



Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(8)JEC2

October 31, 2008

These release notes describe caveats and features for maintenance release Cisco IOS Release 12.3(8)JEC2. This release supports 16-Mb Cisco autonomous access points, including Cisco Aironet 1100, 1200, and 1230 series autonomous access points. The Cisco Aironet 350 series is no longer supported in this release or any future release.

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Installation Notes, page 3](#)
- [New Features, page 6](#)
- [Important Notes, page 8](#)
- [Caveats, page 18](#)
- [Troubleshooting, page 20](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 20](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

Introduction

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

You can configure and monitor 1100, 1200, and 1230, series access points using the command-line interface (CLI), the web-browser interface, or Simple Network Management Protocol (SNMP).

System Requirements

Cisco IOS Release 12.3(8)JEC2 is a general maintenance release that concentrates on bug fixes and includes minor features. You can install Cisco IOS Release 12.3(8)JEC2 on any Cisco Aironet 1100, 1210, or 1230 series access point.



Note

Software upgrades fail when you use the web-browser interface to install Cisco IOS Release 12.3(8)JEC2 on 1200 series access points. The image size exceeds the access point's 4-MB restriction for software upgrades. Use TFTP to upgrade your access point to this release. For complete instructions on using TFTP to upgrade access point software, see the "Working with Software Images" section in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*. Click this link to browse to that document:

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

You can also install this release on 1200 series access points that have been converted to run Cisco IOS software. You can verify that an access point runs VxWorks or Cisco IOS software by looking at the GUI: the GUI on an access point running VxWorks has a yellow and red color scheme, and the GUI on an access point running Cisco IOS software has a green, light-green, and black color scheme.

Your 1200 series access point must run one of these VxWorks releases before you can convert to Cisco IOS software: 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T. If your access point runs version 12.04, you must downgrade to a supported VxWorks release before upgrading to Cisco IOS software.

The conversion upgrade image for 1200 series access points installs Cisco IOS Release 12.2(13)JA2 on your 1200 series access point.



Caution

Do not attempt to load a Cisco IOS image on 1200 series access points that have not been converted. Doing so can disable the access point.

Finding the Cisco IOS Software Version

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 12.3(8)JA:

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.3(8)JA
Copyright (c) 1986-2006 by Cisco Systems, Inc.
```

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

Upgrading to a New Software Release

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

-
- Step 1** Follow this link to the Cisco home page:
<http://www.cisco.com>
 - Step 2** Click **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>

Installation Notes

This section contains information that you should keep in mind when installing Cisco Aironet autonomous access points.

Installation in Environmental Air Space

This section provides information on installing 1100 and 1200 series access points in environmental air space, such as above suspended ceilings.

Cisco Aironet 1100 and 1200 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.

**Note**

If you plan to mount a 1200 series access point with a 5-GHz radio in an area subject to environmental air space, we recommend that you mount the access point horizontally so that its antennas point down. Doing so ensures that the access point complies with regulatory requirements for environmental air space with the 5-GHz radio installed.

Power Considerations

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

**Caution**

The operational voltage range for 1100 series access points is 35 to 57 VDC, and the nominal voltage is 48 VDC. Voltages higher than 60 VDC can damage the equipment.

**Caution**

The nominal voltage for 1200 series access points is 48 VDC, and the access point is operational up to 60 VDC. Voltages higher than 60 VDC can damage the equipment.

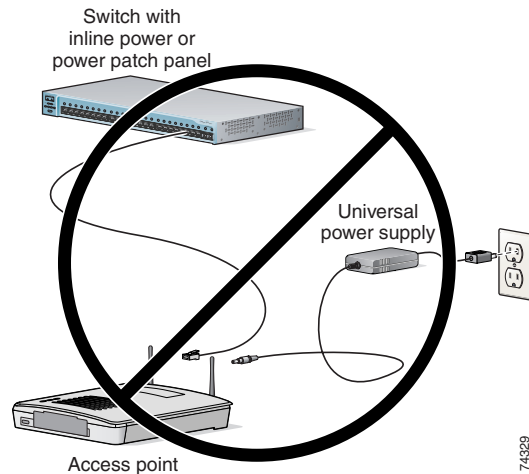
**Caution**

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 1100 and 1200 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*



Using the AC Power Adapter

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

Using a Switch Capable of IEEE 802.3af Power Negotiation

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

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

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

Using a Power Injector

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

Operating 5-GHz Radio Requires Power Injector, Power Module, or Catalyst 3550-24 PWR Switch

The 1200 series power injector and the 1200 series power module support operation of the 5-GHz radio in the access point. The Catalyst 3550-24 PWR switch supports power for both the 2.4-GHz radio and the 5-GHz radio. Other switches and power patch panels might not provide enough power for the 5-GHz radio.

Access Point Requires 1200 Series Universal Power Supply and Power Injector

If you use a power injector or a power module to provide power to a 1200 series access point, you must use a 1200 series universal power supply. If you need to use a power injector to inject power into the access point's Ethernet port, you must use a 1200 series power injector.

Unpowered 1100 Series Access Points Cause Loopback When Connected to Switches Without Loopback Detection

When you connect an unpowered 1100 series access point to a switch without loopback detection, the access point causes a loopback. To avoid this problem, make sure loopback detection is enabled on the switch to which the access point is connected. If your switch does not have loopback detection, disconnect the access point from the switch when the access point power is off.

Antenna Installation

For instructions on the proper installation and grounding of external antennas for 1200 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.

New Features

The following new feature is included in Cisco IOS Release 12.4(10b)JA3. See [“System Log Messages” section on page 16](#) for additional details.:

- System log message enhancement

System Log Message Enhancement

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

Error Message %DOT11-4-LOADING_RADIO: Interface [chars], loading the radio firmware ([chars])

Explanation The radio has been stopped to load new firmware.

Recommended Action Recommended Action: No action is required.

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

Explanation The data link level line protocol has changed state.

Recommended Action No action is required.

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

Explanation A reload or restart was requested.

Recommended Action Notification message only. No action is required.

Error Message %SYS-5-CONFIG_I: Configured from [chars] by [chars]

Explanation The router configuration has been changed.

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

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

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

Recommended Action No action is required.

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

Explanation The SNMP server completed a coldstart.

Recommended Action Notification message only. No action is required.

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

Explanation The system clock has been modified.

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

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

Explanation The logger process has been initialized and started.

Recommended Action No action is required.

Error Message DHCP-6-ADDRESS_ASSIGN

Explanation The DHCP server assigned an IP address to Interface BVI1. (Example: DHCP-6-ADDRESS_ASSIGN (ex.%DHCP-1-ADDRESS_ASSIGN: Interface BVI1 assigned DHCP address 192.168.0.13, mask 255.255.255.0, hostname 1241).

Recommended Action None

Error Message NO_SSID_OR_NO_VLAN

Explanation No SSID or VLAN is configured. (Example:%DOT11-1-NO_SSID_OR_NO_VLAN: No SSID configured. Dot11Radio0 not started.)

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

Important Notes

This section describes important information about the access point.

CCKM and Fast Roaming on Cisco 7921/7925 IP Phones

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

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

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 expected behavior and you should not remove this file. See the caveat CSCsv36602 in the [“Open Caveats” section on page 18](#).

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.

Layer 3 Not supported with NAC for MBSSID

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

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

In this release, Dynamic Frequency Selection (DFS) is automatically enabled on 5-GHz radios configured for use in North America. The 5-GHz radios use DFS to detect radar signals and avoid interfering with them. Radios configured for use in Europe and Singapore also use DFS. Other regulatory domains do not use DFS. Refer to the [“DFS Enabled by Default on 5-GHz Radios in North America” section on page 9](#) for detailed information.

Change to Default IP Address Behavior

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

- When you connect a 1200 or 1230 series access point with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an address, continues to send requests indefinitely.
- When you connect an 1100 series access point with a default configuration to your LAN, the 1100 series access point makes several attempts to get an IP address from the DHCP server. If it does not receive an address, it assigns itself the IP address 10.0.0.1 for 5 minutes. During this 5-minute window, you can browse to the default IP address and configure a static address. If after 5 minutes the access point is not reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the 5-minute window for browsing to the access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

Save Interface Level Configuration Before Upgrading to Releases 12.3(8)JEC2

If the access points have SSIDs configured at the interface level (rather than at the global level), before upgrading to Cisco IOS Release 12.3(7)JA and above, upgrade to Cisco IOS Release 12.3(4)JA, save the configurations, and then upgrade to Release 12.3(8)JEC2. This procedure must be followed to make sure that the SSID configurations are converted from the interface level to global level.

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

In this release, the radio or radios are disabled by default, and there is no default SSID. You must create an SSID and enable the radio or radios before the access point 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 Might Fail to Authenticate

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

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

Default Username and Password Are *Cisco*

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

Some Client Devices Cannot Associate When QoS Is Configured

Some wireless client devices, including Dell Axim handhelds and Hewlett-Packard iPaq HX4700 handhelds, cannot associate to an access point when the access point is configured for quality of service (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 you use to re-enable the radio:

```
AP1134(config)# interface d1
AP1134(config-if)# shut
AP1134(config-if)# no mbssid
AP1134(config-if)# no shut
```

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

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

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

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

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

AIR-RM21A/AIR-RM22A Radio Modules Usually Set to Max Transmit Power

AIR-RM21A and AIR-RM22A radio modules measure transmit power in decibels per milliwatt (dBm), but earlier versions of 802.11a radios in Cisco Aironet access points measure power in milliwatts (mW). Because power settings in mW do not translate directly to settings in dBm, the access point usually uses the default power setting of maximum when you install a new AIR-RM21A or AIR-RM22A radio module.

[Table 1](#) lists 802.11a transmit power settings in mW and the power settings that the access point assigns to a new radio module.

Table 1 Transmit Power Settings Assigned to New Radio Modules

| Power Settings in mW | Power Setting Assigned to New Radio Module |
|----------------------|--|
| 5 | 5 dBm (approximately 3 mW) |
| 10 | maximum (17 dBm) |
| 20 | maximum |
| 40 | maximum |

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 problem 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.

Transmit Power Set to Maximum When You Install 802.11g Radio

When you replace the 802.11b radio in a 1200 series access point with an 802.11g radio, the 802.11g radio is set to the maximum transmit power allowed in your regulatory domain, regardless of the power setting configured on the 802.11b radio. After you install the 802.11g radio and the access point reboots, configure the 802.11g radio to the preferred transmit power.

Use Auto for Ethernet Duplex and Speed Settings

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



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

Use force-reload Option with archive download-sw Command

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

Radio MAC Address Appears in Access Point Event Log

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

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

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

Repeater Access Points Running Cisco IOS Software Cannot Associate to Parent Access Points Running VxWorks

1200 series repeater access points running Cisco IOS software cannot associate to parent access points that do not run Cisco IOS software (1200 series access points that have not been converted to run Cisco IOS software).

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.

Crossover Cable Sometimes Needed When Ethernet Speed and Duplex Set to Fixed on 1100 Series Access Points

If you change the speed and duplex settings from auto to fixed on an 1100 series access point Ethernet port, the auto-MDIX feature on the port is disabled. When auto-MDIX is disabled, you must determine whether to use a straight-through or a crossover cable to connect the access point Ethernet port to another device. If the Ethernet link goes down after you set the speed and duplex to fixed, try changing the Ethernet cable from crossover to straight-through or from straight-through to crossover.

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.

1100 Series Access Points with Boot Loader Version 12.2(4)JA Boot into Monitor Mode

When the Ethernet port is disabled on an 1100 series access point running boot loader version 12.2(4)JA, the access point boots into monitor mode when it reboots. To avoid this problem, connect the access point Ethernet port to one of the following:

- a wired LAN
- the Ethernet port on a PC

Remove power from the access point, and reapply power to reboot the unit. When the access point senses an Ethernet connection, it boots normally.

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.

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 to 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.

System Log Messages

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

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

The command syntax is as follows:

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

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

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

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

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

| Facility Name | Event | Subevent |
|---------------|---|--|
| system | clock config logger (12.3(8)JEC2 only) reload restart | – |
| dot11 | uplink radio rogue ap ssid | failed, down load no-ssid-or-no-vlan |
| rogue ap | – | – |

| | | |
|--------|----------------|-----------------------|
| radius | down up | – |
| link | interface | up-down, link-changed |
| DHCP | address-assign | |
| SNMP | cold-start | – |
| LINE | up-down | – |

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

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

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

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

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

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

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

Caveats

This section lists open and resolved caveats for access points.

Open Caveats

These caveats are open in Cisco IOS Release 12.3(8)JEC2:

- 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.
- 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.
- 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.
- CSCsl62517—Probe response not appearing for all 16 MBSSIDs to broadcast probe request
 Only a subset of all configured 16 MBSSIDS respond to a broadcast probe request.
 Impact—Dependent upon the client implementation, client may not try to associate to if it does not receive its desired SSID.
 Workaround—None
- CSCsr79628—Number of supported BSSID not shown in access point GUI
 The **show controllers** command reports the number of BSSIDs supported, for example Number of supported simultaneous BSSID on Dot11RadioX: 16
 However this information does not appear on the access point GUI.
- CSCsr43516— Cannot configure dot1x on WDS infrastructure access point GUI
- CSCsq64212—Clock save interval doesn't save date with access point.
 When an access point is configured with the **clock save interval** command and is rebooted, the clock reverts back to the default 2002 date. The issue occurs when the access point is configured to authenticate to another access point configured as a bridge or workgroup bridge and the authentication type is EAP-TLS. After the access point reboots, the certificates are considered invalid because of the dates.
 Workaround: Manually set the clock on the access point after each reboot.
- CSCsr53764—Some wired workgroup bridge clients get stuck randomly while roaming.
 The workgroup bridges are installed on a train with its clients running customer-specific applications. The workgroup bridge roams very fast between access points due to the speed of the train. When the the train moves through a tunnel, some workgroup bridges often remain associated

to a specific access point. For example, when the train travels toward access point 020, the workgroup bridge associates with it and wired clients associate with this workgroup bridge. After the workgroup bridge roams to the next access point (for example 021, 022, or 023), some wired clients still show up under access point 020 even though the workgroup bridge has moved to a new access point. As a result, the wired clients associated with the workgroup bridge lose their connection with the outside network.

Workaround: None.

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

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.3(8)JEC2:

- CSCsl00363—Changing 802.1x credentials on workgroup bridge for EAP-FAST requires a reboot
- CSCso70124—Failing to populate SNMP instance for non-VLAN (cd11IfVlanSecurityTable)
- CSCsl22194—CLI command **show dot11 association** shows negative values
- CSCsm34905—Wrong dynamic VLAN assigned after re-authentication
- CSCso10119—1231 access point reboots
- CSCsm78141—Access point never sends authenticate-fail trap
- CSCso62119—CLI command **WlanEncryptionMode** always returns WEP mode even when encryption is set to AES
- CSCso02086—Unable to apply QoS settings on the standalone AP through GUI
- CSCsq29310—Javascript error in file ap_contextmgr_ap.shtml
- CSCsm73025—Workgroup bridge dependent CLI commands not cleared after unconfiguring
- CSCso57659—More events needed in syslog logging levels severity feature support
- CSCsk42319—No error message is generated when key management WPAv1 with AES-CCM
- CSCek69256—A —dot11_mgr_disp.c: coding error
- CSCsq34053—**power client** and **no power client local** added after access point reloads.
- CSCsl49327—ADU 2.x eap-fast does not work in Cisco IOS Release 12.3(8)JEC.
- CSCsr11909—Access point ARPing for non local WLSM tunnel loopback destination address.
- CSCsr27699—Roaming operation does not work correctly.
- CSCsu41132—IP http timeout-policy does not log a user out.
- CSCsm80730—1240 series access point does not send a reassociation response to client.
- CSCir02221—CCKM issue with 1240 series access points.

This caveat is resolved in Cisco IOS Release 12.3(8)JEC3:

- CSCsv04836—Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being

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

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

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

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6>

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 a defect 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>

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)