Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 12.4(21a)JA1

September 2009

These release notes describe caveats and features for maintenance release Cisco IOS Release 12.4(21a)JA1. This release supports 32+Mb Cisco autonomous access points, including Cisco Aironet 1130, 1140, 1240, and 1250 series access points, and 1300 and 1400 series access points/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, 1140, 1240, 1250 series access points, and 1300 and 1400 series access points/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(21a)JA1 on all 1130, 1140, 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(21a)JA1 :

```
ap1240AG> show version
Cisco Internetwork Operating System Software
IOS (tm) C1240 Software (C1240-K9W7-M), Version 12.4(21a)JA1
Copyright (c) 1986-2009 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**.

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.

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 feature is included in Cisco IOS Release 12.4(21a)JA1:

- 1140 series access point—Business-ready 802.11n wireless access
- European DFS support for EN 301 893, version 1.4.1 and 1.5.1
- Regulatory update for Japan
- Manual channel selection in the 5-GHz bands
- Point-to-point and Point-to-Multi Point bridging support for 802.11n platforms
- Support for 802.11n Performance on 1250 Series Access Points with Standard 802.3af PoE
- Firefox support
- Cisco Wireless LAN Services Engine (WLSE) support
- Antenna support
- Client Link

1140 Series Access Point Support

Cisco IOS release 12.4(21a)JA1 provides support for the Cisco Aironet 1140 Series Autonomous Access Point, a business-ready 802.11n access point designed for simple deployment and energy efficiency

The Cisco Aironet 1140 Series features:

- Six times the throughput of existing 802.11a/g networks.
- A sleek industrial design that blends into any enterprise environment.
- 802.11n performance from standard 802.3af Power over Ethernet.
- Intel Connect with Centrino Certified and 802.11n compliant for guaranteed interoperability with a variety of client devices.
- Environmentally friendly multi-unit Eco-Packs and EnergyStar certified power supplies.

For more information on converting Lightweight Access Point Back to Autonomous Mode, see:

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html#wp161272

European DFS support for EN 301 893, version 1.4.1 and 1.5.1

This feature disables channels 120, 124, and 128 to achieve compliance with draft EN 301 893 version 1.4.1 and 1.5.1. New products that ship with the SKU's listed below will automatically support this feature. Cisco recommends that products shipped prior to xxx upgrade to Cisco IOS software 12.4(21a)JA or 12.3(8)JED to ensure compliance.

- Cisco Aironet 1121AG (AIR-AP1121AG-E-K9)
- Cisco Aironet 1131AG (AIR-AP1131AG-E-K9)
- Cisco Aironet 1142AG (AIR-LAP1142-E-K9)
- Cisco Aironet 1232AG (AIR-AP1232AG-E-K9)
- Cisco Aironet 1242AG (AIR-AP1242AG-E-K9)

- Cisco Aironet 1252AG (AIR-AP1252AG-E-K9)
- Cisco Integrated Services Routers

ETSI EN 301 893 version 1.4.1 and 1.5.1 specify DFS requirements that improve radar detection capabilities so that 802.11 equipment operating in the 5 GHz band can better co-exist with radar systems.

Regulatory update for Japan

This feature provides updated W56 support for the Japanese regulatory domain allows the Cisco Aironet 1130 and 1240 Series Access Points to operate in the 5500 to 5700 MHz bands. Wireless LAN clients experience improved performance due to the expanded channel support for the 5 GHz band.

Manual channel selection in the 5-GHz bands

For 802.11a equipment operating in the 5-GHz band this feature provides customers the flexibility to manually choose the channels in which to operate. The Americas (A) Regulatory domain supports manual configuration for UNII-1 and UNII 3. The European (E) and Korean (K) regulatory domains support manual configuration on any channel.

This feature improves client network design by providing customers the flexibility to select channels of operation.

Point-to-point and Multi Point bridging support for 802.11n platforms

This feature provides point-to-point and point-to-multipoint bridging on the Cisco Aironet 1140 and 1250 Series Access Points. The 5 GHz bands support 20- and 40-MHz and the 2.4-GHz bands support 20 MHz.

The following items are supported for AP1140 and AP1250 bridging:

- MIMO, short-range bridging (on campus or inter-building bridge deployments), with dipole and MIMO antennas (line of sight and short range) under 1 Km.
- 20-MHz and 40-MHz 802.11n support.
- Workgroup bridge (WGB) short-range support.
- SISO (single-in, single-out), MCS 0-7 and legacy bridge rates (802.11 a/b/g and 802.11n) using one outdoor antenna.

Note This is only supported using short range links and is not a replacement for the AP-1240/1300/1400 or other Bridge products.

The following items are *not* supported for AP1140 and AP1250 bridging:

- The **distance** CLI command; long-range links over 1 Km currently are not supported, so the **distance** command is not supported.
- Outdoor MIMO bridging using external antennas has not been fully tested and is not fully supported with this release.

Support for 802.11n Performance on 1250 Series Access Points with Standard 802.3af PoE

The Cisco Aironet 1250 Series requires 20W of power for optimum performance of 802.11n on both the 2.4- and 5-GHz bands. This feature allows you to configure one radio to operate using 802.3af. This allows full functionality under 802.3af on one radio while the other radio is disabled. When you eventually upgrade to a powering solution that provides 20W of power to the access point, you can configure the second radio so that both radios are fully functional with 2x3 multiple input multiple output (MIMO) technology.

Firefox support

This feature provides customers the ability to use the Firefox browser to view and configure the access points web GUI. Support for the Firefox browser provides added flexibility and simplified management for network administrators.

Cisco Wireless LAN Services Engine (WLSE) support

This feature provides customers the ability to use the Cisco Wireless LAN Services Engine (WLSE) to view and configure Cisco Aironet 1140 Series access points. WLSE Software Release 2.15.3 is supported on the following access point firmware images:

- Cisco IOS 12.4(21a)JA
- Cisco IOS 12.3(8)JED

Support for the WLSE provides added flexibility and simplified management for network administrators.

Antenna support

This feature provides support for the new antenna, AIR-ANT2451NV-R. This low-profile, omnidirectional antenna features six elements: a set of three antennas for the 2.4-GHz band and a set of three antennas for the 5-GHz band. Peak gain is 2.5-dBi in the 2.4-GHz band and 3.5-dBi in the 5-GHz band. This antenna was specifically designed for use with 802.11n access points to optimize performance.

ClientLink

Cisco ClientLink is an intelligent beamforming technology that directs the RF signal to 802.11a/g devices to improve performance by 65%, improve coverage by up to 27% percent, and reduce coverage holes.

Cisco ClientLink helps extend the useful life of existing 802.11a/g devices in mixed-client networks. It is beneficial for organizations that move to 802.11n and want to ensure that all clients on the network, regardless of type, are guaranteed the bandwidth and throughput they need.

This feature is only available on 1140 and 1250 series access points.

To enable ClientLink, enter this CLI command in interface configuration mode on 802.11n radio interfaces:

```
beamform ofdm
```

ClientLink is disabled by default. Additional details can be found on cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps10092/prod_white_papers_list.html

Installation Notes

This section contains information that you should keep in mind when installing 1130, 1140, 1240, 1250 series access points, and 1300 and 1400 series access points/bridges.

Access Points

This section contains installation notes for access points.

Installation in Environmental Air Space

Cisco Aironet 1130, 1140, 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

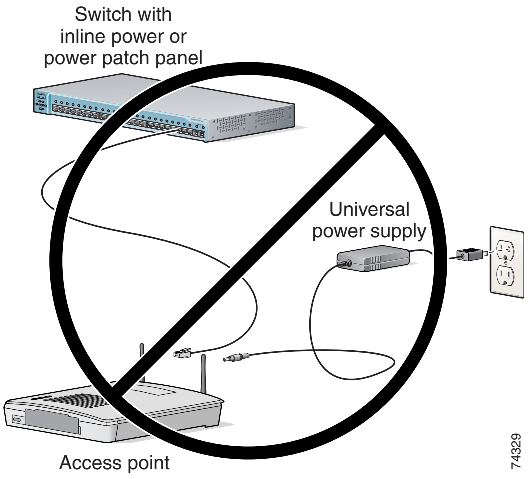
This section describes issues that you should consider before applying power to an access point.

⚠ **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 1 shows the power configuration that can shut down the port on the patch panel or powered switch.

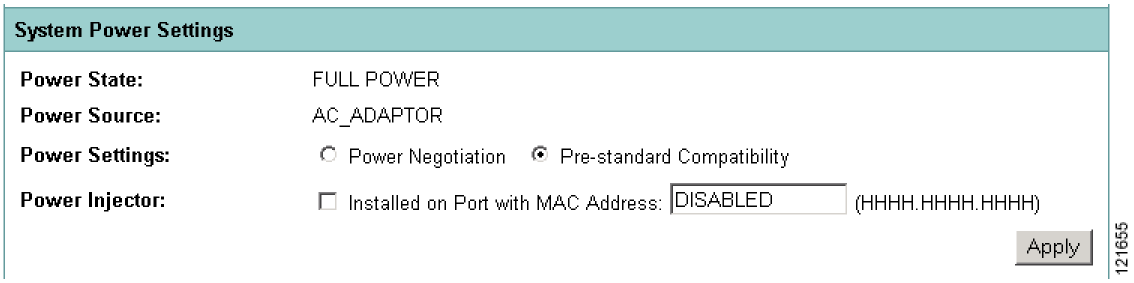
Figure 1 Improper Power Configuration Using Two Power Sources



Configuring Power for 1130, 1140, 1240, and 1250 Series Access Points

The 1130, 1140, 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 2 shows the System Power Settings section of the System Configuration page.

Figure 2 Power Options on the System Software: System Configuration Page



System Power Settings

Power State: FULL POWER

Power Source: AC_ADAPTOR

Power Settings: ○ Power Negotiation ● Pre-standard Compatibility

Power Injector: □ Installed on Port with MAC Address: DISABLED (HHHH.HHHH.HHHH)

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 2	Disabled Enabled (default)	17 Disabled	17 14 (11 per Tx)[2]	17 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 2	Disabled Enabled (default)	17 Disabled	17 20 (17 per Tx)	17 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.

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.

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.

LWAPP to Autonomous Conversion Requires Two Reboots

When you convert an 1142 access point from LWAPP mode to autonomous mode, you might need to reboot the unit twice to complete the conversion.

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 12.4(10b)JA 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 1140 and 1250 Series Access Points with 16 BSSIDs Configured

If your network uses 16 BSSIDs with 1- and 2-Mbps data rates, 1140 and 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, 1140 and 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 and resolved caveats for access points and bridges in Cisco IOS Release 12.4(21a)JA1.

Open Caveats

These caveats are open in Cisco IOS Release 12.4(21a)JA1:

- CSCsv82129—Bad cookie error msg appears in workgroup bridge mode running open.
- CSCsr79628— Number of supported BSSID not shown on access point GUI.

  The **show controllers** command reports the number of BSSIDs supported:
  "Number of supported simultaneous BSSID on Dot11RadioX: 1"

  The above information cannot be seen in the access pont GUI.
- CSCsv75779—Association ping link test page in 1310 GUI produces an error message.

  Workaround: None
- CSCsv97205— 1310 bridge GUI "infrastructure clien" information is invisible.

  Workaround: None

- CSCsx21409—TKIP and CCMP replays generated on queued multicast frames.

  When multicast frames are queued for delivery, then sent, they are sent with bad TSC replay counters. As the client dynamically goes into and out of power save mode, the access point queues multicast frames to be delivered on the next DTIM. Some multicasts may go out immediately and get assigned a higher IV than the queued frames. When the queued frames are delivered, they are sent with their original IV and detected by the WGB as having a TKIP or CCMP TSC Replay.

- CSCsx95753—Last reload always indicate power-on instead of correct reason

  IOS images for 1240 and 801 access points used in c1941w and c890w ARTG platforms always indicate the last reload reason as "power-o" instead of the actual reload reason. Even if the user performs a software load via the console exec prompt, the reload reason is given as "power-on" for the last reload reason.

- CSCsz81157—Security changes disable 11n capability.

  The Cisco access point does not transition properly from PSK to No Security mode. When this transition occurs, 11n stations are not recognized as all MCS rates are absent (sh dot11 ass all). From a protocol perspective, the.11 frames are correct however the AP code does not appear to be working as expected.

  Impact: 11n clients no longer 11n capable. Will not support 11n Tx.

  Conditions:

  - Access point SSID set to use WPA2/AES/PSK.
  - 11n client associated
  - Change SSID to use WPA2/Open
  - Associate 11n client

  Workaround: None. Requires rebooting the access point to reset.

- CSCsz85193— Crash and traceback observed with qos traffic class

  Crash and traceback is observed in access point while configuring radio interface QoS traffic class parameters.

- CSCta75163— Leap to WPA-PSK migration failed on 1300 bridge.

  Workarounds: Change the SSID while migrating from LEAP to WPA-PSK or after migration to WPA-PSK, save the configuration and reload the bridges.

- CSCtb02087—1140 throughput about 70% of H for 1400-byte packets in dual mode.

- CSCtb07019—802.11n access points fail Wi-Fi test case No TKIP + HT rates due to association response.

  The Cisco access point should not send IE45 and IE61 (HT IEs) in the association response to an 802.11n client that is requesting an association using TKIP encryption.

  Correct responses would be:

  1. Do not populate the association request with IE45 and IE61

  2. Do not send a "successfu" association status indicator to the client.

  Conditions: Mixed mode WPA/WPA2 using TKIP and AES must be set on the AP. HT rates enabled on AP. Usually requires a non-conforming client, such as an 802.11n client based on Ralink silicon. Other clients/chipsets may also be able to request TKIP and HT rates.

  Workaround: None

Further Problem Description: The Wi-Fi Alliance is now conducting a negative test case to ensure that an AP does not allow TKIP + HT rates. We currently fail this test case due to our association response.

- CSCtb24821—**dir /all /recursive all-filesystems** CLI causes AP to hang.

  Access point going to hung state if the below commands are executed on the console,

  dir /all /recursive all-filesystems

  dir /recursive /all all-filesystems
- CSCtb55037—Workgroup bridge crashes while shutting and unshutting the radio.
- CSCtb56731—1250 access point in bridge disconnect while operating on DFS channel.
- CSCtb70386—Crash observed with scanner mode AP in RF alpha.
- CSCsz55788—Radio resets and SNMP Q full error is seen in the APs after running radio scan from WLSE.

  The radio resets and SNMP Q full error message is seen when the radio scan on the access point running Cisco IOS Release 12.4(21a)JA1 is triggered from the WLSE and the access points are serving the clients transferring multicast data.

  Workaround:

  - Run the Radio Scan job when the APs are not serving the clients. It is a recommended practice to run the radio scan when the APs are not serving the clients as the radio scan process will disrupts the radio.
  - Downgrade the AP to an earlier version.
- CSCtb60584—Client and access point communication stop at session key update with heavy traffic.

  At session key timeout the station executes session key update the server side windows event log is updated and it shows that session key update completes successfully. After that moment the Chariot and ping stops. On the access point side the following is shown: “%DOT11-4-CCMP_REPLAY: AES-CCMP TSC replay was detected on a packet (TSC 0xD89FF8) received from 001d.7305.0008”. Eventually the access point deauthenticates the station.

  Conditions:[environment] STA:

  - OS: XP+SP3
  - HW: CB72 (2x2)
  - Driver: 7.6.1.264
  - WZC: WPA2-EAP:PEAP(AES)

  Access Point:

  - Software 12.410b.JDA3
  - Cisco AIR-AP1252AG-P-K9
  - Security: WPA2-EAP:PEAP(AES)
  - 2.4GHz/5GHz
  - HT20/40
  - Session key update: 10 min.
  - Group key update: 5 min.

  Radius Server:

  - Windows Server 2008

  - STA/CB72---------Cisco AP1252--------Radius Server

- CSCsz16427—Image recovery process hangs on hard reset.

  The bootable image in flash is not getting erased and the image recovery process hangs after pressing the reset button for more than 20 seconds.

  Workaround: Erase the image in flash manually and then hard reset the access point, or increase the tftpserver timeout value from the default setting.

- CSCtc06925—A 1250 workgroup bridge fails to scan for the uplink when it goes out of A WiFi zone.

  The workgroup bridge fails to scan for the uplink when it goes out of a WiFi zone for more than 30 minutes. When it returns to the WiFi zone the workgroup bridge never gets the uplink, unless the interface is cleared.

  Workaround: Clear the workgroup bridge interface causes it to associate again.

- CSCtc07598—7921 phone disconnects in random fashion and "CM down -feature disable" message is displayed.

  Two 7921 VOIP phones connected to a 1250 or 1130 access point begin a conversation. The call works fine for 45 - 60 minutes but then the call drops and the following message in one of the 7921 phones displays "CM down.feature disable" (receiver phone mostly). After ending the call, the 7921 phone keeps trying to connect the CM IP address, then the phone reassociates with the access point and repeats the cycle.

- CSCtc09255—1140 access point in repeater mode exhibits traceback/crash for WPA-optional.

  Workaround: Shut the interface before changing the security configuration.

- CSCtc15346—AP1252 fails to retransmit missing AMPDU packet in response to block ack

  When a wireless 802.11n client is receiving bulk data—for example, downloading a large file—the transmissions may stall. Pings and other IP connectivity to that client at that time will fail.

  Workaround:

  1. Disable 802.11n on the AP and/or client.

  2. Disable block ack (AMPDU) on the AP and/or client. If the AP is running under WLC control, then use the following commands:

  config 802.11b 11nsupport a-mpdu tx priority all disable

  config 802.11a 11nsupport a-mpdu tx priority all disable

  If the AP is running aIOS, then use this command:

  no ampdu transmit priority 0

  This will cause the AP to transmit bulk data using AMSDU rather than AMPDU, and so may result in a 10-15% throughput reduction.

  Further Problem Description:

  At the time when the transmission stalls, a wireless packet capture will show this sequence of events: The AP1252 transmits an AMPDU packet train. One of the packets in the middle of the train is errored. Client sends a block-ack indicating that the errored packet needs to be retransmitted, but the AP fails to retransmit. Therefore the transmission stalls.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.4(21a)JA1:

- CSCta86845—Workgroup bridge now associates to access point at lower power values on Antenna B.
- CSCtb64826— CCKM FastRoaming no longer fails when workgroup bridge is used as supplicant.
- CSCtb80774—1250 access point in workgroup bridge mode radio operates normally while roaming.
- CSCso07171—Fast roaming no longer fails when CCKM enabled on a workgroup bridge/access point.
- CSCsq99702—Radio Preamble setting is no longer missing on 1250 access point GUI.
- CSCsu33537—Trace back and crash no longer observed on 1240 series infrastructure access point.
- CSCsu37473—1250 series access point can now be placed ROMMON mode.
- CSCsu83607—Hot standby status now shows correct status.
- CSCsu86520—Power level notations are no longer missing in the GUI for 5.8-MHz radio.
- CSCsu99415—Traceback and crash no longer observed on 1300 series non-root bridge.
- CSCsv04096—Clients are now able to join for single basic rate settings.
- CSCsv11772—Traceback no longer observed in WLSE managed 1240 series access point in scanner role.
- CSCsv60216—Encryption flag settings are now cleared when SSID is deleted.
- CSCsv77658—AP reset from watchdog timer no longer expires.
- CSCsv80123—Non-root bridge GUI now displays attributes.
- CSCsv84992—1240 carrier busy test result now displays through repeater.
- CSCsv91069—GUI radio names are now different 2.4- and 5-GHz radios.
- CSCsw20231—Intermittent reachability delay no longer experienced for workgroup bridge client after roam - code port.
- CSCsw27801—1300 series with TLS+CCKM+CKIP-CMIC no longer returns CKIP SEQ replays.
- CSCsw30889—Telnet can now be enabled from 1400 series GUI page.
- CSCsw44775—Programmable Clear Channel Assessment can now be disabled from 1400 series GUI.
- CSCsw49097—FCC DFS test no longer fails on certain off-center frequencies.
- CSCsw59543—Distributor no longer fails to receive message from detector.
- CSCsw70731—Traceback no longer seen when removing SSID on 1250 in bridge mode.
- CSCsw74352—Syslog event CLOCK severity 4 is now operating normally on 1240 series.
- CSCsw75163—IP redirection now functions normally.
- CSCsw75324—TKIP_MIC_FAILURE_REPORT no longer observed on access point.
- CSCsw76942— Wireless service page no longer missing on 1400 series GUI.
- CSCsw78343—GUI-VLAN information no longer missing on the association page.
- CSCsw78812—Hot standby feature no longer inoperative after wnbu_a70 sync.
- CSCsw79801— CKIP_REPLAY no longer observed on 1240 series in repeater mode.

- CSCsw83393—Power Translation Pop up table (mW/dBm) now shows correct values.
- CSCsw91103—The IP address for Client assoc with static IP now displays correctly.
- CSCsw95076—Memory leaks & trace back no longer observed in Alpha testing network.
- CSCsw96918—Upgrade tool v3.4 now retains access point hostname.
- CSCsx07150—Voice gap no longer experienced when phone roams if CAC is not configured on access points.
- CSCsx07791—AP loses no longer loses inbound EAP when marked with QoS.
- CSCsx13673—EAP profile with FAST auth method no longer fails in supplicant authentication.
- CSCsx17666—1250 GigabitEthernet Requested Duplex radio button is now functional.
- CSCsx22544—Tracback & crash no longer observed in WDS/ Infrastructure access point in alpha setup
- CSCsx30348—Request for channel selection menu now displays normally.
- CSCsx31742—GUI cLient-MFP now displays on 1300 series association page.
- CSCsx33413—access points no longer deauthenticates all wireless clients after losing registration to WDS access point.
- CSCsx34747—1252 access point in duplex full connected to a 2950 device no longer shows not connected.
- CSCsx43549—Root bridge page on 1250 GUI displays correct client information.
- CSCsx50775—AES-CCMP TSC no longer replays on 1252 access point running Cisco IOS Release 12.4(10b)JA3.
- CSCsx52177—Workgroup bridge with EAP-FAST authentication no longer fails with new credential.
- CSCsx72921—Remove "broadcast-key rotation interval" on 5-GHz radio now displays correctly on workgroup bridges.
- CSCsx73886—Prestd switch default for autonomous access points now set to change to off.
- CSCsx75087—1310 with CCKM/CMIC now able to associate.
- CSCsx75214—1310 with CCKM/CKIP no longer fails authentication when econcat is enabled or disabled.
- CSCsy26872—Bridge no longer crashes QOS with VLAN while Telnet NRB.
- CSCsy32134—WPAv2 is now defined as a value of **show wlccp wds mn detail**.
- CSCsz06757— WGB radio interface no longer resets after UP-link established.
- CSCsz16621—Access Point GUI menu bar display is now stable.
- CSCsz38571—Radio failed and traceback no longer observed while running radio scan.
- CSCsz43843—Debug dot11 dot11 0/1 command options are no longer missing on CLI.
- CSCsz48460—Access point no longer crashing on dot11_tx.
- CSCsz68391—Call is now admitted in 802.11b when CP7921 surplus BW is set to 1.3000.
- CSCsz71946—AES-CCMP TSC replays seen in alpha nw.
- CSCsz85064—Workgroup bridge connection no longer resets after UP-link established to the roamed access point.
- CSCsz89026—Radio failed traceback and reload no longer observed in nonroot 1300 series bridge.

- CSCta02897— SNMP walk for cd11IfChanSelectTable no longer causes crash and watchdog timer.
- CSCta08443—Clients in WPA migration mode and static WEP clients now receive IP address.
- CSCta42089— Station-role fallback repeater no longer displays as a repeater on GUI.
- CSCta65687—1250 access point in non-root bridge mode no longer crashes multiple times during perf-test.
- CSCta77952—Multicast no longer fails between wireless clients associated to a 1310 bridge.
- CSCtb06469—1200 series access points no longer lock up due to possible memory leak.
- CSCtb10521—1250 series GUI page no longer displays error after linktest is performed.
- CSCtb26913—Two sets of HT IEs are no longer advertised in association response.
- CSCtb45810—Access point no longer crashes when **show interfaces Dot11Radio> history** CLI command issued.
- CSCtb50039—1250 series access point in bridge mode no longer flaps in P2MP setup.

Closed Caveats

These caveats are closed and will not be addressed:

CSCtc33410—Autonomous LAP 1140 MCS rates should not be basic/mandatory by default.

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find select caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at http://www.cisco.com/cisco/web/support/index.html. 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