



Release Notes for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges

February 16, 2002

These release notes describe features and caveats for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges running firmware version 11.08T1. Firmware version 11.08T1 fixes these defects: CSCdw63011, CSCdw63031, and CSCdw63032.

Contents

- [Introduction, page 1](#)
- [New Features, page 2](#)
- [Installation Notes, page 3](#)
- [Limitations and Restrictions, page 4](#)
- [Important Notes, page 7](#)
- [Caveats, page 7](#)
- [Troubleshooting, page 9](#)
- [Related Documentation, page 9](#)
- [Obtaining Documentation, page 9](#)
- [Obtaining Technical Assistance, page 10](#)

Introduction

Cisco Aironet Access Points are wireless LAN transceivers that can act as the center point of a standalone wireless network or as the connection point between wireless and wired networks. Cisco Aironet Bridges are wireless LAN transceivers that connect two or more remote networks into a single LAN. The 350 series bridge can also be used as a rugged access point, providing network access to wireless client devices.



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

The access point and bridge use a browser-based management system. The system settings are on web pages in the system firmware. You use your internet browser to view and adjust the system settings.

New Features

This section describes new software features in firmware version 11.08T, which are also included in version 11.08T1.

Manage Firmware with CiscoWorks 2000 Software Image Management Tool

Software Image Management (SWIM) is an application in the Resource Manager Essentials (RME) portion of CiscoWorks 2000. With firmware version 11.08T you can use SWIM to manage the firmware in Cisco Aironet 340 and 350 series access points and 350 series bridges from a central point of control. For instructions on using SWIM, refer to *Using Resource Manager Essentials* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e_3_x/3_3/u_guide/ug_ea_pps.htm

Block Inter-Client Communication with PSPF Feature

Publicly Secure Packet Forwarding (PSPF) prevents client devices associated to a bridge or access point from inadvertently sharing files with other client devices on the wireless network. PSPF provides Internet access to client devices without providing other capabilities of a LAN. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network. This feature is useful for public wireless networks like those installed in airports or on college campuses.

Follow these steps to enable PSPF on your access point or bridge:

-
- Step 1** Browse to the Association Table Advanced page:
 - a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Advanced** under Associations.
 - Step 2** Select **Yes** for Block ALL Inter-Client Communications (PSPF).
 - Step 3** Click **Apply** or **OK**. PSPF is enabled.
-

Monitor Authentication Progress with EAP Diagnostic Features

Enable the access point's EAP diagnostic features to view each client device's authentication progress and the contents of authentication packets sent between the client device, the access point or bridge, and the RADIUS server. Enter the commands in the command-line interface (CLI) to display the information. You can open the CLI with Telnet or with a terminal emulator through the access point's or bridge's serial port.

Consult the [“Using Command-Line Diagnostics” section on page 9-19](#) in the *Cisco Aironet Access Point Software Configuration Guide* for more information on diagnostic features in the CLI.

Installation Notes

You can find the latest release of access point and bridge firmware at the following URL:

<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

Installation in Environmental Air Space

Cisco Aironet 350 series bridges and metal-case access points are suitable for use in environmental air space in accordance with Section 300-22(c) of the *National Electrical Code*.



Caution

The Cisco Aironet power injector has a smaller operating temperature range (32 to 104°F; 0 to 40°C) than the 350 series bridge and metal-case access point. The power injector is not intended for use in extremely high or low temperatures or in environmental air spaces, such as above suspended ceilings.

Antenna Installation

For instructions on the proper installation and grounding of external antennas, 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 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.

Power Considerations



Caution

The operational voltage range for 350 series access points and bridges is 24 to 60 VDC, and the nominal voltage is 48 VDC. Voltage higher than 60 VDC can damage the equipment.



Caution

Cisco Aironet power injectors are designed for use with 350 series 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.

System Requirements

You must have a Cisco Aironet 340 or 350 Series Access Point or a 350 Series Bridge to install firmware version 11.08T1.

Version Supported

Your access point must be running firmware version 10.x or later to install firmware version 11.08T1.
Your bridge must be running version 11.07 to install firmware version 11.08T1.

Upgrading to a New Firmware Release

Determining the Firmware Version

The firmware version number is in the upper-left corner of most management screens in the web-browser interface and at the top of the home (Summary Status) page in the command-line interface.

Upgrade Procedure

For instructions on installing access point and bridge firmware:

1. Follow this link to the Cisco Aironet documentation home page:
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>
2. Follow this path to the product, document, and chapter:
Aironet 350 Series Wireless LAN Products > Cisco Aironet 350 Series Access Points > Cisco Aironet Access Point Software Configuration Guide > Maintaining Firmware > Updating Firmware
3. Follow this link to the Software Center on Cisco.com and download firmware version 11.08T1:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

**Note**

To upgrade firmware from a file server, you must enter settings on the access point's or bridge's FTP Server Setup page. Refer to the *Cisco Aironet Access Point Software Configuration Guide* for more information.

Limitations and Restrictions

Removing Power During Firmware Update Can Corrupt Radio Firmware

When you update the firmware on an access point or bridge, allow the unit to finish its start-up sequence before removing power. If you update the firmware and remove power before the unit finishes the start-up sequence, the radio firmware might be corrupted, making the unit inoperable. If the radio firmware is corrupted, the radio indicator (the bottom of the three indicators on top of the access point or bridge) lights solid red, and the following error message appears when the access point or bridge starts up:

Failed to start driver for port "awc0" (errno=0x006d0002)

If the radio firmware is corrupted, you must return the unit to Cisco for service.

You can safely remove power after a firmware update when the configuration management pages reappear in the command-line or web-browser interfaces, or when the three status indicators on top of the unit complete the following pattern:

1. All three indicators are solid green, meaning that the access point is beginning to update the firmware.
2. The middle indicator is solid green and the top and bottom indicators are off, indicating that the access point or bridge is updating the radio firmware.

When the middle indicator blinks or the top and bottom indicators blink, you can remove power.

EAP Authentication Requires Matching 802.1x Protocol Drafts



Note

This section applies to wireless networks set up to use LEAP. If you do not use LEAP on your wireless network, you can skip this section.

Wireless client devices use Extensible Authentication Protocol (EAP) to log onto a network and generate a dynamic, client-specific WEP key for the current logon session. If your wireless network uses WEP without EAP, client devices use the static WEP keys entered in the Aironet Client Utilities.

If you use Network-EAP authentication on your wireless network, your client devices and access points must use the same 802.1x protocol draft. For example, if the radio firmware on the client devices that will associate with an access point is 4.16, then the access point should be configured to use Draft 8 of the 802.1x protocol. [Table 1](#) lists firmware versions for Cisco Aironet products and the draft with which they comply.

Table 1 802.1x Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	Draft 10 ¹
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 or later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later ²	—	x	x
AP34x/35x 11.07 and later	—	x	x
AP34x/35x and BR35x 11.08T1	—	x	x

1. The functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1x standard.
2. The default draft setting in access point and bridge firmware version 11.06 and later is Draft 10.

**Note**

Draft standard 8 is the default setting in firmware version 11.05 and earlier, and it might remain in effect when you upgrade the firmware to version 11.06 or later. Check the setting on the Authenticator Configuration page in the management system to make sure the best draft standard for your network is selected.

Use the Authenticator Configuration page in firmware version 11.08T1 to select the draft of the 802.1x protocol the access point or bridge radio should use. Follow these steps to set the draft for your access point or bridge:

-
- Step 1** Browse to the Authenticator Configuration page in the access point management system.
- a. On the Summary Status page, click **Setup**.
 - b. On the Setup page, click **Security**.
 - c. On the Security Setup page, click **Authentication Server**.
- Step 2** Use the 802.1x Protocol Version (for EAP authentication) pull-down menu to select the draft of the 802.1x protocol the access point or bridge radio should use. Menu options include:
- Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.
 - Draft 8—Select this option if LEAP-enabled client devices that associate with this access point or bridge use radio firmware versions 4.13, 4.16, or 4.23.
 - Draft 10—This is the default setting in firmware versions 11.06 and later. Select this option if client devices that associate with this access point or bridge use Microsoft Windows XP EAP authentication or if LEAP-enabled client devices that associate with this access point or bridge use radio firmware version 4.25 or later. The functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1x standard.
- Step 3** Click **Apply** or **OK** to apply the setting. The access point or bridge reboots.
-

Select WEP Key 1 as Transmit Key for EAP Authentication

If you use Network-EAP as the authentication type on your wireless network, you must select key 1 as the transmit key on the access point or bridge AP Radio Data Encryption page. The access point or bridge uses the WEP key you enter in key slot 1 to encrypt multicast data signals that it sends to EAP-enabled client devices. Because the access point or bridge transmits the WEP key used for multicast messages to the EAP-enabled client device during the EAP authentication process, that key does not have to appear in the EAP-enabled device's WEP key list. The access point or bridge uses a dynamic WEP key to encrypt unicast messages to EAP-enabled clients. Bridges use static WEP keys when communicating with other bridges.

If you do not use EAP authentication on your wireless network, you can select any WEP key as the transmit key.

MIB File Compatible with Firmware Version 11.00 and Later

The access point MIB file (AWCVX-MIB) is supported only by access point firmware version 11.00 and later. Earlier versions of firmware do not support this MIB. You can download the access point MIB at <http://www.cisco.com/public/sw-center/sw-wireless.shtml>.

Important Notes

This section lists important information about access points and bridges running firmware version 11.08T1.

Cisco Discovery Protocol Re-Enabled for Individual Interfaces on Reboot

The Cisco Discovery Protocol (CDP) feature is enabled by default, and CDP is enabled for each of the access point's or bridge's individual interfaces by default. However, if you disable CDP for one of the individual interfaces, the access point or bridge re-enables CDP for that interface when it reboots. If you disable CDP completely, the access point or bridge does not re-enable CDP on reboot.

Caveats

This section lists resolved and open software issues in firmware version 11.08T1.

Getting Bug Information on Cisco.com

If you are a registered Cisco user, you can use the Cisco TAC Software Bug Toolkit, which consists of three tools (Bug Navigator, Bug Watcher, and Search by Bug ID Number) that help you identify existing bugs (or caveats) in Cisco software products.

Access the TAC Software Bug Toolkit at <http://www.cisco.com/support/bugtools/>.

Resolved Caveats

The following caveats have been resolved in firmware version 11.08T1:

- Resolved: CSCdw63011--An error can occur with management protocol processing. Please use this URL for further information:
<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw63011>
- Resolved: CSCdw63031--An error can occur with management protocol processing. Please use this URL for further information:
<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw63031>
- Resolved: CSCdw63032--An error can occur with management protocol processing. Please use this URL for further information:
<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw63032>

The following caveats were resolved in firmware version 11.08T and are also resolved in version 11.08T1:

- Resolved: Continuous reboot caused by exception error on access points running firmware version 11.07 (CSCdv20709). Access points running firmware version 11.07 continuously reboot when the following error occurs:

```
instruction access
Exception next instruction access: 0xc0000000
Machine Status Register: 0x08209032
Condition Register: 0x48000040
Task: 0x1b960 "tProtoCDP"
```

The error occurs when a CDP-unaware device, such as a hub that does not support CDP, forwards CDP messages containing the power consumption TLV from one access point to another. The access point receiving the forwarded CDP message reboots.

- Resolved: Settings for Require EAP and Default Unicast Filter missing from CLI (CSCdu74974). On the CLI, the AP/Root Radio Advanced page does not contain the Require EAP and Default Unicast Address Filter settings.

Open Caveats

The following caveats have not been resolved for firmware version 11.08T1:

- Protocol filter settings sometimes revert to defaults during filter setup (CSCdu02040).

When you add a new protocol filter set, you can set the filter's default disposition and time-to-live on the first filter configuration page. You add specific protocols to the filter set on subsequent pages. If you change the default disposition or default time to live values from the defaults, these values revert to default settings after you add specific protocols to complete the filter setup. Make sure the default disposition and time-to-live values are correct before you apply the filter set.

- IP Port filters do not block pings (CSCdu05324).

Table B-3 in Appendix B of the *Cisco Aironet Access Point Software Configuration Guide* lists PING as the additional identifier for the echo IP Port filter entry. However, the echo entry does not block standard pings. To block standard pings, set up an IP Protocol filter to block ICMP.

- Cannot access workgroup bridges associated with access point or bridge (CSCdu10993).

When a workgroup bridge (WGB34x or WGB352) is associated to an access point, you cannot access the WGB console menus or ping the WGB from a station on the wired LAN connected to the access point's Ethernet port. However, you can access the WGB from any client device connected to the WGB's Ethernet port and from any client device associated to the access point that is associated to the WGB. Radio traffic between the access point and the WGB is not affected.

- Access point ignores vendor specific options from DHCP servers (CSCdu19500).

Access points ignore the vendor specific option (VSO) sent from DHCP servers in response to the access point's vendor class identifier, also called a DHCP identifier in the access point's web browser interface and CLI.

- SNMP community name must include extra privilege to access all information (CSCdt31925).

SNMP community names entered on the Express Setup page have limited access to access point configuration information. To provide full access to the SNMP community you specify on the Express Setup page, use the User Manager pages to assign firmware privilege to the community

name. Refer to the *Cisco Aironet Access Point Software Configuration Guide* for complete instructions on using the User Manager. Refer to the *Cisco Aironet Access Point Software Configuration Guide* for more information on using the User Manager.

- Filters can be disabled but not edited from the command-line interface (CSCdt34104).
You cannot edit MAC address filters with the command-line interface. However, you can use the CLI's Ethernet Protocol Filters and Root Radio Protocol Filters pages to disable filters.
- Access point sometimes loads wrong firmware when updating from an FTP server (CSCdu38857).
When you update access point firmware through FTP file retrieval in the web-browser interface, the access point searches for any valid firmware files if it does not find the firmware file on the FTP server. If the access point finds a valid firmware file, it uses the alternate file and does not indicate on the web-browser interface that it is loading an alternate firmware image. After you update firmware through FTP file retrieval in the web-browser interface, verify that the access point loaded the correct firmware version. The access point firmware version number appears in the upper-left corner of most management screens in the web-browser interface.
- Web-browser interface sometimes requires multiple logins (CSCdu68659).
When User Manager is enabled and you browse to the Cisco Services Setup page, you must log into the User Manager system. If you browse from the Cisco Services Setup page to another restricted page, you must log in again.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac>. Select **Wireless LAN** under Top Issues.

Related Documentation

Use the following documents with this document.

- *Quick Start Guide: Cisco Aironet Access Points*
- *Cisco Aironet Access Point Hardware Installation Guide*
- *Cisco Aironet Access Point Software Configuration Guide*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used with the documents listed in the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0705R)

Copyright © 2002, Cisco Systems, Inc.
All rights reserved.