Release Notes for Cisco Aironet 1410 Bridges for Cisco IOS Release 12.3(2)JA1

November 15, 2004

These release notes describe new features and open and resolved caveats for Cisco IOS Release 12.3(2)JA1. They also provide important information about the Cisco Aironet 1410 Bridge (hereafter called *bridge*).

Contents

These release notes contain the following sections:

CISCO SYSTEMS

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).

Cisco IOS Release 12.3(2)JA1 supports the features and bug fixes included in release 12.3(2)JA. Release 12.3(2)JA1 also resolves CSCeg27630.

System Requirements

You can install Cisco IOS Release 12.3(2)JA1 on all 1400 series bridges.

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(13)JA2:

```
bridge> show version
Cisco Internetwork Operating System Software
IOS (tm) C1410 Software (C1410-K9W7-M), Version 12.2(13)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.

New Features

Cisco IOS Release 12.3(2)JA1 does not include new features. However, it supports the features included in release 12.3(2)JA. This section lists the new features in Cisco IOS Release 12.3(2)JA.

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.

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.

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.

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.

CLI Command power client n Is Not Supported

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

Default IP Address Behavior

When an unconfigured 1400 series bridge boots, it starts up in the *install* mode as a root bridge. In this mode, the bridge attempts to obtain an IP address from a DHCP server. If no DHCP response is received, the bridge assigns an IP address of 10.0.0.1 to the BVI interface and starts a five minute timer. During this five-minute time window, you can browse to the default IP address and configure a static IP address. If after five minutes, the bridge is not reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from a DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five-minute window for browsing to the bridge at 10.0.0.1, you can power-cycle the bridge to repeat the process.

If have configured a static IP address and want to reset the bridge to its default settings but retain the 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 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 bridge FastEthernet0 interface apply only to the link between the bridge port and port 0 on the power injector. They are entirely independent of the speed and duplex settings used on the RJ45 port (port 1) on the power injector. Therefore, for best performance, you should not change the port 0 default settings. The default settings result in a 100Mbps, full-duplex configuration used on the link between the 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.

New Express Security Page Simplifies Security Setup

The new Express Security page in the access point 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 the SSID. However, you can delete the SSID and re-create it.

- 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 the SSID to a VLAN that is already configured on the bridge. To assign the SSID to an existing VLAN, use the Security SSID Manager page.

- You cannot configure combinations of authentication types on the same SSID. To configure combinations of authentication types, use the Security SSID Manager page.

For complete instructions on using the Express Security page, see the *Cisco Aironet 1400 Series Wireless Bridge Software Configuration Guide*.

Figure 1   *Express Security Page*

Telnet Session Sometimes Hangs or Will Not Start During Heavy Traffic

When the bridge is transmitting and receiving heavy traffic, you sometimes cannot start a Telnet session and some existing Telnet sessions freeze or hang. However, this behavior is expected because the bridge gives top priority to data traffic and a lower priority to Telnet traffic.

Caveats

This section lists open and resolved caveats in Cisco IOS Release 12.3(2)JA1 for the bridge.

Open Caveats

These caveats are open in Cisco IOS Release 12.3(2)JA1 for the bridge:

- CSCec78900—High CPU use sometimes slows throughput on bridges.
- CSCef96804—The RSSI DC output port gives an incorrect signal strength indication.

  Workaround: When installing the bridge link, use the bridge LEDs for antenna alignment. If the bridges are already installed, use the **dot11 d0 linktest target** *H.H.H* privileged exec CLI command to start a link test between the root and non-root bridge and display the RSSI measurement.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.3(2)JA1:

- CSCeg27630—A bridge configured at the factory for use in the United States now provides the full range of transmit power allowed in the US regulatory domain.

These caveats are resolved in Cisco IOS Release 12.3(2)JA and in 12.3(2)JA1:

- CSCec25430—Bridges no longer reload when they receive a corrupt CDP packet.
- CSCed46039—After a reboot, the bridge's CCA noise floor setting no longer changes from 62, which is the default setting, to 0.
- CSCed68575—The SNMP process no longer triggers the bridge to reload its image.
- CSCee23653—Administrative packets no longer cause the bridge link to fail.
- CSCee26301—SSH now operates correctly when you change the bridge host name.
- CSCee30632—Bridges now support SNTP.
- CSCee45192—You can now enable both debugging notifications and Syslog messages on the bridge GUI.
- CSCee51677—When you configure a time zone on the bridge GUI, the bridge configuration viewed on the CLI now matches the GUI setting.
- CSCed78149—A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

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

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

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

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

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

This advisory is posted at
http://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.cpni.gov.uk/.

- CSCef46191—A specifically crafted TCP connection to a telnet or reverse telnet port of a bridge Cisco IOS software no longer blocks further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and HTTP access to the bridge.

- CSCef60659—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.cpni.gov.uk/.

- 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.cpni.gov.uk/.

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 ft (2 m).

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.