# Release Notes for Cisco Aironet 1410 Bridges for Cisco IOS Release 12.2(13)JA4

**April 19, 2004**

These release notes describe caveats for Cisco IOS Release 12.2(13)JA4. They also provide important information about the Cisco Aironet 1410 Bridge (hereafter called *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 1400 Series Bridge is a wireless device designed for building-to-building wireless connectivity. Operating in the 5.8-GHz UNII 3 band (5725 to 5825 MHz), derived from the 802.11a standard, the bridge delivers 6 to 54 Mbps data rates without the need for a license. The bridge is a self-contained unit designed for outdoor installations, providing differing antenna gains as well as coverage patterns and supports both point-to-point and point-to-multipoint configurations.

The bridge uses a browser-based management system, but you can also configure the bridge using the command-line interface (CLI) through a Telnet session, Cisco IOS commands, or Simple Network Management Protocol (SNMP).

# System Requirements

You should install Cisco IOS Release 12.2(13)JA4 on your bridge to incorporate the fixes identified in the Resolved Caveats section.

## Finding the Software Version

To find the version of Cisco IOS software running on your bridge, use a Telnet session to log into the bridge and enter the **show version** EXEC command. This example shows command output from a bridge running Cisco IOS Release 12.2(11)JA:

```
bridge> show version
Cisco Internetwork Operating System Software
IOS (tm) C1410 Software (C1410-K9W7-M), Version 12.2(11)JA
Copyright (c) 1986-2003 by Cisco Systems, Inc.
```

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

## Upgrading to a New Software Release

For instructions on installing bridge software:

1. Click this link to go to the Product/Technology Support page:

   http://www.cisco.com/cisco/web/psa/default.html

   Choose **Wireless > Outdoor Wireless > Cisco Aironet 1400 Series**, scroll down and click **Configure Guides**.

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

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

   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.

# Installation Notes

This section contains important information to keep in mind when installing your bridge.

## Bridge Installation

The bridge is available in two configurations:

- Integrated antenna bridge (with 22.5-dBi directional antenna)
- External antenna bridge (with antenna connector for use with an external antenna)

**Note** To meet regulatory restrictions, the external antenna bridge 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 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.

## Stacking Bridges

You can double the throughput or create a standby link by stacking two bridges. A stacked installation consists of two bridge systems installed at the same physical location. For detailed mounting instructions refer to the *Cisco Aironet 1400 Series Wireless Bridge Mounting Instructions* that shipped with your bridge.

**Note** The bridge antennas must be separated by a minimum of 6.56 ft (2 m) from each other and from other co-located antennas.

# Important Notes

This section describes important information about the bridge.

## Default SSID and Distance Settings Change When You Change Role in Radio Network

If the bridge's SSID has not been changed from the default setting and you select **Install Automatic Mode** as the bridge's role in radio network setting, the SSID automatically changes from *tsunami* to *autoinstall*. When you change the role in radio network from Install Automatic Mode to Root or Non-Root, the SSID changes automatically from *autoinstall* back to *tsunami*. However, if you change the SSID from its default setting, changing the role in radio network setting does not change the SSID.

In Install Automatic Mode, the default distance setting is 99 km. When you change the role in radio network from Install Automatic Mode to Root or Non-Root, the distance setting changes automatically from 99 km to 0 km.

## Cisco Aironet Software Requires Completion of Encryption Authorization Form

To access Cisco Aironet software from the Software Center on Cisco.com, you must now fill out a form to receive authorization to download encrypted software. Registered Cisco.com users are required to fill out the form only once, but public users must do so once each session, each time software is downloaded. A form is automatically created for public users. The form for Registered Cisco.com users is located at the following URL:

https://sso.cisco.com/autho/forms/CDClogin.html

## Default Encryption Key 2 Is Set by Bridge

The encryption key in slot 2 is the transmit key by default. If you enable WEP with MIC, use the same WEP key as the transmit key in the same key slot on both root and non-root bridges.

## Limitation to PAgP Redundancy on Switches Connected by Bridge Links

When two switches configured for Port Aggregation Protocol (PAgP) are connected by redundant wireless bridge links, the PAgP switchover takes at least 30 seconds, which is too slow to maintain TCP sessions from one port to another.

## power client n CLI Command Is Not Supported

The bridge does not support the **power client n** command in the browser or CLI interfaces.

```
bridge(config-if)# power client n
(where n is a value of 12, 15, 18, 21, 22, 23, 24, or maximum)
```

The bridge does not perform any action when you enter this command.

## Default Infrastructure SSID

When VLAN is enabled, the WEP encryption mode and the WEP key are applicable only to a native VLAN. Any SSID configured should have the Infrastructure-SSID parameter enabled for that SSID. With the Infrastructure-SSID parameter enabled, the bridge ensures that a non-native VLAN cannot be assigned to that SSID.

## ARP Table Is Corrupted When Multiple BVIs Are Configured

The bridge supports only one bridge virtual interface (BVI). Multiple BVIs should not be configured because the ARP table may become corrupted.

# Bridge Power Up LED Colors

During power up the bridge LEDs display the following color sequences:

1. The Install LED is initially turned off.
2. The Install LED turns amber.
3. The Status LED turns amber during the boot loader process.
4. The Ethernet, Status, and Radio LEDs turn green during the loading of the operating system.
5. The Ethernet, Status, and Radio LEDs turn amber during the loop-back test.
6. The Status LED starts to blink green then the Ethernet LED starts to blink green.
7. The Ethernet, Status, and Radio LEDs blink amber twice to indicate that the auto install process has started.
8. During the auto install process, the Ethernet, Status, and Radio LEDs turn off for a short time period then go through a blinking sequence twice. Each LED sequentially blinks at the following rates before becoming continuously amber:
   a. Slow blinking rate of 1 blink per second.
   b. Medium blinking rate of 2 blinks per second.
   c. Fast blinking rate of 4 blinks per second.
9. The Install LED starts to blink amber to indicate that the bridge is searching for a root bridge.
10. When the bridge associates to a root bridge, the Install LED turns amber.
11. When the bridge becomes a root bridge and is waiting for a non-root bridge to associate, the Install LED blinks green.
12. When the root bridge has a non-root bridge associated, the Install LED turns green.

# Bridge Cannot Detect Simultaneous Image Downloads

Do not attempt to load software images into the bridge from both a Telnet session and console session simultaneously. The bridge cannot detect that two images are being loaded at the same time. For best results, use the **archive download** command in the CLI.

# Bridge Cannot Detect Invalid Software When Using copy Command

The bridge sometimes cannot detect invalid software images when you load software using the copy command. For best results, use the **archive download** command in the CLI to load new software.

# Caveats

This section lists open and resolved caveats in Cisco IOS Release 12.2(13)JA4 for the bridge.

## Open Caveats

These caveats are open in Cisco IOS Release 12.2(13)JA4 for the bridge:

- CSCec40452—When you run a link test or install the bridge using the autoinstall mode, the RSSI reading is 4 dB lower than actual at room temperature and 8 dB lower than actual when the outdoor ambient temperature is higher than approximately 45° C. There is no workaround for this issue.
- CSCin57580—MAC address filtering sometimes fails to stop traffic from filtered addresses. There is no workaround for this issue.

## Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.2(13)JA4:

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-ios, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-nonios.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the

sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-ios, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-nonios.

- CSCdz32659—Memory allocation failure (MALLOCFAIL) messages no longer occur for Cisco Discovery Protocol (CDP) processes.
- CSCed40563—Problems with the CDP protocol have been resolved.

These caveats are resolved in Cisco IOS Release 12.2(13)JA, 12.2(13)JA1, and 12.2(13)JA2:

- CSCea28990—The bridge now passes IP traffic when the bridge # route IP command is configured.
- CSCea57649—The CLI **Help** command no longer produces incorrect output for the radio interface.
- CSCea77473—HTTP software upgrade no longer fails with Netscape version 7.x.
- CSCea81730—The web interface for the non-root bridge now correctly displays the root-bridge MAC address on the radio page.
- CSCeb05835— The web interface no longer shows incorrect STP Root information on a bridge setup with multiple VLANs.
- CSCeb12740—The virtual radio connection can now be made after the station role is changed.
- CSCeb15923—Radio firmware recovery now works reliably.
- CSCeb17296—The **clear dot client** command now works with traffic being passed.
- CSCed21588—Bridges no longer disassociate bridges when WEP is enabled.

# 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 1400 Series Wireless Bridge Mounting Instructions* provides detailed instructions for installing and mounting the bridge.

## Stacking Bridges Section Changes

The separation distance between the two stacked bridge antennas is a minimum of 6.56 ft (2 m).

# New Transmit Power Options for Low-Power Bridges

If your bridge is configured at the factory for use in a regulatory domain other than North America or Korea, the transmit power options for the **power local** command differ from the power options listed in the *Cisco Aironet 1400 Series Bridge Software Configuration Guide* and in the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*. The transmit power options for low-power bridges are **16**, **13**, **12**, **10**, **9**, **8**, **7**, and **4** dBm. Note that the maximum transmit power for your bridge depends on your regulatory domain.

# New suspend Option in bridge protocol ieee Command

The **bridge protocol ieee** command, which enables Spanning Tree Protocol (STP) on the bridge, now contains a **suspend** option. This option suspends STP on the bridge until you re-enable it.

# New Event Messages

Table 1 lists new event messages added to the Error and Event Messages appendix in the *Cisco Aironet 1400 Series Bridge Software Configuration Guide*.

***Table 1 New Event Messages***

| Message | Explanation | Recommended Action |
|---|---|---|
| **Software Auto Upgrade Messages** | | |
| AUTO_INSTALL_STATION_ROLE | The radio is operating in automatic installation mode. | Use the station-role command to change the role in radio network setting for the radio. |
| AUTO_INSTALL_STATUS | The radio is operating in automatic installation mode. | Use the station-role command to change the role in radio network setting for the radio. |
| AUTO_INSTALL_IP_ADDRESS_ DHCP:<br>IP address dhcp selected | The radio is operating in automatic installation mode and obtained an IP address from a DHCP server. | Use the station-role command to change the role in radio network setting for the radio. |

# Related Documentation

These documents describe the installation and configuration of the bridge:

- *Quick Start Guide: Cisco Aironet 1400 Series Wireless Bridge*
- *Cisco Aironet 1400 Series Wireless Bridge Software Configuration Guide*
- *Cisco Aironet 1400 Series Wireless Bridge Hardware Installation Guide*
- *Cisco IOS Command Reference for Access Points and Bridges*
- *Cisco Aironet 1400 Series Wireless Bridge Mounting Instructions*
- *Cisco Aironet 1400 Series Wireless Bridge 9-dBi Omnidirectional Antenna*
- *Cisco Aironet 1400 Series Wireless Bridge 10-dBi Sector Antenna*
- *Cisco Aironet 1400 Series Wireless Bridge 28-dBi Dish Antenna*
- *Cisco Aironet 1400 Series Wireless Bridge Roof Mount Assembly Instructions*

# 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:

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.

---

This document is to be used in conjunction with the documents listed in the Related Documentation section.