



FIRST DRAFT - CISCO CONFIDENTIAL

Release Notes for Cisco Aironet 350 Series Workgroup Bridges Running Firmware Release 8.89

August, 2004

These release notes describe caveats in firmware maintenance release 8.89 for Cisco Aironet 350 Series Workgroup Bridges. These release notes also contain important information about the device.

Contents

These release notes describe the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Upgrading to a New Firmware Release, page 2](#)
- [New Features, page 3](#)
- [Installation Notes, page 3](#)
- [Important Notes, page 4](#)
- [Caveats, page 5](#)
- [Troubleshooting, page 6](#)
- [Documentation Updates, page 6](#)
- [Related Documentation, page 6](#)
- [Obtaining Documentation, page 6](#)
- [Documentation Feedback, page 7](#)
- [Obtaining Technical Assistance, page 7](#)
- [Obtaining Additional Publications and Information, page 9](#)



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Introduction

Workgroup bridges are small, standalone units that provide wireless infrastructure connections for Ethernet-enabled devices. A device connected to a bridge communicates with a network infrastructure through Cisco Aironet access points.

The workgroup bridge connects to a hub through a standard Ethernet port using a 10BASE-T (twisted pair) RJ-45 connector, and up to eight wired Ethernet client devices can be connected to the hub. You can use an Internet browser or Telnet to configure the workgroup bridge.

System Requirements

You must have a Cisco Aironet 350 Series Workgroup Bridge to install firmware version 8.89.

Minimum Firmware Version Required on Access Points

Access points with which the workgroup bridge associates must contain firmware version 11.06 or later.

Upgrading to a New Firmware Release

Finding 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.

Obtaining the Workgroup Bridge Image

The workgroup bridge image file can be obtained from the Cisco.com software center using these steps:

-
- Step 1** Follow this link to the Software Center on Cisco.com, and download firmware version 8.89:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
 - Step 2** Click **Option 2: Aironet Wireless Software Display Tables**.
 - Step 3** Find the workgroup bridge firmware and utilities section, and click **Cisco Aironet 350 Series**.
 - Step 4** Click **WGB350v889.exe**, the workgroup bridge image file.
 - Step 5** On the Encryption Authorization Form, enter the requested information, read the encryption information, and check the boxes that apply.
 - Step 6** Click **Submit**.
 - Step 7** Read and accept the terms and conditions of the Software License Agreement.
 - Step 8** Select the image file again to download it.
 - Step 9** Download and save the image file to your hard drive, and then exit the Internet browser.

FIRST DRAFT - CISCO CONFIDENTIAL

- Step 10** Double-click **WGB350v889.exe** to expand the downloaded file, and record the location where you stored the expanded .img file.
-

Upgrading the Workgroup Bridge Firmware

Follow these steps to upgrade the workgroup bridge firmware image by using an Internet browser:

- Step 1** Open an Internet browser on a computer that is on the same network as the bridge.
- Step 2** Enter the bridge IP address in the browserlocation field. Click **Enter**.
- Step 3** When the bridge management home page appears, click **Allow Config Changes** in the upper-left corner.
- Step 4** In the Diagnostics menu, click **Load**.
- Step 5** Enter the path and filename of the new image file in the entry field, such as c:\firmware\WGB350v889.img.
- Step 6** Click **Send**. The workgroup bridge loads the new firmware and reboots.
- Step 7** If an error message appears stating that the page cannot be refreshed without resending the information, click **Cancel**. The workgroup bridge loads the new firmware, and you can ignore the message.
- Step 8** To verify that the upgrade is successful, repeat [Step 1](#) and [Step 2](#). When the bridge management home page appears, verify that the new firmware version number (8.89) appears beside the model name in the upper-left corner of the page.
-

New Features

There are no new features in this software maintenance release.

Installation Notes

Verify Mounting Hole Measurement

If you make a photocopy of the mounting template (included in *Mounting Instructions for the Cisco Aironet Access Points, Base Stations, and Workgroup Bridges with Plastic Cases*), make sure that the distance between the holes is 4 3/4 in. (12.06 cm) before you drill the holes. Some photocopy machines do not make exact duplicates of the original.

Important Notes

Cisco Aironet Software Requires Completion of Encryption Authorization Form

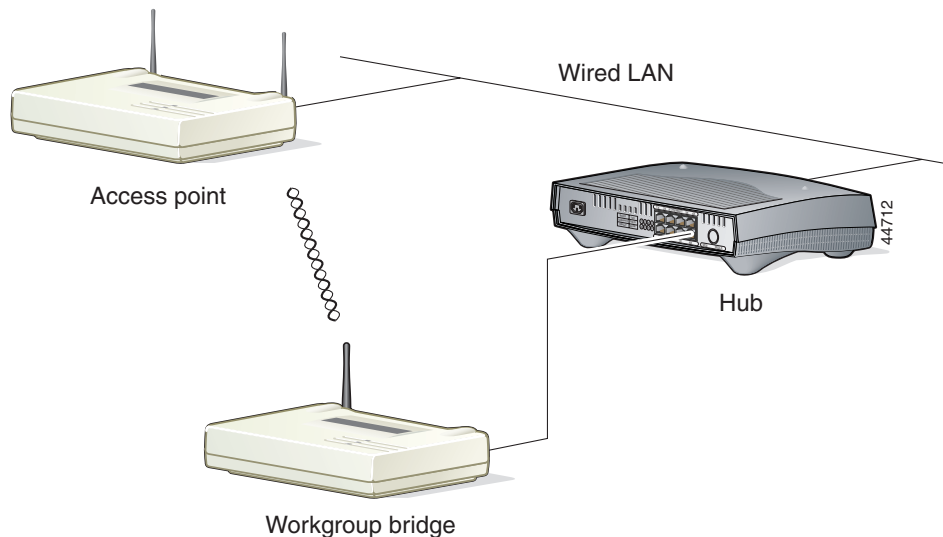
To access Cisco Aironet software from the Software Center on Cisco.com, you must complete a form to receive authorization to download encrypted software. Registered Cisco.com users are required to fill out the form only once, while public users must do so once each session, each time software is downloaded. A form is automatically created for public users. The form for registered Cisco.com users is at the following URL:

http://www.cisco.com/cgi-bin/Software/Crypto/crypto_main.pl

Bridge Loop Can Occur with Incorrect Network Topology

If the workgroup bridge is connected to the wired LAN and is communicating with an access point on the same LAN, a network problem known as a *bridge loop* can occur. Avoid a bridge loop by disconnecting the workgroup bridge from the wired LAN immediately after you configure it. [Figure 1](#) shows the network configuration in which the loop occurs.

Figure 1 Bridge Loop Caused by a Workgroup Bridge Connected to the Wired LAN

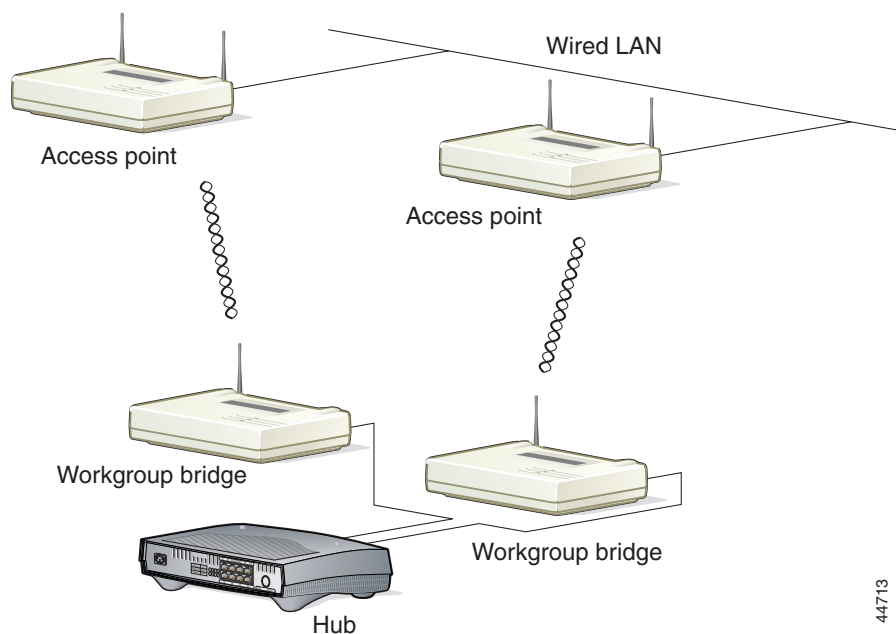


FIRST DRAFT - CISCO CONFIDENTIAL

A bridge loop can also occur if two or more workgroup bridges are connected to the same remote hub. To prevent this bridge loop, always connect only one workgroup bridge to a remote hub.

Figure 2 shows the network configuration in which the bridge loop occurs.

Figure 2 Bridge Loop Caused by Two Workgroup Bridges on the Same Remote Hub



44713

Caveats

This section describes the resolved caveats for firmware version 8.89.

Getting Bug Information on Cisco.com

If you are a Cisco.com registered user, you can use the Cisco TAC Software Bug Toolkit to identify existing bugs (or caveats) in Cisco software products. Access the TAC Software Bug Toolkit at:

<http://www.cisco.com/support/bugtools/>.

Open Caveats

- CSCea59101—Signal strength test does not display level until a warm reload is performed.
When the workgroup bridge has been running for a day or more, performing the signal strength test does not display the signal level bar unless the unit is restarted (warm reloaded) using the Telnet or browser interface.

FIRST DRAFT - CISCO CONFIDENTIAL

Resolved Caveats

The following caveats were resolved in firmware version 8.89:

- CSCee83100—Workgroup bridge does not automatically LEAP reauthenticate after a failure.
- CSCea64630—Workgroup bridge resets to factory defaults by itself.
- CSCed33613—Link tests parameter is reset to factory default by rebooting the workgroup bridge.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at this URL (select **Product Support** > **Wireless** > **Wireless LAN**):

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

Documentation Updates

This section describes errors, omissions, and changes in user documentation for workgroup bridges.

Staleout Time Setting

The workgroup bridge management system includes a wired LAN staleout time setting on the Configuration > Ethernet page. Use this setting to control the number of seconds that the workgroup bridge continues to track a device in its association table when the device is inactive. Enter a value between 5 and 1000 seconds. (Five minutes equals 300 seconds; ten minutes equals 600 seconds.)

If the same devices are always connected to the workgroup bridge, enter **5** for the staleout time setting. If the devices connected to the workgroup bridge change frequently, enter **300** (equal to five minutes) for the staleout time setting. If you disconnect the Ethernet cable from the workgroup bridge and reconnect it, the workgroup bridge removes all devices from its association table and relearns them, regardless of the staleout time setting.

Related Documentation

Use the following documents with this document:

- *Quick Start Guide: Cisco Aironet Workgroup Bridges*
- *Cisco Aironet Workgroup Bridge Hardware Installation Guide*
- *Cisco Aironet Workgroup Bridge Software Configuration Guide*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

FIRST DRAFT - CISCO CONFIDENTIAL

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

FIRST DRAFT - CISCO CONFIDENTIAL

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

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

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

FIRST DRAFT - CISCO CONFIDENTIAL

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:
<http://www.cisco.com/go/marketplace/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>

FIRST DRAFT - CISCO CONFIDENTIAL

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



Copyright © 2004 Cisco Systems, Inc. All rights reserved.