



Release Notes for Cisco Aironet 1100 and 1200 Series Access Points for Cisco IOS Release 12.2(11)JA3

April 15, 2004

Cisco IOS Release 12.2(11)JA3 resolves caveats for 1100 and 1200 series access points but does not introduce new features. These release notes describe caveats for Cisco IOS Release 12.2(11)JA3 and features and enhancements introduced in Cisco IOS Release 12.2(11)JA.

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Installation Notes, page 5](#)
- [Important Notes, page 7](#)
- [Caveats, page 8](#)
- [Troubleshooting, page 11](#)
- [Related Documentation, page 11](#)
- [Obtaining Documentation and Submitting a Service Request, page 11](#)



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 Access Point is a wireless LAN transceiver that acts as the connection point between wireless and wired networks or as the center point of a standalone wireless network. In large installations, the roaming functionality provided by multiple access points enables wireless users to move freely throughout the facility while maintaining uninterrupted access to the network.

You can configure and monitor 1100 and 1200 series access points using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

System Requirements

You can install Cisco IOS Release 12.2(11)JA3 on 1100 series access points and on 1200 series access points that have been configured at the factory to run Cisco IOS software (model AP1230).

To install this release on a 1200 series access point that does not run IOS software, use the conversion utility to convert to IOS software without losing your current configuration. To convert to IOS software without saving your configuration, load the conversion image. The access point reboots with IOS software and factory default settings. Your 1200 series access point must run one of these VxWorks versions before you can convert to IOS software: 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T. If your access point runs version 12.04, you must downgrade to a supported VxWorks version before you can upgrade to IOS software.

**Note**

Cisco Aironet 340 Series Access Points do not support IOS software. Do not attempt to load an IOS image on 340 series access points or on 350 and 1200 series access points that have not been converted.

Finding the IOS Software Version

To find the version of IOS software running on your access point, use a Telnet session to log into the access point and enter the **show version EXEC** command. This example shows command output from an access point running Cisco IOS Release 12.2(8)JA:

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(8)JA
Copyright (c) 1986-2003 by Cisco Systems, Inc.
```

On access points running IOS software, you can also find the software version on the System Software Version page in the access point's web-browser interface.

If your access point does not run IOS software, the software version appears at the top left of most pages in the web-browser interface.

Upgrading to a New Software Release

For instructions on installing access point software:

1. Follow this link to the Cisco Support page:
<http://www.cisco.com/cisco/web/support/index.html>
2. Follow this path to the product, document, and chapter:
Aironet 1200 Series Wireless LAN Products > Cisco Aironet 1200 Series Access Points > Aironet 1200 Series Access Points, Cisco IOS Rel. 12.2(13)JA > Cisco IOS Software Configuration Guide for Cisco Aironet Access Points > Managing Firmware and Configurations > Working with Software Images
3. Click this link to browse to the Cisco IOS Software Center on Cisco.com:
<http://www.cisco.com/cisco/software/navigator.html>
Log into Cisco.com to use the Cisco IOS Upgrade Planner.

Converting to Cisco IOS Software

If your 1200 series access point does not run IOS software, you can use the conversion utility or the conversion image to convert the access point system to IOS software. Use the conversion utility to maintain the current configuration after the conversion, or load the conversion image to convert to IOS software without saving the current configuration. Your access point must run one of these VxWorks firmware versions before you can convert to IOS software: 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T.

**Note**

The upgrade image and the conversion tool do not support VxWorks version 12.04. Access points running operating system version 12.04 must be downgraded to a supported operating system version before you can use the upgrade image or the conversion tool.

To download the conversion utility or the converter image, click this link to browse to the Cisco IOS Software Center on Cisco.com:

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

Log into Cisco.com to use the Feature Navigator or the Cisco IOS Upgrade Planner, or click **Wireless Software** to go to the Wireless LAN Software page. Download the conversion utility or the conversion image for 1200 series access points. You can also download instructions for using the utility and the image.

New Features

Cisco IOS Release 12.2(11)JA3 does not introduce new features. This section lists features that were introduced in Cisco IOS Release 12.2(11)JA.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is now supported on Cisco Aironet access points. WPA is the Wi-Fi Alliance specification for interoperable wireless LAN security. It supports IEEE 802.1X authentication using extensible authentication protocol (EAP) authentication types and temporal key integrity protocol (TKIP) encryption.

Fast Secure Roaming

Fast secure roaming for Cisco or Cisco Compatible wireless client devices using the Cisco Centralized Key Management (CCKM) protocol is available with this release. Fast, secure roaming is used to support time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP) or Citrix-based solutions. Fast secure roaming is a component of wireless domain services.

IEEE 802.1X Local Authentication Service

This feature allows a Cisco IOS software enabled device to authenticate wireless clients when connectivity to the AAA server is not available. It incorporates an IEEE 802.1X enabled RADIUS server that supports EAP authentication types into Cisco IOS software. This allows the Cisco Aironet access point to authenticate wireless clients when the wide area network (WAN) link is down or the RADIUS server at the central site is not available. This provides remote site survivability by allowing an access point to continue to access local resources such as file servers or printers in remote site deployments with non-redundant WAN links.

This release supports the EAP authentication type Cisco LEAP and operates with Cisco Secure Access Control Server (ACS) version 2.6 or later. IEEE 802.1X local authentication service is a component of wireless domain services.

Wireless Domain Services

Wireless domain services (WDS) is a collection of Cisco IOS software features that enhance wireless LAN (WLAN) client mobility and simplify WLAN deployment and management. The WDS feature set supported in this release includes fast secure roaming and IEEE 802.1X local authentication service.

Installation Notes

This section contains information you should keep in mind when installing 1100 and 1200 series access points.

Installation in Environmental Air Space

This section provides information on installing 1200 series access points in environmental air space, such as above suspended ceilings.

Cisco Aironet 1100 and 1200 Series Access Points provide adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the *National Electrical Code* (NEC) and Sections 2-128, 12-010(3) and 12-100 of the *Canadian Electrical Code*, Part 1, C22.1.

**Caution**

The power injector does not provide fire resistance and low smoke-producing characteristics and is not intended for use in extremely high or low temperatures or in environmental air spaces, such as above suspended ceilings.

**Note**

If you plan to mount a 1200 series access point with a 5-GHz radio in an area subject to environmental air space, Cisco recommends that you mount the access point horizontally so that its antennas point down. Doing so ensures that the access point complies with regulatory requirements for environmental air space with the 5-GHz radio installed.

Power Considerations

This section describes issues you should consider before applying power to an access point.

**Caution**

The operational voltage range for 1100 series access points is 24 to 60 VDC, and the nominal voltage is 48 VDC. Voltage higher than 60 VDC can damage the equipment.

**Caution**

The nominal voltage for 1200 series access points is 48 VDC, and the access point is operational up to 60 VDC. Voltage higher than 60 VDC can damage the equipment.

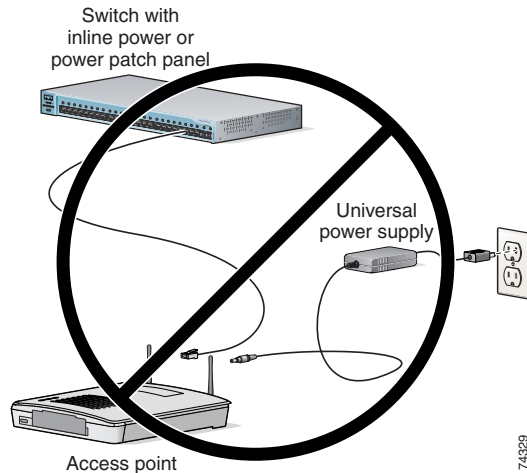
**Caution**

Cisco Aironet power injectors are designed for use with Cisco Aironet access points and bridges only. *Do not use the power injector with any other Ethernet-ready device.* Using the power injector with other Ethernet-ready devices can damage the equipment.

Use Only One Power Option

You cannot provide redundant power to the access point with both DC power to its power port and inline power from a patch panel or powered switch to the access point's Ethernet port. If you apply power to the access point from both sources, the switch or power patch panel might shut down the port to which the access point is connected. [Figure 1](#) shows the power configuration that can shut down the port on the patch panel or powered switch.

Figure 1 *Improper Power Configuration Using Two Power Sources*



Operating 5-GHz Radio Requires Power Injector, Power Module, or Catalyst 3550-24 PWR Switch

The 1200 series power injector and the 1200 series power module support operation of the 5-GHz radio in the access point. Currently, the Catalyst 3550-24 PWR switch supports power for both the 2.4-GHz radio and the 5-GHz radio. Other switches and power patch panels might not provide enough power for the 5-GHz radio.

Access Point Requires 1200 Series Universal Power Supply and Power Injector

The 350 series universal power supply and power injector are not compatible with the 1200 series access point. If you use a power injector or a power module to provide power to a 1200 series access point, you must use a 1200 series universal power supply. If you need to use a power injector to inject power into the access point's Ethernet port, you must use a 1200 series power injector.

Antenna Installation

For instructions on the proper installation and grounding of external antennas for 1200 series access points, refer to the National Fire Protection Association's *NFPA 70, National Electrical Code*, Article 810, and the Canadian Standards Association's *Canadian Electrical Code*, Section 54.



Warning

Do not install 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.

Important Notes

This section describes important information about the access point.

Radio MAC Address Appears in ACU

When a Cisco Aironet client device associates to an 1100 or 1200 series access point running IOS software, the access point MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Radio MAC Address Appears in Access Point 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 radio in access point bravo. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

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 GUI behaves the same way that a mask behaves when you enter it in the CLI. If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address that you entered in the IP Address field.

Repeater Access Points Running IOS Software Cannot Associate to Parent Access Points Not Running IOS Software

Repeater access points running Cisco IOS software cannot associate to parent access points that do not run IOS software (340 and 350 series access points, and 1200 series access points that have not been converted to run IOS software).

Repeater Access Points Cannot Be Configured As WDS Access Points

Repeater access points do not support WDS. You cannot configure a repeater access point as a WDS access point, and if a root access point becomes a repeater in fallback mode, it cannot provide WDS.

Crossover Cable Sometimes Needed When Ethernet Speed and Duplex Set to Fixed on 1100 Series Access Points

If you change the speed and duplex settings from auto to fixed on an 1100 series access point's Ethernet port, the auto-MDIX feature on the port is disabled. When auto-MDIX is disabled, you must determine whether to use a straight-through or a crossover cable to connect the access point Ethernet port to another device. If the Ethernet link goes down after you set the speed and duplex to fixed, try changing the Ethernet cable from crossover to straight-through or from straight-through to crossover.

Cannot Perform Link Tests on Non-Cisco Aironet Client Devices

The link test feature on the web-browser interface does not support non-Cisco Aironet client devices.

Firmware Upgrade Sometimes Fails Using Microsoft Internet Explorer 5.01 SP2

A firmware upgrade sometimes fails when you use Microsoft Internet Explorer version 5.01 SP2 to upgrade firmware using the HTTP Upgrade page in the web-browser interface. Use a later version of Microsoft Internet Explorer to perform HTTP firmware upgrades.

Caveats

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

Open Caveats

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

- CSCea88706—You cannot modify existing MAC address and Ethertype filters on the access point web-browser interface.
Workaround: Instead of modifying the filter, delete the filter and recreate it using the web-browser interface.
- CSCea88862—You cannot run a link test using thousands of packets on the web-browser interface.
Workaround: When running link tests on the web-browser interface, limit the test to hundreds of packets, or use the CLI to run link tests using thousands of packets.
- CSCea89985—When you configure hot standby mode using a broadcast MAC address to specify the access point to be monitored, the access point generates a traceback.
Workaround: Do not use a broadcast MAC address when configuring hot standby.

- CSCea91378—When you run a carrier busy test on the web-browser interface when the access point radio is disabled, the web-browser interface reports that the test failed.

Workaround: Enable the radio interface before running the carrier busy test on the web-browser interface, or run the carrier busy test on the CLI.

- CSCea91424—When a CCKM client device roams to a foreign network using proxy Mobile IP, these error messages sometimes appear even though the client associates successfully:

```
Apr 30 20:36:34.521: %DOT11-7-AUTH_FAILED: Station 000b.fd75.4180 Authentication failed
Apr 30 20:36:37.712: %DOT11-6-ASSOC: Interface Dot11Radio0, Station STL-CLIENT-3 000b.fd75.4180 Associated KEY_MGMT[CCKM]
```

You can ignore these messages.

- CSCeb06139—When several mobile clients are using Cisco Centralized Key Management (CCKM), the access point sometimes reboots when you enter the **show wlccp wds mn detail** command and the command displays the mobile node details at the same time that a mobile node expires and is deleted.

Workaround: Before entering the **show wlccp wds mn detail** command, enter **terminal length 0** in privileged EXEC mode to display the **show wlccp wds mn detail** command output without breaking it into multiple pages.

- CSCin44512—If 8 or more VLANs are configured on your access point, you cannot apply filters using the Apply Filters page in the web-browser interface.

Workaround: Use the CLI to apply filters when 8 or more VLANs are enabled.

- CSCin44591—When you use the web-browser interface to enable PSPF on a non-native VLAN, PSPF does not work.

Workaround: Use the CLI to enable PSPF on a non-native VLAN.

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>

- CSCec55538—Access points no longer send static WEP keys in clear text to the SNMP server when you enable the **snmp-server enable traps wlan-wep** command.
- CSCed26579—When you upgrade a 1200 series access point in the EMEA regulatory domain from VxWorks to Cisco IOS software, the upgrade no longer changes the maximum transmit power on the 2.4-GHz radio to 100 mW.
- 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**.

Related Documentation

This section lists documents related to Cisco IOS Release 12.2(11)JA and to 1100 and 1200 series access points:

- *Quick Start Guide: Cisco Aironet 1100 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1200 Series Access Points*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *Installation Instructions for Cisco Aironet Power Injectors*

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.

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. 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.