Release Notes for Cisco Aironet 1310 Outdoor Access Point/Bridge for Cisco IOS Release 12.2(15)JA

April 29, 2004

These release notes describe open caveats for Cisco IOS Release 12.2(15)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.

- Introduction, page 2
- System Requirements, page 2
- New Features, page 3
- Installation Notes, page 4
- Important Notes, page 7
- Caveats, page 12
- Troubleshooting, page 13
- Documentation Updates, page 13
- Related Documentation, page 13
- Obtaining Documentation and Submitting a Service Request, page 14

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 a wireless bridge, access point, 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 Layer 2 Roaming, QoS, and VLANs.

System Requirements

Cisco IOS Release 12.2(15)JA is factory installed on your 1310 access point/bridge. As new Cisco IOS releases become available for the access point/bridge, you should consider upgrading.

Determining the 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:

```
bridge> 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.

Upgrading to a New Software Release

For instructions on installing 1300 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 12.2(15)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:

- IEEE 802.11d World Mode Support
- Cisco Compatible Extensions information element
- IEEE 802.1X Support for EAP-FAST
- Wi-Fi Protected Access (WPA)
- Fast secure roaming non-root wireless bridge
- Workgroup bridge (WGB) mode

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

IEEE 802.11d World Mode Support

The 802.11d standard for world mode is supported by Cisco Aironet access points and bridges in this release. World mode enables the 1310 access point/bridge to inform an 802.11d client device which radio setting the device should use to conform to local regulations.

Cisco Compatible Extensions Information Element

This information element allows a Cisco Aironet access point to inform Cisco Compatible Extensions client devices about the Cisco Compatible release version that it supports.

IEEE 802.1X Support for EAP-FAST

This Cisco Wireless Security Suite feature supports the IEEE 802.1X standard port-based authentication Extensible Authentication Protocol (EAP) type EAP-Flexible Authentication through Secure Tunneling (EAP-FAST). EAP-FAST can also be supported by access points running Cisco IOS Release 12.2(11)JA or later.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is now supported on Cisco Aironet access points and wireless bridges. WPA is the Wi-Fi Alliance specification for interoperable wireless LAN security. It supports IEEE 802.1X authentication using extensible authentication protocol (EAP) authentication types and Temporal Key Integrity Protocol (TKIP) encryption.

Fast Secure Roaming Non-root Wireless Bridge

This feature offers fast secure Layer 2 roaming for a non-root wireless bridge or workgroup bridge to the wired infrastructure using a wireless root bridge or an access point.

Workgroup Bridge (WGB) Mode

This feature allows a Cisco Aironet series bridge or access point to be configured to operate as a workgroup bridge (WGB) client.

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
- Wireless Domain Services (WDS)
- IEEE 802.1X local authentication services
- IEEE 802.11a support

Note LACP is not supported in a BR1310 because the device cannot forward LACP frames.

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.

1300 Series 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 1300 series 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.

New Express Security Page Simplifies Security Setup

The new Express Security page in the 1300 series web-browser interface makes it easier to create SSIDs and assign security settings to them. Figure 1 shows the Express Security page.

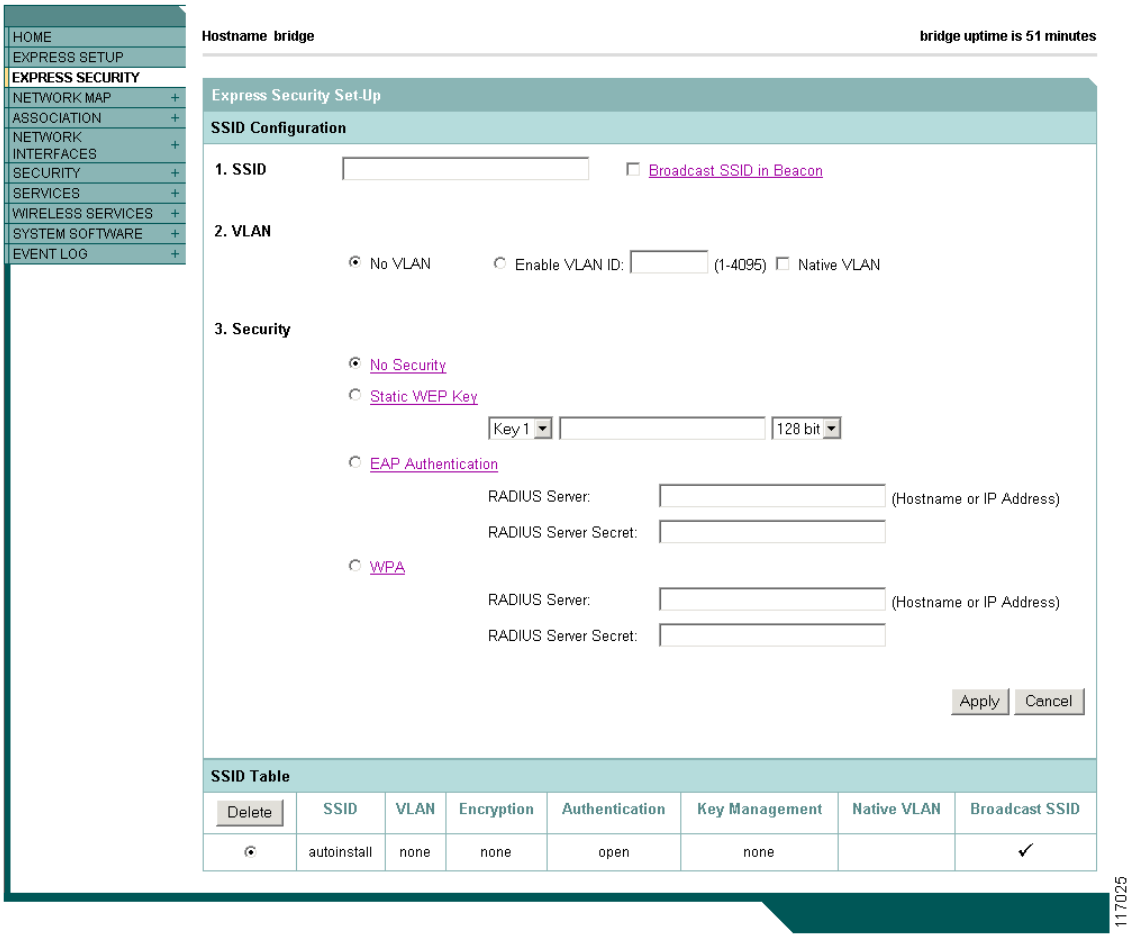
Limitations of the Express Security page include:

- 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 Chapter 2, "Configuring Basic Security Settings," in the *Cisco Aironet 1300 Series Wireless Bridge Software Configuration Guide.*

Figure 1 Express Security Page



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.

Repeater Access Points Running IOS Software Cannot Associate to Parent Access Points Not Running IOS Software

Repeater access points running Cisco IOS software cannot associate to parent access points that do not run IOS software (all 340 series access points, and 350 and 1200 series access points that have not been converted to IOS software).

Repeater Access Points Cannot Be Configured as WDS Access Points

Repeater access points do not support WDS. You cannot configure a repeater access point as a WDS access point, and if a root access point becomes a repeater in fallback mode, it cannot provide WDS.

Cannot Perform Link Tests on Non-Cisco Aironet Client Devices and on Cisco Aironet 802.11g Client Devices

The link test feature on the web-browser interface does not support non-Cisco Aironet client devices nor Cisco Aironet 802.11g client devices.

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 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.

Enabling CKIP When in Bridge Mode

For higher throughput and enhanced security, Cisco recommends enabling CKIP when the 1310 access point/bridge is in the bridge mode.

Cisco CKM Supports Spectralink Phones

Cisco CKM (CCKM) key management is designed to support voice clients that require minimal roaming times. To date, CCKM supports only Spectralink Wireless Phones. Other voice clients have not been tested with CCKM and are not supported.

Non-Cisco Aironet Clients Sometimes Fail 802.1x Authentication

Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the 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**.

Limitation to PAgP Redundancy on Switches Connected by Bridge Links

When running PAgP on swtiched connected to 1310 seriess 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.

Caveats

This section lists open caveats in Cisco IOS Release 12.2(15)JA for the 1310 access point/bridge.

Open Caveats

These caveats are open in Cisco IOS Release 12.2(15)JA for the 1310 access point/bridge:

- CSCee17177—Memory allocation failures with multiple tracebacks observed

  Root bridge experiences multiple memory allocation failures with subsequent tracebacks on three different processes: CDP Protocol, Pool Manager, and “Dot11 aaa process.

- CSCin71087—A 350 series workgroup bridge running LEAP fails to associate in WPA Migration mode.

  Workaround: create a standalone SSID for the workgroup bridge.

- CSCed66444—TKIP Michael MIC failure occurs in non-root bridge packets when the non-root bridge is associated to a root bridge with WPA-PSK configured.
- CSCed94862—Bridge does not forward SSTP message when Spanning Tree Protocol is disabled.
- CSCed86456—TKIP/WPA has no replay detection for links with concatenation enabled.

  Workaround: Use CKIP (Cisco’s proprietary TKIP) when using concatenation. This mode offers the best combination of security and throughput performance for bridges. If TKIP must be used, disable concatenation, but with reduced throughput performance.

- CSCee18627—If the access point/bridge is not configured as a local authenticator, the access point/bridge reboots when you enter the **clear radius local-server user** *user* command.
- CSCed59485—SSH is still enabled after user disables it and reboots.

  Workaround: disable SSH from the CLI by issuing the following commands:

  - **crypto key zerosize rsa** (answer **yes** to remove all rsa keys).
  - **no ip domain-name (***domain-name)*

- CSC in64553—Tracebacks received and TACACS+ authentication fails when DHCP is selected.

  Workaround: Assign a static IP address instead of DHCP when using TACACS+.

- CSCed50298—Inconsistent association table before and after changing modes from non-root bridge to workgroup bridge.
- CSCin72424—350 bridge fails to associate to a remote bridge in WPA Migration Mode.
- CSCed84862—Failure to configure MAC authentication server via WDS when local MAC is configured.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.2(15)JA for the 1310 access point/bridge:

- CSCec16481

  A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

  The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.

  Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040818-ospf.html.

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**, select **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 1300 series.

Related Documentation

This section lists documents related to Cisco IOS Release 12.2(15)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 12.2:

Technical Documents > Documentation Home Page > Cisco IOS Software Configuration > Cisco IOS Release 12.2

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.