



# Release Notes for Cisco Aironet 1410 Bridges for Cisco IOS Release 12.2(11)JA3

---

April 15, 2004

These release notes describe caveats for Cisco IOS Release 12.2(11)JA3. They also provide important information about the Cisco Aironet 1410 Bridge (hereafter called *bridge*).

## Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Installation Notes, page 3](#)
- [Important Notes, page 5](#)
- [Caveats, page 7](#)
- [Troubleshooting, page 9](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation and Submitting a Service Request, page 10](#)



---

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

# 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(11)JA3 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)JA2:

```
bridge> show version
Cisco Internetwork Operating System Software
IOS (tm) C1410 Software (C1410-K9W7-M), Version 12.2(11)JA2
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.

## Warnings



**Warning**

**This warning symbol 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 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).**



**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. (240 VAC, 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 conductor. 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 connect or disconnect cables during periods of lightning activity.**



**Warning**

**Do not operate your wireless network device 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.**

---

## Safety Information

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

### FCC Safety Compliance Statement

The FCC, 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.
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.

If an accident should occur with the power lines call for qualified emergency help immediately.

## 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 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** configuration interface command on the web-browser or CLI interfaces. The bridge does not perform any action if you use 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/second.
  - b. Medium blinking rate of 2 blinks/second.
  - c. Fast blinking rate of 4 blinks/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.

## Caveats

This section lists [Open Caveats](#) and [Resolved Caveats](#) in Cisco IOS Release 12.2(11)JA3 for the bridge.

### Open Caveats

These caveats are open in Cisco IOS Release 12.2(11)JA3 for the bridge:

- CSCea28990—Cannot pass IP traffic when the bridge `# route IP` command is configured.  
The **bridge # route ip** command must not be configured for the bridge groups assigned to non-native VLANs because this setting stops IP traffic across the bridge for those non-native VLANs.
- CSCea57649—The CLI **Help** command produces incorrect output for the radio interface.  
When using the CLI **Help** command from the radio interface, the command output is repeated multiple times.  
There is no workaround for this problem.
- CSCea75989—The non-root bridge does not reset the dot11 association counters when it reassociates to the root bridge.  
There is no workaround for this problem.
- CSCea81730—The web interface for the non-root bridge incorrectly displays the root-bridge MAC address on the radio page.  
There is no workaround for this problem.
- CSCeb03832—Bridge does not detect some invalid software images when the copy command is used.  
Workaround: Use the CLI **archive download** command.
- CSCeb04390—Bridge does not detect simultaneous software downloads when the **copy** command is used in different sessions.  
Workaround: Use the CLI **archive download** command.
- CSCeb05054—Multiple non-root bridges do not associate to the root bridge after any configuration changes to the radio interface.  
The root bridge in a point-to-multipoint link does not allow non-root bridges to reassociate after configuration changes are made to the radio interface until the root bridge has rebooted (power turned off and on).  
Workaround: After changing the radio interface configuration on a point-to-multipoint link, you must reboot the root bridge (turn power off and on).
- CSCeb05835— The web interface shows incorrect STP Root information on a bridge setup with multiple VLANs.  
There is no workaround for this problem.
- CSCeb08817—The root bridge cannot ping a non-root bridge after reassociation.  
Workaround: Use the CLI **clear arp-cache** command to clear the root bridge ARP cache.

- CSCeb10911—Linktest reports higher RSSI readings for the remote site.  
There is no workaround for this problem.
- CSCeb12740—The virtual radio connection cannot be made after the station role is changed.  
After you change the station role of two bridges while the link is active, the radios get associated but the virtual radio interfaces do not function.  
Workaround: After changing the station roles, you must restart both root and non-root bridges using the browser interface (**System Software > System Configuration > Restart**) or the CLI **reload** command.
- CSCeb14603—Telnet session locks up under heavy traffic.  
There is no workaround for this problem.
- CSCeb15923—Radio firmware recovery does not work reliably.  
There is no workaround for this problem.
- CSCeb17296—**Clear dot client** command does not work with traffic being passed.  
When traffic is being passed through the bridges at around 30 to 40 percent CPU utilization, the CLI **clear dot client H.H.H** command does not clear the counters on the non-root bridge even though the association did clear.  
There is no workaround for this problem.
- CSCea77473—HTTP software upgrade with Netscape version 7.x intermittently fails.  
When you are upgrading software with Netscape version 7.x, the Web interface cascades through all open Netscape windows. The upgrade intermittently fails or the browser states that the upgrade failed when in fact the upgrade actually worked.  
Workaround: Use Netscape version 4.7 or another browser.

## Resolved Caveats

These caveats are resolved in Cisco IOS release 12.2(11)JA3:

- 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://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, 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://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- 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://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, 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://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

## 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 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 feet (2 meters).

## 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, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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

---

This document is to be used in conjunction with the documents listed in the [Related Documentation](#) section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [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. (1005R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.