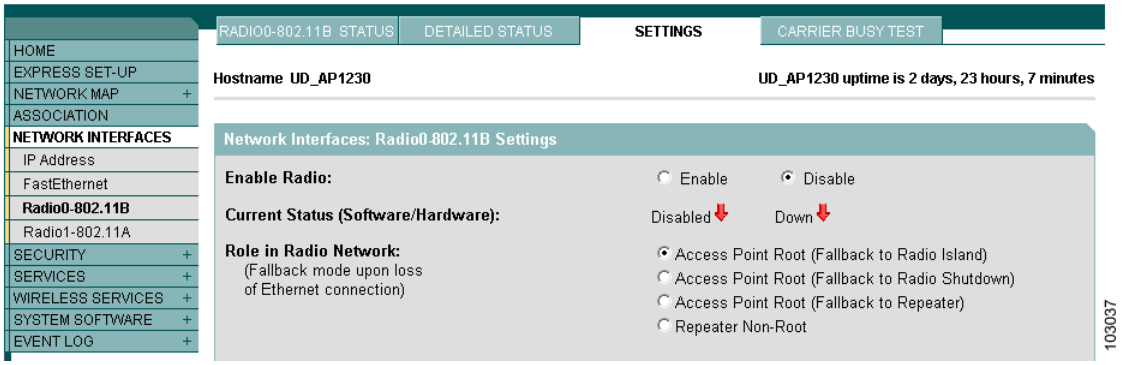
## Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

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

The following new features are included in Cisco IOS Release 12.4(10b)JA3:

- Software support for 801 series access points
- System log messages
- Enhanced PSPF functionality for the 1300 series outdoor access point/bridge
- Ability for 1300 series outdoor access point/bridge to detect Ethernet failure
- Enhanced PoE for 1250 series access point

## Software Support for 801 Series Access Points

Software release 12.4(10b)JA3 supports the AP801, an access point that is embedded in the Cisco 860, 880, 890, and 1900 Series Integrated Services Routers (ISRs). This integrated access point uses its own software image separate from the router and operates as an autonomous access point.Currently, the AP801 is preloaded with autonomous Cisco IOS Release 12.4(10b)JA3 and an LWAPP recovery image. The AP801 has a single 2.4-GHz 802.11n radio. For more information on the AP801, refer to the documentation for the 800 series routers at this URL:

http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html

## System Log Messages

With this release, 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 | reload | – |
| dot11 | uplink | failed, down |
| | radio | failed |
| | rogue ap | – |
| rogue ap | – | – |
| radius | down<br>up | – |
| link | interface | up-down, link-changed |

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.

## Enhanced PSPF Functionality for the 1300 Series Outdoor Access Point/Bridge

Public Secure Packet Forwarding (PSPF) prevents client devices associated to a bridge or access point from inadvertently sharing files with other client devices on the wireless network. PSPF provides Internet access to client devices without providing other capabilities of a LAN. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network. This feature is useful for public wireless networks like those installed in airports or on college campuses.

This release provides support for 1300 series outdoor access points/bridges.

PSPF is disabled by default. To enable PSPF using CLI commands on the wireless device, use bridge groups. Beginning in privileged EXEC mode, follow these steps to enable PSPF:

| Command | Description |
|---|---|
| **config terminal** | Enter configuration mode. |
| **interface dot11 radio {0 \|1}** | Select radio interface |
| **bridge-group port-protected** | Enables protected port for public secure mode. |

Use the **no** form of the command to disable PSPF.

## Ability for the 1300 Series Outdoor Access Point/Bridge to Detect Ethernet Failure

Prior to this release, a 1300 series outdoor access point/bridge was unable to detect whether the Ethernet port on the 1300 power injector was down. Because of this, infrastructure clients associated to a non-root bridge continue to be shown as associated, even when the Ethernet port goes down. This situation results in the clients non roaming to another non-root device, which essentially causes all connections to the client to cease.

To eliminate this situation, a new IOS command **link status timer** is implemented in release 12.4(10b)JA3. Using this command, users can ping the gateway to check for connectivity between it and the 1300 device. The command syntax is as follows:

**link status timer [seconds]**

The **seconds** option specifies the number of seconds that the 1300 device checks the link status. The following values are available:

- 30 seconds
- 60 seconds
- 90 seconds

The command causes the 1300 to ping the gateway for the specified length of time. If the gateway is down, the 1300 radio is disabled, thus permitting any associated clients to disassociate and reassociate with another non-root bridge in the network.

The feature uses the ICMP module to ping the gateway and to check connectivity with the backbone server.

The command is disabled by default.

The following example sets the link status timer to 30 seconds:

```
ap(config)#int fa0
ap(config-if)#link status timer 30
```

A debug command, **debug fast ethernet status** is also added in this release. This command checks the status of Ethernet connectivity by checking whether the 1300 is pinging the default gateway. The command also prints the IP address of the 1300 and the IP address of the configured default gateway. The following example shows the command and its output:

```
ap#debug fastethernet status
Fast Ethernet Status debugging is on
ap#!!!!!
*Mar 9 06:44:07.091: The IP address of the gateway: xx.xx.xx.x
*Mar 9 06:44:07.091: IP address of the AP: XX.XX.XX.X

ap#
```

### Enhanced PoE for 1250 Series Access Points

The 1250 series access point requires 20 watts of power to operate. Most current 802.3af devices do not provide this much power. However there are some Cisco devices that support 802.3af increased power levels and others will be available in the future. See the documentation for your 802.3af device for additional details. See "Power Considerations" section on page 7for additional information.

# 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

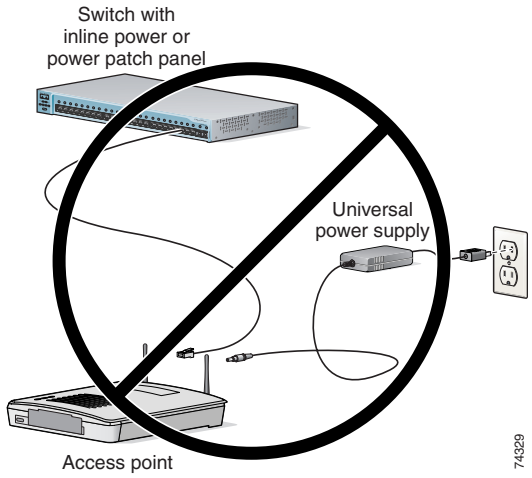
This section describes issues that you should consider before applying power to an access point.

**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.

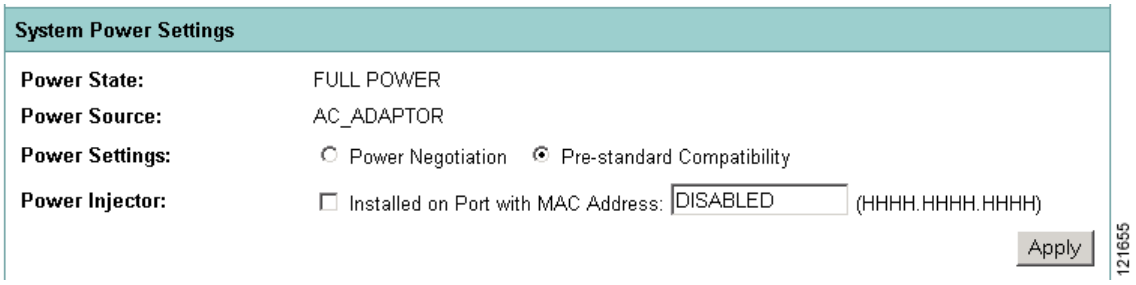
*Figure 2 Improper Power Configuration Using Two Power Sources*




## Configuring Power for 1130, 1240, and 1250 Series Access Points

The 1130, 1240, and 1250 series access points disable 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*




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)[1] | | |
|---|---|---|---|---|---|---|
| | | | | 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<br>2 | Disabled<br>Enabled (default) | 17<br>Disabled | 17<br>14 (11 per Tx)[2] | 17<br>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<br>2 | Disabled<br>Enabled (default) | 17<br>Disabled | 17<br>20 (17 per Tx) | 17<br>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 Bridge

This section contains installation information for the 1400 series bridge.

## 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 the radar is detected. This is an exepected behavior and you should not remove this file. See the caveat CSCsv36602 in the "Open Caveats" section on page 19.

## Bridge Configuration Not Tested on 1250 Series Access Point

Bridging functions have not been tested on the 1250 series access point even though bridge configuration commands are available.

## 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 (insert Krypton release number here) does 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 a new bootloader image 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

## 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, Resolved Caveats access points and bridges in Cisco IOS Release 12.4(10b)JA3.

## Open Caveats

These caveats are open in Cisco IOS Release 12.4(10b)JA3:

- 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.

- CSCso07662—WPA/TKIP downstream throughput degraded when compared to previous versions

  When using WPA/TKIP, normal throughput to a single client is far less than that seen in version 12.4(10b)JA..

  Workaround: None

- CSCsm12509—DOT11-4-MAXRETRIES increase exponentially after upgrade

  After upgrading from Cisco IOS version 12.3(7)JA or a rebuild to either 12.3(8)JEB or 12.3(11)JA1, the following system log message appears:

  DOT11-4-MAXRETRIES

  This message is seen with much greater frequency than before. Quantity of these messages have increased by a factor of 10 to 15. This increase in messages can overflow the syslog server, and changing the logging level less than 4 is unacceptable as other significant system messages will be missed.

  Workaround—Downgrade to a previous version.

- CSCsk80813—Vista's anonymous provisioning does not work with access point local AAA server
- CSCsm62622—Applying access-group to physical int modifies ACL in running-config

  Applying access-group to physical interfaces modifies ACL in running-config when using bridge mode on the physical interfaces.

  When making a physical interface part of a bridge group and the physical interface has an ip access-group <list> [in/out] assigned from a corresponding Access List (ACL) and if this ACL has the logging labeled, the running-config gets modified at the first list match that hits any of the bridged interfaces in such a way that the logging is removed from the ACL.

  Workaround—Instead of assigning the ACL to a physical interface, create a BVI interface for the bridge group and assign the ACL to the BVI.

- CSCsl58293—1242 access point failed to associate using Authentication Shared

  1242 fails to associate via authentication shared using 12.4(10b)JA release image. The same behavior occurs on C3202/C3205 Wireless MICs when they try to associate via authentication shared on their 12.4(3)JK release images.

  Conditions—Configure AP1242 (or C3202/C3205 Wireless MICs) to be root and client devices with authentication method to be authentication shared under the SSID configuration.

  Workaround—Configure a more secure method by using authentication open with WPA-PSK key management.

- CSCsm24495—Configuration change for adding data rate does not reflect in running config
- CSCsm31801—TKIP+ WPAV2+CCKM does not work

  When combination of authentication key-management WPA version 2 CCKM + encryption mode ciphers TKIP is configured, an association failure occurs.

  Workaround—None.

- CSCsm34905—Wrong dynamic VLAN assigned after re-authentication

  After re-association, Wireless-Client gets access to wrong VLAN (Different VLAN then assigned via AAA)

  Conditions—IOS AP, VLAN assignment via AAA, WPAv2 (AES encryption).

  Workaround—Disable PMK caching on wireless client site.

- CSCsm38303—Coverage display on WLSE does not display correctly

  The problem occurs when the coverage display in the location manager on WLSE changes to red, causing an incorrect display. This issue seems to occur on software versions later than 12.4(3g)JA. It does not appear to occur on older versions such as 12.3(11)JA2. The problem has been observed on the following platforms and versions:

  - CWWLSE-1133-K9,1130 / version 2.15
  - - AP1130AG: 12.3(11)JA, 12.4(10b)JA
  - - AP1240AG: 12.4(3g)JA, 12.4(10b)JA

  Workaround—Use an older access point image.

- CSCsm80730—1240 access point does not send a re-association response to client

  When a client tries to roam from one access point to another, during one of the roams the client sends a re-association request, the WDS 1240 Responds with an ACK but does not send a re-association response. The client then sends a deauthentication request and tries to do a full reauthentication.

- CSCsm97867—Autonomous workgroup bridge does not send out bad MIC on broadcast frame

  The autonomous workgroup bridge is used to generate bad MIC TKIP frames for testing access points for proper MIC countermeasures operation. However, when a radio is configured as a workgroup bridge or a repeater, it will not send out the bad MIC frame on a broadcast packet. The radio sends the bad MIC out if it is in root mode, but not workgroup bridge or repeater mode.

  This issue occurs on versions 12.3(8)JA, 12.3(11)JA, 12.4(3g)JA, and 12.4(10b)JA.

- CSCso02086—Unable to apply QoS settings on a standalone access point using the GUI

  QoS settings cannot be applied on a standalone access point using the GUI regardless of which Internet browser used.

  Workaround—Create the QoS policy and apply it to an interface using the command line interface.

- CSCso07171—Fast roaming fails when CCKM is enabled on an access point in workgroup bridge mode.

  When CCKM is enabled in infra-root access points in workgroup bridge mode, fast roaming fails. This issue also seen on ADU CB21AG/PI21AG card clients. It is working correctly with ACU 11a card clients.

- CSCsd99067—AVVID priority map incorrectly maps COS 5 to COS 7 within same VLAN.

  The AVVID priority mapping in the CoS advanced parameters is incorrectly mapping the CoS value to 7 when making a call to a wired phone in same VLAN. This situation occurs in an 802.11g network running one 7921 and one access point.

  Workaround—None.

- CSCse34644—Shared authentication with non-native vlan is not working.

  Workaround—Save the configuration, and reload the access point. When the access point comes up, both clients authenticate. Edit the authentication SSID as follows:

  Add open authentication; remove shared authentication. Then remove open and add shared authentication, and the client will associate. Save the configuration, and reload the access point.

- 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 this 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
```

- CSCsf06407—Packets from Cisco 7920 phones always fall into the COS 6 queue. This problem occurs when the stream feature is enabled.

  Workaround: None.

- CSCsg80305—When 16 SSIDs are configured, client devices sometimes fail to associate to the 16th SSID.

  Workaround: Save the configuration and reload the UC520.

- CSCsg90606—When an SSID is configured with WPA version 2+CCKM and encryption is set to TKIP, wireless clients fail to authenticate to the access point.

  Workaround: None.

- CSCsh84949—Wireless client fails to receive multicast data stream.

  Workaround—Configure **no ip igmp snooping** on the access point.

- CSCsh86675—1310 Bridge continuously authenticates and deauthenticates with LEAP enabled.

  Occurs when 1310 configured as an access point and associating with an Intel 2915 802.11g radio. Client running LEAP associates and disassociates with the client deauthenticating.

- CSCsi10705—The throughput on dual-radio 1200 series access points is sometimes lower than the throughput on a single-radio 1200 series access points.

  Workaround: None.

- CSCsj86643—When you use the a workgroup bridge (WGB) to simulate a WMM/TSPEC client, the WGB/pagent-sourced UP 6 traffic (followed by a TSPEC) is downgraded to best effort when ACM is enabled. This downgrade occurs because the access point and WGB shared driver code assumes that the workgroup bridge is an access point and the uplink traffic is invalid, and thus downgrades all packets.

  Workaround: None.

- 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.

- CSCsk13961—The following MIB objects display incorrect values for 802.11n radios in 1250 series access points:
  - cd11IfAssignedSta
  - cd11IfPhyMacSpecification
  - cd11IfPhyDsssMaxCompatibleRate
  - cd11IfErpOfdmTxPowerLevel5
  - cd11IfClientCurrentTxPowerLeve1

  Workaround: None.
- CSCsk58820—Station roles have different possible RTS threshold values (some 4000 some 2347).

  Workaround: None.
- CSCsk78264—A change in the RF domain name takes effect only after a reboot.

  Workaround: Reboot the controller after changing the RF domain name.
- CSCsl76740—Access point crashes after SNMP query

  An Access point may crash when an SNMP query is performed over an interface where a QoS policy is configured.

  Workaround: None.

# Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.4(10b)JA3:

- 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 vulnerabilityis 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://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20071019-eap
- CSCsg74791—Time-based ACLs do not work properly on Cisco Aironet autonomous access points.
- CSCsm52655—Basic association of infrastructure devices causes traceback.
- CSCsl42896—Roaming between an access point to a non-root bridge prevents network traffic if client is silent.
- CSCsj68025—Roaming between a 1240 series access point bridged on radio 1 fails due to WPA-PSK authentication failure.
- CSCsl49327—Aironet Desktop Utility 2.x EAP-FAST does not work in 12.3(8)JEC and other Cisco IOS releases.
- CsCsk35829—1400 series bridge GUI allows WPAv2 selection as a WPA setting even though AES encryption is not supported.

- CSCsm54952—Access point GUI support needed for adding and displaying local user with “secret.”
- CSCsm70942—Access point sends invalid MAC address in unicast IAPP.
- CSCsm37686—Workgroup bridge configured for TKIP-only cannot associate to (WPA+TKIP)+(WPA2+AES) WLAN.
- CSCsk28551—Root bridge does not update its bridge table.
- CSCsl95464—Access point crashes on WLCCP WDS process.
- CSCsk44106—cDot11ClientUnicastCipher shows incorrect client ciphers at times.
- CSCsl84045—Traceback and bad refcount in datagram_done errors seen on 1230 and 1240 series access points.
- CSCsl22021—The web services page in the access point GUI fails to load,
- CSCsm15944—Nonroot bridge shows env: WARNING: No reading temperature monitoring is at INITIA.
- CSCsl95939—Access point displays misleading “Adhoc client not allowed” message.
- CSCsl72417—Workgroup bridge association problem with WPA-TKIP-CCKM security type.
- CSCsl85710—802.11a workgroup bridge cannot disable DFS channels or enable mobile station.
- CSCsl85798—After DFS event, workgroup bridge does not rescan.
- CSCsb85791—1130 access point crashes just after installation of the new image.
- CSCsk85945—WPA1 workgroup bridge cannot associate to a WPA1+WPA2 WLAN.
- CSCsk63882—Bad ID error with traceback seen when 12.4-Based 802.11 access point starts up.
- CSCsl36227—Tracebacks on workgroup bridge:%SM-4-BADEVENT: Event eapResp is invalid.
- CSCsl46209—1242 access point in workgroup bridge mode 11g radio locks in reset and stops transmitting.
- CSCsl58071—Workgroup bridge occasionally takes a long time to reauthenticate in EAP-TLS.
- CSCsl72417—Workgroup bridge association problem with WPA-TKIP-CCKM security type.
- CSCsl39499—Access point displays%SYS-3-BADLIST_DESTROY traceback then reloads.
- CSCsk70798—Access point does not transmit ppp negotiation and Microsoft VPN stops working

## 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 visit the Technical Support page on cisco.com at the following URL:

http://www.cisco.com/en/US/support/index.html

# 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