



# Release Notes for Cisco Aironet 1310 Outdoor Access Point/Bridge for Cisco IOS Release 12.3(2)JA6

---

**April 3, 2006**

These release notes describe caveats for Cisco IOS Release 12.3(2)JA6. They also provide important information about the Cisco Aironet 1310 Outdoor Access Point/Bridge (hereafter called the *access point/bridge*).

## Contents

These release notes contain the following sections.

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 3](#)
- [Installation Notes, page 5](#)
- [Important Notes, page 8](#)
- [Caveats, page 13](#)
- [Troubleshooting, page 17](#)
- [Documentation Updates, page 17](#)
- [Related Documentation, page 18](#)
- [Obtaining Documentation and Submitting a Service Request, page 18](#)



---

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

© 2006 Cisco Systems, Inc. All rights reserved.

# 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 access point/bridge provides deployment personnel with a flexible, easy to use solution that meets the security requirements of wide area networking professionals.

The 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 unified wireless network solution. Based on Cisco IOS, the 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)JA6 on any 1310 outdoor access point/bridge.

## Finding the IOS Software Version

To determine the version of IOS running on your 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 access point/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 access point software for your access point:

- 
- Step 1** Follow this link to the Cisco home page:  
<http://www.cisco.com>
  - Step 2** Click **Technical Support and Documentation**. The Technical Support and Documentation page appears.
  - Step 3** Click **Wireless**. The Wireless Support Resources page appears.
  - Step 4** Scroll down to the Wireless LAN Access section.
  - Step 5** Click **Cisco Aironet 1300 Series**. The Cisco Aironet 1300 Series Introduction page appears.
  - Step 6** Under the Configure section, click **Configuration Guides**. A list of configuration documents appears.

- Step 7** Click **Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.3(15)JA**.
- Step 8** Navigate to the Managing Firmware and Software chapter.

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>

## New Features

This release does not contain new features. It supports the features introduced in Cisco IOS Release 12.3(2)JA. 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 access point features as Cisco Aironet 1100 Series Access Points in Cisco IOS Software Release 12.2(13)JA and earlier Cisco IOS 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 wireless bridge features as the Cisco Aironet 1400 Series Wireless Bridge in Cisco IOS Release 12.2(13)JA and earlier Cisco IOS 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 (WMM) 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 RADIUS server to assign a client to a VLAN identified by its VLAN name. In releases before 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 feature 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 Release 12.2(13)JA or earlier that are not supported by the 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 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 equipment. 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 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 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)JA5.

### WPA/2 With Concatenation Not Supported

Cisco IOS Release 12.3(2)JA5 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](http://www.cisco.com/en/US/products/hw/wireless/ps4570/tsd_products_support_configure.html)

**Figure 1 Express Security Page**

Hostname ap ap uptime is 1 minute

**Express Security Set-Up**

**SSID Configuration**

1. SSID  ☒ Broadcast SSID in Beacon

2. VLAN

☒ No VLAN ☐ Enable VLAN ID:  (1-4095) ☐ Native VLAN

3. Security

☒ No Security

☐ Static WEP Key

Key 1  128 bit

☐ EAP Authentication

RADIUS Server:  (Hostname or IP Address)

RADIUS Server Secret:

☐ WPA

RADIUS Server:  (Hostname or IP Address)

RADIUS Server Secret:

**SSID Table**

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input checked="" type="radio"/>	tsunami	none	none	open	none		✓

## 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.

## Access Point/Bridge Does Not Support Loopback Interface

When configuring the 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 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 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 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 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 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 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 access point/bridge accepts any IP address. If you enter 0.0.0.0, the 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](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 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 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 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 100 Mbps, 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 for Cisco IOS Release 12.3(2)JA and resolved caveats in Cisco IOS Releases 12.3(2)JA, 12.3(2)2JA5, and 12.3(2)JA6 for the access point/bridge.

## Open Caveats

These caveats are open in Cisco IOS Release 12.3(2)JA for the 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.

- CSCee87287—Access points sometimes fail to generate accounting records when a wireless client is re-authenticated on an automatic interval (for example, when the access point is configured using the **dot1x reauthentication seconds** command).
- 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.

- CSCef45010—The 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.

- 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.

- CSCsa40042, CSCsa40045—The user interfaces on the access point/bridge allow you to configure the bridge to fall back to repeater mode if the Ethernet link fails. However, repeater mode is not supported on the access point/bridge.

## Resolved Caveats in Cisco IOS Release 12.3(2)JA6

- CSCsc64976

A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at the following URL:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051201-http>

- CSCee45312

RADIUS authentication on a device that is running certain versions of Cisco IOS and configured with a fallback method to none can be bypassed.

Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

More details can be found in the security advisory which posted at the following URL:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050629-aaa>

## Resolved Caveats in Cisco IOS Release 12.3(2)JA5

The following caveat is resolved in Cisco IOS Release 12.3(2)JA5:

- CSCei61732

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051102-timers>.

- CSCei76358—Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability.

## Resolved Caveats in Cisco IOS Release 12.3(2)JA

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

- CSCee51985—Access points now correctly apply QoS priorities to DSCP-tagged packets.
- CSCee90230—When the access point is configured for TACACS+ administrator authentication and uses an IP address from the DHCP server, tracebacks no longer occur when the access point reboots.
- CSCef60659, CSCsa59600—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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050412-icmp>.

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 posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef66724—The access point/bridge no longer loses packets due to encryption errors with WPAv2/PSK and concatenation enabled.
- CSCef70234—When the access point is configured to select the least-congested channel at start-up, the access point now selects the least-congested channel.
- CSCef71351—When CDP is enabled on a radio interface with VLANs configured, the radio output drop counter no longer incorrectly increments when the access point sends a CDP packet.
- CSCef75475—When an access point reboots and reloads, the reason for the reboot is now included in the output for the **show version** command and stack information is included in the output for the **show stack** command.
- CSCef87205—Problems with the following SNMP MIB object identifiers in the CISCO-DOT11-SSID-SECURITY-MIB have been resolved:
  - cdot11SecAuxSsidVlanName
  - cdot11SecSsidInformationElement
  - cdot11SecSsidRedirectFilter
  - cdot11SecAuxSsidWirelessNetId
  - cdot11SecAuxSsidAuthKeyMgmtOpt
  - cdot11SecAuxSsidLoginUsername
  - cdot11SecAuxSsidInfraStruct
  - cdot11SecSsidRedirectDestAddr
  - cdot11SecAuxSsid
  - cdot11SecAuxSsidWpaPsk
  - cdot11SecVlanName
- CSCef90780—Access points now correctly retrieve a configuration file using TFTP even when the initial response from the DHCP server is delayed.
- CSCef95164—ARP caching no longer disrupts transmission of UDP packets.
- CSCef95472—Symbol client devices no longer have difficulty communicating with the 802.11b radio in an access point after being associated for a period of several weeks.
- CSCeg12593—Bridges now pass VTP traffic correctly when the native VLAN is not VLAN1.
- CSCeg15035—The transmit queue is no longer disrupted when you configure the **drop packet** option in the **packet retries** command.
- CSCeg20875—802.11g radios no longer transmit a CCK header that is 2 microseconds too long.
- CSCeg28056—The Filters Classes field on the IP Filters page in the access point GUI no longer truncates filter information.
- CSCeg29580—The access point now correctly forwards IPv6 Router Advertisements from the LAN to associated clients.
- CSCeg30167—The access point LEDs that indicate Ethernet and radio traffic now operate correctly.



- CSCeg34694—The access point now accepts TACACS+ commands while using TFTP to download a configuration file.
- CSCeg36184—Error messages no longer appear on the bridge when client devices authenticate to a local RADIUS server using WPA and LEAP.
- CSCeg46554—Enabling the QBSS element on the access point no longer blocks calls from Cisco 7920 IP phones.
- CSCeg51737—Access points now include I/O memory information in core dumps to an FTP server.
- CSCin46434—The access point now correctly prompts for the password when configured for TACACS+ authentication.
- CSCin82864—The MIB object *ciscoFlashCopyTable* now returns a correct response.
- CSCsa39460—When a 1310 series access point in workgroup bridge mode roams from one access point to another, the client devices connected to the workgroup bridge no longer lose their network connection. Aironet 350 series bridges have a similar defect, described in CSCeg22389.
- CSCsa42723, CSCuk25470—Access points no longer reboot when receiving SNMP traps.
- CSCsa43898—1310 series access points in workgroup bridge mode now correctly perform LEAP authentication when LEAP is not the first protocol offered by the authentication server.
- CSCsa44872—Access points now correctly forward multicast and broadcast messages from the LAN interface to radio interfaces.
- CSCsa45409—Access points no longer fail to boot when the file *flash:env\_vars* is missing.
- CSCsa45470—The **boot system flash:** command no longer generates an unexpected exception error.

## 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 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/en/US/support/index.html>. Click **Tools and Resources**, and choose the resource that best suits your troubleshooting needs.

## Documentation Updates

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

## Related Documentation

This section lists documents related to Cisco IOS Release 12.3(2)JA6 and to access point/bridges.

## 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 Outdoor Access Point Software Configuration Guide*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *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 all Cisco IOS Releases for the outdoor access point/bridge, including Release 12.3(2)JA:

**Technical Support and Documentation > Documentation > Wireless > Cisco Aironet 1300 Series.**

## 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.

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned 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. (1110R)