Release Notes for Cisco Aironet 1410 Wireless Bridges for Cisco IOS Release 12.3(11)JA4

July 27, 2007

This release is a maintenance release and contains no new features. These release notes list open and resolved caveats for Cisco IOS Release 12.3(11)JA4. This document also provides 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.

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).

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

System Requirements

You can install Cisco IOS Release 12.3(11)JA4 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(11)JA4:

```
bridge> show version
Cisco Internetwork Operating System Software
IOS (tm) C1410 Software (C1410-K9W7-M), Version 12.3(11)JA4
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.

Obtaining the Software Image

To obtain the Cisco IOS software for your bridge, follow these instructions to reach the Cisco IOS Software Center on Cisco.com:

Step 1 Follow this link to the Cisco wireless document home page:

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

Step 2 Scroll down to the Outdoor Wireless section.

Step 3 Click **Cisco Aironet 1400 Series**. The Cisco Aironet 1400 Series Introduction page appears.

Step 4 Click **Download Software**. The Software Download page appears.

Note You must register or be a registered user to obtain the software image. Follow the registration instructions.

Step 5 Click **Cisco Aironet 1400 Wireless Bridge** and the software release page appears.

Step 6 Click **12.3(11)JA4 > Wireless LAN > Download** and the Software License Agreement page appears.

Step 7 Read the agreement, click **Agree**, and enter your username and password on the Log In screen.

Step 8 Follow the prompts to save the software on your PC.

Upgrading to a New Software Release

For instructions on installing new software for your bridge:

Step 1 Follow this link to the Cisco wireless document home page:

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

Step 2 Scroll down to the Outdoor Wireless section.

Step 3 Click **Cisco Aironet 1400 Series**. The Cisco Aironet 1400 Series Introduction page appears.

Step 4 Under the Configure section, click **Configuration Guides**. A list of configuration documents appears.

Step 5 Click **Cisco IOS Software Configuration Guide for Cisco Aironet 1400 Series Wireless Bridge**.

Step 6 Navigate to the Managing Firmware and Configurations chapter.

New Features

No new features for the bridge are introduced in Cisco IOS Release 12.3(11)JA4.

Caveats

This section lists open and resolved caveats for the bridge.

Open Caveats

These caveats are open in Cisco IOS Release 12.3(11)JA4:

- 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
  ```

- CSCsd91189—Bad cookie is returned from driver resulting in loss of client association.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.3(11)JA4:

- CSCsh58082—When receiving a series of packets destined for port 5060, Cisco devices running an affected version of IOS that supports Session Initiation Protocol (SIP) may be required to reload the device. This issue is compounded by a related bug that allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.
- CSCsi78162—A router that has the SNA Switch feature enabled can generate several messages along with tracebacks.
- CSCsj16292—After an upgrade to 12.2(18)SXF9, the following message is displayed:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error-Traceback=
  ```

- CSCsj18014—The caller ID is received with extra characters.
- CSCsj44081—Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures. This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  Details: The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp: May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error. The error message is then followed by a traceback.
- CSCse56501—A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. 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-20080326-IPv4IPv6

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.)

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.