Release Notes for Cisco Aironet 1300 Series Outdoor Access Point/Bridge for Cisco IOS Release 12.3(4)JA2

April 3, 2006

These release notes describe open and resolved caveats for Cisco IOS Release 12.3(4)JA2 on the Cisco Aironet 1300 Series Outdoor Access Point/Bridge (hereafter called the *access point/bridge*). They also provide important information about the access point/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 1300 Series Outdoor Access Point/Bridge is an 802.11b/g device that provides high speed and cost-effective wireless connectivity between multiple fixed or mobile networks and clients. The flexibility of the device allows it to operate as an access point, wireless bridge, or workgroup bridge. Building a metropolitan area wireless infrastructure with the access point/bridge provides deployment personnel with a flexible, easy to use solution that meets the security requirements of wide area networking professionals.

The access point/bridge supports the 802.11b/g standard, providing 54-Mbps data rates with a proven, secure technology. Cisco makes the maintenance and installation of the access point/bridge easy by integrating it with your wired network using the Cisco unified wirelesss network solution. Based on the Cisco IOS software, the access point/bridge includes advanced features such as Fast Secure Roaming, QoS, and VLANs.

System Requirements

You can install Cisco IOS Release 12.3(4)JA2 on any 1300 series outdoor access point/bridge.

Finding the IOS Software Version

To determine the version of IOS running on your access point/bridge, use a Telnet session to log into the access point/bridge and enter the **show version** EXEC command. This example shows command output from an access point/bridge running Cisco IOS Release 12.2(15)JA:

```
ap> show version
Cisco Internetwork Operating System Software
IOS (tm) C1310 Software (C1310-K9W7-M), Version 12.2(15)JA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
```

You can also find the software version on the System Software Version page in the device's web-browser interface. The software version appears at the top left of most pages in the web-browser interface.

Upgrading to a New Software Release

To install access point software, follow these steps:

Step 1 Follow this link to the Cisco home page:

http://www.cisco.com

Step 2 Click **Technical Support and Documentation**. The Technical Support and Documentation page appears.

Step 3 Click **Documentation**.

Step 4 Click **Wireless**. The Wireless Support Resources page appears.

Step 5 Scroll down to the Wireless LAN Access section.

Step 6 Select the access point model for which you need the information. The Introduction page for the model you selected appears.

Step 7 Under the Configure section, click **Configuration Guides**. A list of configuration documents appears.

Step 8 Click **Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.3(2)JA**.

Step 9 Navigate to the Managing Firmware and Software chapter.

For information on Cisco IOS software, click this link to browse to the Cisco IOS Software Center on Cisco.com:

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

Updates to Existing Features

These existing features are now supported on access points/bridges running Cisco IOS Release 12.3(4)JA:

- IP-Based Wireless Domain Services (WDS)
- Layer 3 Mobility Service via Fast Secure Roaming Tunnels
- Access point/bridge as a repeater access point
- Access point/bridge as non root bridge with clients

New Features

This release does not contain new features. It supports the features introduced in Cisco IOS Release 12.3(4)JA. This section lists new features in Cisco IOS Release 12.3(4)JA for the access point/bridge.

The following new features are supported by the access point/bridge:

- Support for multiple basic SSIDs (mBSSID)
- Support Wi-Fi 802.11h and Dynamic Frequency Selection (DFS)
- Wireless IDS - Excess Management Frame Detection
- Wireless IDS - Authentication Attack Detection
- Wireless IDS - Active termination for managed clients
- Frame Monitor Mode
- Location Based Services
- SNMPv3

Support for Multiple Basic SSIDs

This feature permits a single access point to appear to the WLAN as multiple virtual access points. It does this by assigning an access point with multiple Basic Service Set IDs (MBSSIDs) or MAC addresses.

Wireless IDS – Excess Management Frame Detection

This feature provides scanner access points the ability to detect that WLAN management and control frames exceeded a configurable threshold.

Wireless IDS – Authentication Attack Detection

This feature requires Cisco Aironet access points to detect and report on excessive attempted or failed authentication attempts (Authentication failure detection and Excess EAPoL authentication).

Frame Monitor Mode

This feature requires a Scan-only access point to forward all 802.11 frames seen to a protocol analysis station for network troubleshooting from remote sites through partner applications or partner Intrusion Detection companies or both.

Location Based Services (LBS)

This feature allows a Cisco Aironet access point to detect frames from a LBS clients and send them to a pre-configured IP destination, such as a third-party LBS server.

SNMPv3

This feature enables SNMPv3 support on Cisco Aironet access points to provide an additional level of security.

Installation Notes

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

Warnings

Warning **This warning 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 in 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.: NFPA70, 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. (240vac, 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 connector. 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 disconnect cables during periods of lightning activity.**

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

Vehicle Installations

The following warnings apply to vehicle installations:

Warning **A readily accessible two-pole disconnect device must be incorporated in the fixed wiring.**

Warning **Connect the unit only to CD power source that complies with the safety extra-low (SELV) requirements in IEC 60950 based safety standards.**

Safety Information

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

FCC Safety Compliance Statement

FCC Compliance with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified eqipment. 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. Your Cisco sales representative can explain which mounting method to use for the size and type antenna you are about to install.
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.
8. If an accident should occur with the power lines call for qualified emergency help immediately.

1300 Series Installation

The 1300 series access point/bridge is available in two configurations:

- Integrated antenna access point/bridge (with 13-dBi patch array antenna)
- External antenna access point/bridge (with antenna connector for use with an external antenna)

Note To meet regulatory restrictions, the external antenna 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 access point/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.

Important Notes

This section describes important information about the access point/bridge.

SNTP Replaces NTP

In Cisco IOS Release 12.3(4)JA1, access points and bridges support SNTP instead of NTP. This change improves the reliability of the system time on access points and bridges, allows access points and bridges to synchronize with any NTP server, and prevents client devices from synchronizing to an access point or bridge that might not be accurate.

Default Username and Password Are *Cisco*

When you open the 1300 series interface, you must enter a username and password. The default username for administrator login is *Cisco*, and the default password is *Cisco*. Both the username and password are case sensitive.

Changes to the Default Configuration—Radios Disabled and No Default SSID

In this release, the radio or radios are disabled by default, and there is no default SSID. You must create an SSID and enable the radio or radios before the access point/bridge will allow wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points and bridges.

Enabling MBSSIDs Without VLANs Disables Radio Interface

If you use the mbssid configuration interface command to enable multiple BSSIDs on a specific radio interface but VLANs are not configured on the access point, the access point disables the radio interface. To re-enable the radio, you must shut down the radio, disable multiple BSSIDs, and re-enable the radio.

This example shows the commands you use to re-enable the radio:

```
AP(config)# interface d1
AP(config-if)# shut
AP(config-if)# no mbssid
AP(config-if)# no shut
```

After you re-enable the radio, you can enable VLANs on the access point and enable multiple BSSIDs.

Some Client Devices Cannot Associate When QoS Is Configured

Some wireless client devices, including Dell Axim handhelds and Hewlett-Packard iPaq HX4700 handhelds, cannot associate to an access point when the access point is configured for QoS. To allow these clients to associate, disable QoS on the access point. You can use the QoS Policies page on the access point GUI to disable QoS, or enter this command on the CLI:

ap(config-if)**#no dot11 qos mode**

Proxy Mobile-IP Feature Removed

The proxy Mobile-IP feature is not supported in Cisco IOS Releases 12.3(2)JA and later.

WPA/2 With Concatenation Not Supported

Cisco IOS Release 12.3(4)JA1 does not support this feature.

Hard Coded Ethernet Port Settings Degrade GUI Performance

Ethernet port settings on the access point/bridge must be set to auto speed and auto negotiation. If you use any other setting, the GUI operates very slowly.

TACACS+ and DHCP IP Address Sometimes Locks Out Administrators

When you configure an access point for TACACS+ administration and to receive an IP address from the DHCP server, administrators might be locked out of the access point after it reboots if the administrator does not have a local username and password configured on the access point. This issue does not affect access points configured with a static IP address. Administrators who have been locked out must regain access by using the mode button to reset the unit to default settings.

Access Point/Bridge Does Not Support Loopback Interface

When configuring the access point/bridge as an access point, you must not configure a loopback interface.

Caution Configuring a loopback interface might generate an IAPP GENINFO storm on your network and disrupt network traffic.

Non-Cisco Aironet 802.11g Clients Might Require Firmware Upgrade

Some non-Cisco Aironet 802.11g client devices require a firmware upgrade before they can associate to the 802.11g radio in the access point/bridge when it is configured as an access point or workgroup bridge. If your non-Cisco Aironet 802.11g client device does not associate to the access point/bridge, download and install the latest client firmware from the manufacturer's website.

Throughput Option for 802.11g Radio Blocks Association by 802.11b Clients

When you configure the 802.11g 1300 series radio for best throughput, the access point/bridge sets all data rates to basic (required). This setting blocks association from 802.11b client devices. The **best throughput** option appears on the web-browser interface Radio0-802.11G Settings pages and in the **speed** CLI configuration interface command.

Use force-reload Option with archive download-sw Command

When you upgrade access point or bridge system software by entering the **archive download-sw** command on the CLI, you must use the **force-reload** option. If the access point or bridge does not reload the Flash after the upgrade, the pages in the web-browser interface might not reflect the upgrade. This example shows how to upgrade system software successfully using the **archive download-sw** command:

```
AP# archive download-sw /force-reload /overwrite tftp:/10.0.0.1/ image-name (image name)
```

Radio MAC Address Appears in ACU

When a Cisco Aironet client device associates to an access point or bridge running IOS software, the device's MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point or bridge radio. The MAC address for the access point or bridge's Ethernet port is printed on the label on the back of the access point or bridge.

Radio MAC Address Appears in Access Point/Bridge Event Log

When a client device roams from an access point (such as access point *alpha*) to another access point (access point *bravo*), a message appears in the event log on access point alpha stating that the client roamed to access point bravo. The MAC address that appears in the event message is the MAC address for the access point/bridge.

Mask Field on IP Filters Page Behaves the Same As in CLI

In Cisco IOS Release 12.2(8)JA and later, the mask that you enter in the Mask field on the IP Filters page in the access point/bridge GUI behaves the same way as a mask that you enter in the CLI. If you enter 255.255.255.255 as the mask, the access point/bridge accepts any IP address. If you enter 0.0.0.0, the access point/bridge looks for an exact match with the IP address that you entered in the IP Address field.

System Software Upgrade Sometimes Fails Using Microsoft Internet Explorer 5.01 SP2

A system software upgrade sometimes fails when you use Microsoft Internet Explorer version 5.01 SP2 to upgrade system software using the HTTP Upgrade page in the web-browser interface. Use a later version of Microsoft Internet Explorer to perform HTTP system software upgrades, or use TFTP to upgrade system software. Click this URL to browse to the *Cisco 1300 Series Wireless Bridge Software Configuration Guide* for complete instructions on performing software upgrades:

http://www.cisco.com/en/US/docs/wireless/access_point/1300/12.3_4_JA/configuration/guide/brsc1234.html

Corrupt EAP Packet Sometimes Causes Error Message

During client authentication, the access point/bridge sometimes receives a corrupt EAP packet and displays this error message:

```
Oct  1 09:00:51.642 R: %SYS-2-GETBUF: Bad getbuffer, bytes= 28165
-Process= "Dot11 Dot1x process", ipl= 0, pid= 32
-Traceback= A2F98 3C441C 3C7184 3C604C 3C5E14 3C5430 124DDC
```

You can ignore these messages.

When Cipher is TKIP Only, Key Management Must Be Enabled

When “Cipher TKIP” is configured on a VLAN, the SSID(s) for that VLAN must use WPA or CCKM key management. If you do not configure the SSID(s) for that VLAN with WPA or CCKM, client authentication fails on the SSIDs.

Non-Cisco Aironet Clients Sometimes Fail 802.1x Authentication

Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the access point/bridge unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

Pings and Link Tests Sometimes Fail to Clients with both Wired and Wireless Network Connections

When you ping or run a link test from an access point to a client device installed in a PC running Microsoft Windows 2000, the ping or link test sometimes fails when the client has both wired and wireless connections to the LAN. Microsoft does not recommend this configuration. For more information, refer to Microsoft Knowledge Base article 157025 at this URL:

http://support.microsoft.com/default.aspx?scid=kb;en-us;157025&Product=win2000

Limitation to PAgP Redundancy on Switches Connected by Bridge Links

When running PAgP on switched connected to series bridges, for ethernet traffic redundancy and load balance be aware that PAgP switchover takes at least 30 seconds, which is too slow to maintain certain traffic (for example, TCP) when switching from port to the other. There is no workaround for this limitation.

Default IP Address Behavior

When an unconfigured access point/bridge boots, it attempts to obtain an IP address from a DHCP server. If it fails to locate a DHCP server, it continues attempting to request an IP address from the DHCP server. To eliminate this behavior, you must access the access point/bridge through its console port and assign a static IP address.

If you want to reset the access point/bridge to its default settings and a static 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 access point/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 RJ 45 jack on the power injector.

The speed and duplex settings on the access point/bridge FastEthernet0 interface apply only to the link between the access point/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 access point/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.

Caveats

This section lists open caveats for Cisco IOS Release 12.3(4)JA and resolved caveats in Cisco IOS Releases 12.3(4)JA, 12.3(4)JA1, and 12.3(4)JA2 for the access point/bridge.

Open Caveats

These caveats are open in Cisco IOS Release 12.3(4)JA for the access point/bridge:

- CSCeb52431—When logging into a TACACS+ server, access points sometimes send hundreds of additional authentication requests to the server after a successful authentication.
- CSCsa53019—UDP traffic performance problem when using WEP.

  When WEP is used with UDP traffic, a throughput input is experienced in the Ethernet interface. If the **show interface fastethernet 0** command is executed, throttle counters increase but no high CPU or buffers failure occurs.
- CSCeh29970—EAP authentication appears to fail at reload when SSID configured with WPA+TKIP with EAP-FAST as the authentication mechanism.

  An authentication failed message appears at the time of reload, but after a few seconds, the authentication succeeds without any configuration change or change in the client's profile.

Resolved Caveats in Cisco IOS Release 12.3(4)JA2

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a **show buffers** command, is passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been inserted.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at the following URL:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051201-http

- CSCee45312

  RADIUS authentication on a device that is running certain versions of Cisco IOS and configured with a fallback method to none can be bypassed.

  Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

  Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

  Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

  More details can be found in the security advisory which posted at the following URL:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050629-aaa

- CSCef67660—SSHv2 malform client ignore message no longer causes damage to router

Resolved Caveats in Cisco IOS Release 12.3(4)JA1

The following caveat is resolved in Cisco IOS Release 12.3(4)JA1:

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051102-timers.

- CSCei76358—Through normal software maintenance processes, Cisco is removing depreciated functionality. These changes have no impact on system operation or feature availability.

Resolved Caveats in Cisco IOS Release 12.3(4)JA

These caveats are resolved in Cisco IOS Release 12.3(4)JA for the access point/bridge:

- CSCee90230—Traceback no longer occurs at reboot when access point is configured for TACACS+ administrator authentication.
- CSCeb82510—You can now configure authentication, authorization, and accounting (AAA) methods for telnet and HTTP independent of the console.
- CSCec12884—The AAA user command authorization no longer fails through HTTP access.
- CSCee42617—Users are now correctly authenticated through the RADIUS server, and accounting information is sent to the RADIUS server.
- CSCee87287—Access points no longer fail to generate accounting records when a wireless client is re-authenticated on an automatic interval (for example, when the access point is configured using the **dot1x reauthentication** *seconds* command).
- CSCef11167—Response value of 4294967292 when polling Dot11ActiveWireless Clients via SNMP no longer occurs.
- CSCef45010—The GUI now performs normally when half duplex and a specified speed are part of its configuration.
- 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/.
- CSCef65076—The access point GUI no longer reports a Bad Request error when you enter a RADIUS server hostname on the access point.
- CSCef89795—Access points no longer send IAPP traffic on the wrong VLAN when layer 3 mobility is enabled.
- CSCeg64999—Access points now support EAP-SIM authentication.
- CSCeg87391—Bridges now display temperature correctly when you enter the **show env** command.

- CSCeh06200—With TACACS configured, administrators can now log into the access point GUI when idle time is configured on the TACACS server.
- CSCeh08952—Access points now correctly filter traffic through the TCP port when an IP filter is configured.
- CSCsa40042, CSCsa40045—The user interfaces on the access point/bridge no longer allow you to configure the bridge to fall back to repeater mode.
- CSCsa40861—Access points configured for a fallback role now assume the fallback role if the LAN interface is down when they reboot.
- CSCsa52462—Access points configured for CKIP or CMIC now indicate CKIP and CMIC support in beacons.
- 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/.
- CSCsa61263—Client devices assigned to a non-native VLAN and connected to a workgroup bridge no longer lose their network connection when the workgroup bridge roams from one root device to another.
- CSCsa64627—STP now functions properly when the native VLAN is not VLAN 1.

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 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

This section lists changes, errors, and omissions from user documentation for access points.

Omissions

Access point/bridge quick start guides do not yet describe these features:

- Changes to the default configuration—In the default configuration for this release, there is no default SSID and the radio interface is disabled by default. You must create an SSID and enable the radio interface before the unit allows wireless associations from other devices.
- Default IP address behavior—When an unconfigured access point/bridge boots, it attempts to obtain an IP address from a DHCP server. If it fails to locate a DHCP server, it continues attempting to request an IP address from the DHCP server. To eliminate this behavior, you must access the access point/bridge through its console port and assign a static IP address.

Related Documentation

This section lists documents related to Cisco IOS Release 12.3(4)JA1 and to access points/bridges.

Platform-Specific Documents

These documents describe installation and configuration of the 1300 series:

- *Quick Start Guide: Cisco Aironet 1300 Series Wireless Bridge*
- *Cisco Aironet 1300 Series Wireless Bridge Hardware Installation Guide*
- *Cisco Aironet 1300 Series Bridge Mounting Instructions*
- *Cisco Aironet 14-dBi Vertically Polarized Sector Antenna (AIR-ANT2414S-R)*

Cisco IOS Software Documentation Set

You can find the most current Cisco IOS documentation on Cisco.com. Follow this link path to find the documentation for Cisco IOS Release 12.3:

Technical Documents > Documentation Home Page > Cisco IOS Software Configuration > Cisco IOS Release 12.3

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.
