Release Notes for Cisco Aironet 1410 Wireless Bridges for Cisco IOS Release 12.3(8)JEA

August 31, 2006

These release notes describe minor features and caveats for Cisco IOS Release 12.3(8)JEA. They also provide important information about the Cisco Aironet 1410 Wireless Bridge (hereafter called *bridge*).

Contents

These release notes contain the following sections:

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.

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

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 can install Cisco IOS Release 12.3(8)JEA 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 12.3(7)JA:

```
bridge> show version
Cisco Internetwork Operating System Software
IOS (tm) C1410 Software (C1410-K9W7-M), Version 12.3(7)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 access point software for your access point:

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

No new bridge features are introduced in Cisco IOS Release 12.3(8)JEA.

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 a customer-supplied 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.

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 for the bridge.

Open Caveats

These caveats are open in Cisco IOS Release 12.3(8)JEA:

- CSCed36462—Per-VLAN crypto settings are nonfunctional with wireless bridges.

  On wireless bridges, all VLANs traversing the bridge link must use the same encryption settings. To avoid confusion, do not use the “vlan <vlan-id> keyword on the encryption command as shown in the following example:

```
interface dot11radio0
encryption key 1 size 128bit AAAAABBBBBCCCCCDDDDDEEEEEF transmit-key
encryption mode wep mandatory mic
```

Resolved Caveats

The following caveats are resolved in Cisco IOS Release 12.3(11)JA:

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

  This advisory will be posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080610-snmpv3

- CSCek26492

  Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-ip-option

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-ip-option

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  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-20070124-crafted-tcp

- CSCsa53334

  The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

  - Fragmented IP packets may be used to evade signature inspection.
  - IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

  There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

  This advisory is posted at:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070213-iosips.

- CSCsb04925—Bridge displays junk characters when **show controllers** command is issued.

  When **show controllers dot110** is entered, it displays a serial number with a junk character.

- CSCsc21018—1400 Series bridge shows non-root IP address as 0.0.0.0

  When non-root bridges are configured to use DHCP IP Address, the **show dot11 association** output shows non-root IP address as 0.0.0.0 despite the fact that IP address has been successful allocated and received by the non-root bridge. This does not affect any IP communication of root or non-root bridge at all.

  Workaround: Issuing a **shutdown** and **no shutdown** command on the non-root radio interface will allow non-root to re-associate to the root bridge after it receives the DHCP IP address and communicates the IP address to the root bridge.

  Alternatively, use the **mac-address** command to set the BVI 1 interface mac-address to the same as the non-root radio mac-address will allow root bridge to snoop the DHCP IP address and update the association table automatically. Normally, BVI 1 mac-address is the FastEthernet mac-address of the bridge. All IP traffic uses this BVI mac-address while root bridge keeps track of non-root with the uplink.

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 select 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/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).

Optional Antenna Clarification

The *Quick Start Guide: Cisco Aironet 1400 Series Wireless Bridge* states on page 6 that the external antenna version of the bridge connects to an optional antenna. The statement is incorrect. The external antenna of the bridge has no installed antenna. The customer must purchase the antenna for the this version. There are three antenna options available for the external antenna version and the customer must purchase at least one to make the bridge operational.

A revision to this guide will be released at a future date.

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.