Release Notes for Cisco Aironet 1310 Outdoor Access Point/Bridge for Cisco IOS Release 12.3(2)JA

November 4, 2004

These release notes describe open caveats for Cisco IOS Release 12.3(2)JA. They also provide important information about the Cisco Aironet 1310 Outdoor Access Point/Bridge (hereafter called the *1310 access point/bridge*).

Contents

These release notes contain the following sections.

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

Introduction

The Cisco Aironet 1310 Outdoor Access Point/Bridge is an 802.11b/g device that provides high speed and cost-effective wireless connectivity between multiple fixed or mobile networks and clients. The flexibility of the device allows it to operate as an access point, wireless bridge, or workgroup bridge. Building a metropolitan area wireless infrastructure with the 1310 access point/bridge provides deployment personnel with a flexible, easy to use solution that meets the security requirements of wide area networking professionals.

The 1310 access point/bridge supports the 802.11b/g standard, providing 54-Mbps data rates with a proven, secure technology. Cisco makes the maintenance and installation of the access point/bridge easy by integrating it with your wired network using the Cisco SWAN solution. Based on the Cisco IOS operating system, the 1310 access point/bridge includes advanced features such as Fast Secure Roaming, QoS, and VLANs.

System Requirements

You can install Cisco IOS Release 12.3(2)JA on the 1310 outdoor access point/bridge.

Finding the IOS Software Version

To determine the version of IOS running on your 1310 access point/bridge, use a Telnet session to log into the access point/bridge and enter the **show version** EXEC command. This example shows command output from a 1310 access point/bridge configured as a bridge running Cisco IOS Release 12.2(15)JA:

```
ap> show version
Cisco Internetwork Operating System Software
IOS (tm) C1310 Software (C1310-K9W7-M), Version 12.2(15)JA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
```

You can also find the software version on the System Software Version page in the device's web-browser interface. 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 1310 series software:

1. Follow this link to the Cisco Support page:

   http://www.cisco.com/cisco/web/support/index.html

   Follow this path to the product, document, and chapter:

   Aironet 1300 Series Wireless LAN Products > Cisco Aironet 1300 Series Bridge Software Configuration Guide > Managing Firmware and Configurations > Working with Software Images

2. Click this link to browse to the Cisco IOS Software Center on Cisco.com:

   http://www.cisco.com/cisco/software/navigator.html

3. On the Web page, log in to access the Feature Navigator or the Cisco IOS Upgrade Planner, or click **Wireless Software** to go to the Wireless LAN Software page.

New Features

This section lists new features in Cisco IOS Release 12.3(2)JA for the 1310 access point/bridge.

The Cisco Aironet 1310 Outdoor Access Point/Bridge supports the same Cisco IOS Software access point features as Cisco Aironet 1100 Series Access Points in Cisco IOS Software Release 12.2(13)JA and earlier Cisco IOS Software releases with the exception of radio management aggregation, Wireless Domain Services (WDS), and IEEE 802.1X local authentication service.

The 1310 access point/bridge supports the same Cisco IOS Software wireless bridge features as the Cisco Aironet 1400 Series Wireless Bridge in Cisco IOS Software Release 12.2(13)JA and earlier Cisco IOS Software releases with the exception of IEEE 802.11a.

The following new features are supported by the 1310 access point/bridge:

- HTTPS – HTTP with SSL 3.0
- AES-CCMP (when in access point and bridge mode)
- IEEE 802.1X local authentication service for EAP-FAST
- Wi-Fi Multimedia (WWM) required elements
- VLAN assignment by name
- Microsoft WPS IE SSIDL
- HTTP Web Server v1.1
- IP-Redirect

To learn more about all the features supported by the 1310 access point/bridge, refer to the IOS Feature Navigator at the following link on Cisco.com:

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

HTTPS - HTTP with SSL 3.0

This feature supports a Secure Sockets Layer (SSL)/Secure Hypertext Transfer Protocol (HTTPS) method of managing Cisco Aironet access points via a Web browser using HTTP.

AES-CCMP

This feature is active when the 1310 is in the access point and bridge modes. The feature supports Advanced Encryption Standard–Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). In the access point mode, the 1310 supports both AES-CCMP and WPA2. In the bridge mode, the 1310 supports AES-CCMP but not WPA2 because WPA2 cannot be tested in the bridge mode. AES-CCMP is required for Wi-Fi Protected Access 2 (WPA2) and IEEE 802.11i wireless LAN security.

IEEE 802.1X Local Authentication Service for EAP-FAST

This feature expands wireless domain services (WDS) IEEE 802.1X local authentication to include support for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST). IEEE 802.1X local authentication was introduced in Cisco IOS Software release 12.2(11)JA.

Wi-Fi Multimedia (WMM) Required Elements

This feature supports the required elements of Wi-Fi Multimedia (WMM). WMM is designed to improve the user experience for audio, video and voice applications over a Wi-Fi wireless connection. WMM is a subset of the IEEE 802.11e Quality of Service (QoS) draft standard. WMM supports QoS prioritized media access via the Enhanced Distributed Channel Access (EDCA) method. Optional elements of the WMM specification including call admission control using traffic specifications (TSPEC) are not supported in this release.

VLAN Assignment By Name

This feature allows the Remote Authentication Dial-In User Service (RADIUS) server to assign a client to a virtual LAN (VLAN) identified by its VLAN name. In releases before Cisco IOS Software release 12.3(2)JA, the RADIUS server identified the VLAN by ID. This feature is important for deployments where VLAN IDs are not used consistently throughout the network.

Microsoft WPS IE SSIDL

This feature allows the Cisco Aironet access point to broadcast a list of configured SSIDs such as SSID Lists (SSIDL) in the Microsoft Wireless Provisioning Services Information Element (WPS IE). A client with the ability to read the SSIDL can alert the user to the availability of the SSIDs. This feature provides a bandwidth-efficient, software-upgradeable alternative to multiple broadcast SSIDs (MB/SSIDs).

HTTP Web Server v1.1

This feature provides a consistent interface for users and applications by implementing the HTTP 1.1 standard (see RFC 2616). In previous releases, Cisco software supported only a partial implementation of HTTP 1.0. The integrated HTTP Server API supports server application interfaces. When combined with the HTTPS and HTTP 1.1 Client features, provides a complete, secure solution for HTTP services to and from Cisco devices.

IP-Redirect

This features provides the capability to redirect traffic intended for a particular destination to another IP address specified by the administrator.

Features Not Supported

The following features that were introduced in Cisco IOS Software Release 12.2(13)JA or earlier that are not supported by the Cisco Aironet 1310 access point/bridge:

- Radio management
- Radio management aggregation
- Layer 3 Mobility Service via fast secure roaming tunnels
- Wireless Domain Services (WDS)
- IEEE 802.11a support

Installation Notes

This section contains important information to keep in mind when installing your 1310 access point/bridge.

Warnings

Warning **This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.**

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Warning **Do not locate 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 in contact with such circuits, as they may cause serious injury or death. for proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:**
120 VAC, 15A U.S. (240vac, 10A International)

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Warning **Read the installation instructions before you connect the system to its power source.**

Warning **Do not work on the system or disconnect cables during periods of lightning activity.**

Warning **Do not operate your wireless network near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.**

Warning **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft. (2 m) from your body or nearby persons.**

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.**

Vehicle Installations

The following warnings apply to vehicle installations:

Warning **A readily accessible two-pole disconnect device must be incorporated in the fixed wiring.**

Warning **Connect the unit only to CD power source that complies with the safety extra-low (SELV) requirements in IEC 60950 based safety standards.**

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the 1300 series.

FCC Safety Compliance Statement

FCC Compliance with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified eqipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

Warning **Do not locate 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. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.:NFPA 70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).**

Each year hundreds of people are killed or injured when attempting to install an antenna. In many of these cases, the victim was aware of the danger of electrocution, but did not take adequate steps to avoid the hazard.

For your safety, and to help you achieve a good installation, please read and follow these safety precautions. **They may save your life!**

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type antenna you are about to install.
2. Select your installation site with safety, as well as performance in mind. Remember: electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
4. Plan your installation carefully and completely before you begin. Successful raising of a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task, and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
5. When installing your antenna, remember:
   a. **Do not** use a metal ladder.
   b. **Do not** work on a wet or windy day.
   c. **Do** dress properly—shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember, the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line complete an electrical path through the antenna and the installer: **you!**
7. If any part of the antenna system should come in contact with a power line, **don't touch it or try to remove it yourself. Call your local power company**. They will remove it safely.
8. If an accident should occur with the power lines call for qualified emergency help immediately.

1310 Installation

The 1310 access point/bridge is available in two configurations:

- Integrated antenna access point/bridge (with 13-dBi patch array antenna)
- External antenna access point/bridge (with antenna connector for use with an external antenna)

Note To meet regulatory restrictions, the external antenna configuration and the external antenna must be professionally installed.

Note When installing the dual-coax cable, it is acceptable to unzip or pull the two cables apart at the ends if more separation is needed between the male F connectors.

Personnel installing the 1310 access point/bridge must understand wireless bridging techniques, antenna alignment and adjustment, and grounding methods. The integrated antenna configuration can be installed by an experienced IT professional.

Important Notes

This section describes important information about the access point.

Default Username and Password Are *Cisco*

When you open the 1310 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.

Proxy Mobile-IP Feature Removed From This Release

The proxy Mobile-IP feature is not supported in Cisco IOS Release 12.3(2)JA.

WPA/2 With Concatenation Not Supported

Cisco IOS Release 12.3(2)JA does not support this feature.

Hard Coded Ethernet Port Settings Degrade GUI Performance

Ethernet port settings on the 1300 must be set to auto speed and auto negotiation. If you use any other setting, the GUI operates very slowly. For additional information, caveat CSCef45010 in the "Open Caveats" section on page 13.

New Express Security Page Simplifies Security Setup

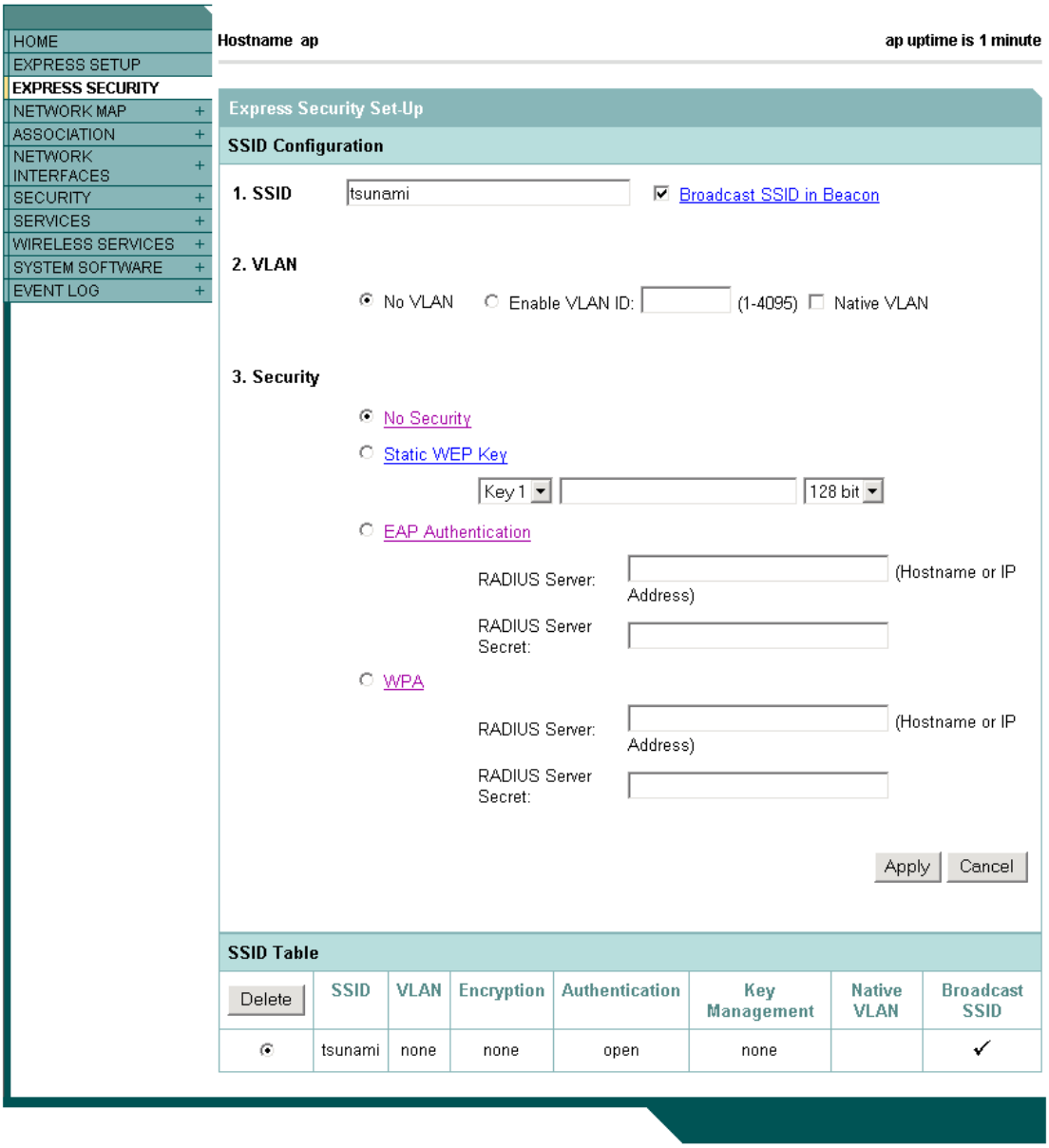
The new Express Security page in the 1310 web-browser interface makes it easier to create SSIDs and assign security settings to them. Figure 1 shows the Express Security page.

Limitations of the Express Security page include:

- You cannot edit SSIDs. However, you can delete SSIDs and re-create them.
- You cannot assign SSIDs to specific radio interfaces. The SSIDs that you create are enabled on all radio interfaces. To assign SSIDs to specific radio interfaces, use the Security SSID Manager page.
- You cannot configure multiple authentication servers. To configure multiple authentication servers, use the Security Server Manager page.
- You cannot configure multiple WEP keys. To configure multiple WEP keys, use the Security Encryption Manager page.
- You cannot assign an SSID to a VLAN that is already configured on the access point. To assign an SSID to an existing VLAN, use the Security SSID Manager page.
- You cannot configure combinations of authentication types on the same SSID (such as MAC address authentication and EAP authentication). To configure combinations of authentication types, use the Security SSID Manager page.

For complete instructions on using the Express Security page, see the "Configuring Basic Security Settings" section on page 2-11 in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*. Click this URL to browse to that document:
http://www.cisco.com/en/US/products/hw/wireless/ps4570/tsd_products_support_configure.html

Figure 1 Express Security Page



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 using the mode button to reset the unit to default settings.

1310 Access Point/Bridge Does Not Support Loopback Interface

When configuring the 1310 access point/bridge as an access point, you must not configure a loopback interface.

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 1310 access point/bridge when it is configured as an access point or workgroup bridge. If your non-Cisco Aironet 802.11g client device does not associate to the 1310 access point/bridge, 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 1300 series radio for **best throughput**, the 1310 access point/bridge 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 Radio0-802.11G Settings pages and in the **speed** CLI configuration interface command.

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 after the upgrade, the pages in the web-browser interface might not reflect the upgrade. This example shows how to upgrade system software successfully using the **archive download-sw** command:

```
AP# archive download-sw /force-reload /overwrite tftp:/10.0.0.1/ image-name (image name)
```

Radio MAC Address Appears in ACU

When a Cisco Aironet client device associates to an access point or bridge running IOS software, the device's MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point or bridge radio. The MAC address for the access point or bridge's Ethernet port is printed on the label on the back of the access point or bridge.

Radio MAC Address Appears in 1310 Access Point/Bridge 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 1310 access point/bridge.

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 1310 access point/bridge 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 1310 access point/bridge accepts any IP address. If you enter 0.0.0.0, the 1310 access point/bridge looks for an exact match with the IP address that you entered in the IP Address field.

System Software Upgrade Sometimes Fails Using Microsoft Internet Explorer 5.01 SP2

A system software upgrade sometimes fails when you use Microsoft Internet Explorer version 5.01 SP2 to upgrade system software using the HTTP Upgrade page in the web-browser interface. Use a later version of Microsoft Internet Explorer to perform HTTP system software upgrades, or use TFTP to upgrade system software. Click this URL to browse to the *Cisco 1300 Series Wireless Bridge Software Configuration Guide* for complete instructions on performing software upgrades:

http://www.cisco.com/en/US/docs/wireless/access_point/1300/12.3_4_JA/configuration/guide/brsc1234.html

Corrupt EAP Packet Sometimes Causes Error Message

During client authentication, the 1310 access point/bridge 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 these messages.

When Cipher is TKIP Only, Key Management Must Be Enabled

When “Cipher TKIP” is configured on a VLAN, the SSID(s) for that VLAN must use WPA or CCKM key management. If you do not configure the SSID(s) for that VLAN with WPA or CCKM, client authentication fails on the SSIDs.

Non-Cisco Aironet Clients Sometimes Fail 802.1x Authentication

Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the 1310 access point/bridge 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**.

Microsoft Patch Fixes WPA Authentication Delay

When the 1310 access point/bridge is configured for optional or mandatory WPA authentication, client adapters in Windows XP platforms sometimes experience a delay when initially authenticating to the access point immediately after it starts up. A patch from Microsoft resolves this issue. The patch is described in Microsoft Knowledge Base Article 826942.

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

Limitation to PAgP Redundancy on Switches Connected by Bridge Links

When running PAgP on switched connected to 1310 series bridges, for ethernet traffic redundancy and load balance be aware that PAgP switchover takes at least 30 seconds, which is too slow to maintain certain traffic (for example, TCP) when switching from from port to the other. There is no workaround for this limitation.

Default IP Address Behavior

When an unconfigured access point/bridge boots, it attempts to obtain an IP address from a DHCP server. If it fails to locate a DHCP server, it continues attempting to request an IP address from the DHCP server. To eliminate this behavior, you must access the access point/bridge through its console port and assign a static IP address.

If you want to reset the access point/bridge to its default settings and a static IP address, use the *write erase* or *erase /all nvram* command. If you want to erase everything including the static IP address, in addition to the above commands, use the *erase* and *erase boot static-ipaddr static-ipmask* command.

Caution You should never delete any of the system files prior to resetting defaults or reloading software.

Ethernet Duplex Settings

The access point/bridge is implemented with an unmanaged and unconfigurable 10/100baseT switch embedded in the power injector. All ports on the switch are set for auto-speed, auto-duplex, and auto-MDIX. Port 0 on the switch is used for the coaxial link to the access point/bridge. Port 1 on the switch is used for the RJ45 jack on the power injector.

The speed and duplex settings on the access point/bridge FastEthernet0 interface apply only to the link between the access point/bridge port and port 0 on the power injector. They are entirely independent of the speed and duplex settings used on the RJ45 port (port 1) on the power injector. Therefore, for best performance, you should not change the port 0 default settings. The default settings result in a 100Mbps, full-duplex configuration used on the link between the access point/bridge and the power injector switch.

The connecting port (the port on the device connected to the power injector's RJ45) must be set to half duplex or (preferably) auto duplex. If it is set to auto-duplex, the power injector switch port should negotiate full duplex. If it is set to half duplex, the power injector switch port falls back to half-duplex. The connecting port must not be configured to full duplex. If it is, the power injector switch port fails to negotiate full-duplex, falls back to half duplex, which causes a duplex mismatch.

The following guidelines for setting Ethernet speed and duplex should always be observed:

- The internal FastEthernet0 interface should always be set for speed auto and duplex auto regardless of the settings of the device to which the external LAN port on the power injector is connected (the connecting port).
- The connecting port should always be set for one of the following:
  - 100 Mbps, auto duplex (recommended)
  - 100 Mbps, half duplex
  - 10 Mbps, auto duplex
  - 10 Mbps, half duplex

Note Setting the port to 10 Mbps will most likely degrade throughput.

- The connecting port should never be set to full duplex.

Failure to follow these guidelines will result in lost data due to late collisions, CRC errors, etc.

Caveats

This section lists open caveats in Cisco IOS Release 12.3(2)JA for the 1310 access point/bridge.

Open Caveats

These caveats are open in Cisco IOS Release 12.3(2)JA for the 1310 access point/bridge:

- CSCeb52431—When logging into a TACACS+ server, 1100 series access points sometimes send hundreds of additional authentication requests to the server after a successful authentication.
- CSCed50298—Inconsistent association table before and after changing modes from non-root bridge to workgroup bridge.

- CSCee90230—When the access point is configured for TACACS+ administrator authentication, this traceback occurs sometimes when the access point reboots:

  ```
  Traceback= 2C120 2C150 2EFC4 2BE34 2BD50 330724 3EBD44 19C888 19E5B0 2A3FC0 3AAA04
  1337F8
  ```

  This occurs if the access point has a DHCP IP address. It does not occur when the access point has a static IP address.

- CSCef11167—When polling cDot11ActiveWireless Clients via SNMP, the response may have a value of 4294967292. This occurs in the CiscoWorks Wireless Solution Engine (WLSE) as AP in Overloaded state.

  There is no workaround for this caveat.

- CSCef67806—When you enter the show cdp traffic command on a repeater access point or the parent to which the repeater is associated, the access point reports an inaccurate total of CDP packets.

- CSCef65076—The access point GUI sometimes reports this error when you add a RADIUS server hostname to the access point:

  ```
  HTTP 400 - Bad Request
  ```

  Workaround: Enter the server IP address instead of the hostname.

- CSCef71825—When a memory allocation failure occurs on the access point, it sometimes fails to respond to authentication requests from client devices running Microsoft Windows CE. The access point again responds to client requests after you reboot it.

- CSCef45010—1310 access point/bridge GUI performs poorly when half duplex and a specified speed are part of its configuration.

  If you hardcode the duplex and speed into a configuration for the fast Ethernet interface, the GUI becomes extremely slow. You may also experience a high number of input errors when you try to use the GUI. Telnet or console traffic is not affected.

  Workaround: Set the 1310 Ethernet port settings to Auto Speed and Auto Negotiation.

- CSCef75032—When you disable the 802.11g radio on the access point GUI, the radio is disabled but the Settings page and the Network Interfaces page sometimes indicate that the radio is still enabled.

- CSCef66724—Access point/bridge loses packets due to encryption errors with WPAv2/PSK and concatenation enabled.

  When a 1310 device is configured for WPAv2/PSK and concatenation is enabled, the statistics page shows all Rx packets to have WEP errors even though no packet concatenations are occurring due to low traffic volume. No WEP, MIC, or replay errors occur if concatenation is disabled.

- CSCef87205—There are problems with the following SNMP MIB object identifiers in the CISCO-DOT11-SSID-SECURITY-MIB:
  - cdot11SecAuxSsidVlanName is not writable unless the value corresponds to the same VLAN as the cdot11SecAuxSsidVlan already set for the SSID. The same cdot11SecAuxSsidVlanName and cdot11SecAuxSsidVlan must correspond to an existing entry in the cdot11SecVlanNameTable.
  - cdot11SecSsidInformationElement value cannot be modified after it has been set.
  - cdot11SecSsidRedirectFilter allows you to set an ACL number that is outside the valid range.
  - cdot11SecAuxSsidWirelessNetId allows you to set a value only from 0 to 4095.

- Setting cdot11SecAuxSsidAuthKeyMgmtOpt value to true without also configuring key management creates an invalid configuration.
- You can set cdot11SecAuxSsidLoginUsername without configuring the required corresponding authentication type for the SSID.
- cdot11SecAuxSsidInfraStruct is not of the TruthValue type as described in some object descriptions, and only infraStructure(1) and nonInfraStructure(2) are supported.
- The default address for cdot11SecSsidRedirectDestAddr should be 0.0.0.0 but is " ".
- cdot11SecAuxSsid does not allow you to enter non-hexadecimal characters such as + or /.
- cdot11SecAuxSsidWpaPsk is implemented with a maximum length of 32 characters instead of the 128 characters indicated in the MIB.
- cdot11SecVlanName does not allow you to enter a number greater than 4095 as the VLAN name. It only allows alphabetic characters to be used as VLAN names.
- You cannot use this MIB to configure shared and network-EAP authentication.

Workaround: Use the OIDs in the CISCO-DOT11-IF-MIB.

Resolved Caveats

- CSCec25430—Access points no longer reload when they receive a corrupt CDP packet.
- CSCec74066—The access point GUI now includes a **Restart** button to reset a standby access point that has taken the place of the monitored unit. When the monitored access point comes back online, browse to the Services: Hot Standby page on the standby access point and click **Restart** to put the standby unit back into standby mode.
- CSCed03154—The access point no longer indicates that a client device is associated when the client is not associated.
- CSCed46039, CSCeg18102—Clear Channel Assessment (CCA) value no longer reverts to 0 after bridge reboots.
- CSCed62173—The access point now sends the list of adjacent access points to qualified client devices when they associate to the access point and when the list of adjacent access points is updated.
- CSCed63953—The access point information element now transmits the value that you enter for default QoS CWMin value for best effort regardless of the value that you enter for that setting.
- CSCed66444, CSCef40123—TKIP Michael MIC failure no longer occurs in non-root bridge packets when the non-root bridge is associated to a root bridge with WPA-PSK configured.
- CSCed68575—SNMP process no longer triggers a reload.
- CSCed75292—The access point radio no longer reboots when a client device attempts to authenticate at the same time that you enter this command on the access point CLI:

  ```
  show aaa user all
  ```

- CSCed84527—The access point no longer deauthenticates roaming client devices when the 1 and 2 Mbps datarates are disabled on the access point.

- CSCed78149—A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages 2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks 3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its postings can be found at the website of Centre for the Protection of National Infrastructure.
- CSCed84862—MAC authentication server is now configured via WDS when local MAC is configured.
- CSCed86456—TKIP/WPA has replay detection for links with concatenation enabled.
- CSCed87329—Access points now use only one DHCP client identifier when they boot.
- CSCed91130—When an 802.11g radio in an access point configured for use in Japan is set to channel 14, you can no longer select **Best Throughput** for the data rate setting on the access point GUI.
- CSCed92054—The access point now uses the same MAC address format for both authentication and accounting when sending MAC addresses to the RADIUS server.
- CSCed21433—Entry fields on the access point GUI now accept all characters except the following:

  "
  ]
  +
  /
  Tab
  Trailing space
- CSCee09515—The Associations page on the access point GUI now includes all associated client devices in its count of associated clients.
- CSCee09624—The transmitted fragment counter on the access point now counts all transmitted fragments.
- CSCee12053—Access points do not support the **service compress-config** command, and the command has no effect on access points when you enter it.
- CSCee14096—If the access point is not configured as a local authenticator, the access point no longer reboots when you enter the **clear radius local-server user** *user* command.

- CSCee14599—Access points in standby mode no longer allow client associations when the Ethernet port is disabled.
- CSCee18627—Access point no longer reboots when **clear radius local-server user** command is issued.
- CSCee20478—Console no longer freezes when changing between static IP and DHCP.
- CSCee24611—After several days of connectivity, access points no longer fail to communicate with workgroup bridges that are LEAP authenticated.
- CSCee26301—SSH now operates correctly when you change the access point host name.
- CSCee29096—Access point error messages now comply with ISO standards.
- CSCee29948—The access point now correctly assigns the **ntp broadcast client** command to the bvi1 interface.
- CSCee30632—Access points now support SNTP.
- CSCee30896—Access points configured as local authenticators no longer unnecessarily authenticate clients twice.
- CSCee32246—The **rts retries** command now works as expected.
- CSCee35686—When you set an 802.11g-only data rate to **required** on the access point 802.11g radio, the access point GUI now displays a reminder that the setting prevents associations from 802.11b client radios.
- CSCee34600—BR1310 WMIC now sends a blank SSID when guest mode is disabled for all SSIDs.
- CSCee38517—The access point now sends an EAP-FAILURE message to a client device that fails authentication when the ACS server sends an ACCESS-REJECT message.
- CSCee39180—The default link to online help files is now automatically updated when you upgrade the access point software.
- CSCee39809—Access points configured for LEAP no longer randomly reboot.
- CSCee44666—Software upgrade no longer disables TACACS+.
- CSCee45192—You can now enable both debugging notifications and Syslog messages on the access point GUI.
- CSCee50581—SSIDs that contain spaces are no longer truncated in the Adjacent Nodes list on the Network Map page on the access point GUI.
- CSCee51677—When you configure a time zone on the access point GUI, the access point configuration viewed on the CLI matches the GUI setting.
- CSCee56830—The hot standby access point no longer shuts down the radio of the primary access point when the standby access point radio is disabled.
- CSCee61010—The access point now requires 63 hexadecimal characters for the WPA pre-shared key.
- CSCee62546—The access point GUI now warns users that Aironet extensions must be enabled when you configure MIC or per-packet keying on the access point.
- CSCee63875—The createAndWait option in the CISCO-FLASH-MIB now operates correctly on access points.
- CSCee64873—The password hash function of WLCCP no longer changes the resulting hash with every execution.

- CSCee66841—When VLANs are enabled and WEP encryption is added to the infrastructure SSID, an access point in fallback repeater mode can now associate to a root access point and successfully pass traffic.
- CSCee70832—When the primary ACS server fails, the access point now switches to the next ACS server in the access point's server priority list.
- CSCee17177—Memory allocation failures with multiple tracebacks observed

  This caveat is not a defect and has been closed.
- CSCee77277—Access points now correctly send these RADIUS accounting attributes: Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets.
- CSCee78082—Throughput is now the same for unicast and multicast packets sent by the access point.
- CSCee78757—Non-Cisco client adapters now are able to associate to the 802.11g radio in an access point when OFDM data rates (6, 9, 12, 18, 24, 36, 48, and 54 Mbps) are enabled.
- CSCee87254—You can now use the access point GUI to disable SSH.
- CSCee90065—An access point with a default configuration no longer sends a DHCP request when you click the **Network Interfaces: IP Address** link on the access point GUI.
- CSCef01790—When access point interfaces are configured to allow unicast-flooding and the configuration is saved, the unicast-flooding command is now applied after the unit reboots.
- CSCef02795—Access point no longer allows simultaneous MAC-address authentication and WPA-PSK configurations.
- CSCef06846—The access point no longer has a memory leak.
- CSCef06976—Applying a service policy to input traffic on the access point radio interface to classify traffic now carries through to the 802.1d marking on the Ethernet trunk.
- CSCef14899—The drop-down menu on online help pages now operates correctly.
- CSCef23452—The access point data packet counter now increments correctly.
- CSCef24269—The Time Server entry field now allows more than 15 characters on the Services: NTP page on the access point GUI.
- CSCef41592—After booting from factory defaults, an access point now automatically sets its hostname to the name returned in the DNS PTR record corresponding to any of the access point's IP addresses.
- CSCef45558—BR1310 now loads default radio interface settings when configuring AP only mode.
- CSCef46191—A specifically crafted TCP connection to a telnet or reverse telnet port of an access point running Cisco IOS software no longer blocks further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and HTTP access to the access point.
- CSCef49603—The Cisco IOS Software Configuration Guide for Cisco Aironet Access Points now contains a description for the RADSRV-4-NAS_UNKNOWN error message.
- CSCef53367—Access points no longer display runtime errors when you browse to the Express Setup page on the GUI.
- CSCef53401—Client devices associated to an access point no longer fail to receive IP addresses from the DHCP server.
- CSCef55725—Transmit power no longer drops on channel 14 on access points configured for use in Japan.

- CSCef59317—When a failed authentication holdoff time is configured on the access point, the access point now allows three authentication failures before it invokes the holdoff time for the failed user.
- CSCef62817—User passwords configured on a local authenticator access point now appear as either clear text or nthash.
- CSCef66214—Uninitialized message structures no longer cause the access point to reboot.
- CSCef71351—The radio output drop counter no longer increments when the access point sends a CDP packet.
- CSCef72922—Client is now able to pass data to an access point configured to use WPA or CCKM with TIKP.
- CSCef83419—Dot11 association MIB client table now returns all direct clients.
- CSCef88753—Access point/bridge no longer experiences intermittent connectivity.
- CSC in64553—TACACS+ authentication no longer fails when DHCP is selected.
- CSCin72424, CSCin71087—350 bridge now associates to a remote bridge in WPA Migration Mode.
- CSCin74956—Client devices that associate to the access point using an SSID with CKIP+CMIC encryption now receive IP addresses from the DHCP server.
- CSCsa32966—Access points no longer send randomly corrupted beacons that cause them to appear as rogue devices on the WLSE.

If You Need More Information

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

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

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

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at http://www.cisco.com/cisco/web/support/index.html. Click **Technology Support**, choose **Wireless** from the menu on the left, and click **Wireless LAN**.

Documentation Updates

The *Cisco Aironet 1300 Series Wireless Bridge Mounting Instructions* provides detailed instructions for installing and mounting the 1310 access point/bridge.

Related Documentation

This section lists documents related to Cisco IOS Release 12.3(2)JA and to 1310 access point/bridge.

Platform-Specific Documents

These documents describe installation and configuration of the 1300 series:

- *Quick Start Guide: Cisco Aironet 1300 Series Wireless Bridge*
- *Cisco Aironet 1300 Series Wireless Bridge Hardware Installation Guide*
- *Cisco Aironet 1300 Series Bridge Mounting Instructions*
- *Cisco Aironet 14-dBi Vertically Polarized Sector Antenna (AIR-ANT2414S-R)*

Cisco IOS Software Documentation Set

You can find the most current Cisco IOS documentation on Cisco.com. Follow this link path to find the documentation for Cisco IOS Release 12.3:

Technical Documents > Documentation Home Page > Cisco IOS Software Configuration > Cisco IOS Release 12.3

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.