



# Release Notes for Cisco Aironet Workgroup Bridges Running Firmware Release 8.80

---

May 31, 2002

These release notes describe features and caveats contained in this maintenance release for Cisco Aironet Workgroup Bridges running firmware release 8.80. 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 5](#)
- [Caveats, page 6](#)
- [Troubleshooting, page 7](#)
- [Documentation Updates, page 7](#)
- [Related Documentation, page 8](#)
- [Obtaining Documentation, page 8](#)
- [Obtaining Technical Assistance, page 9](#)



---

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

Copyright © 2002. 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 10BaseT/RJ-45 (twisted pair) connector, and up to eight 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 340 or 350 Series Workgroup Bridge to install firmware version 8.80.

## Minimum Firmware Version Required on Access Points

Access points with which the workgroup bridge associates must contain firmware version 11.05 or later. The firmware version number appears in the upper-left corner of most access point management screens in the browser interface and at the top of the home (Summary Status) page in the command-line interface.

## Upgrading to a New Firmware Release

### Determining the Firmware Version

The firmware version number appears in the top left corner of the screen in the browser-based management system. To view the browser-based management system, type the device's IP address in the Internet browser address line.

### Upgrade Procedure

Follow these steps to upgrade the firmware in your workgroup bridge:

- 
- Step 1** Use one of the following URLs to find firmware version 8.80  
<http://www.cisco.com/cgi-bin/tablebuild.pl/aironet-340>  
or  
<http://www.cisco.com/cgi-bin/tablebuild.pl/aironet-350>
  - Step 2** Make sure you select the firmware version 8.80 for 340 and 350 series workgroup bridges.
  - Step 3** In the Filename column, click [firmware version 8.80 for workgroup bridges]. Follow the instructions for saving the file to your local drive.
  - Step 4** Use an Internet browser to open the management system on the workgroup bridge. To browse to the management system, type the workgroup bridge's IP address in the browser address line and press **Enter**.
  - Step 5** When the management system opens, click **Allow Config Changes** in the top left corner of the page.

- Step 6** Click **Load** in the Diagnostics column near the top of the page.
- Step 7** In the Value column, click **Browse**. Find the local drive where you saved the new firmware version and select the firmware file.
- Step 8** Click **Send**. The new firmware is loaded and the workgroup bridge reboots.
- 

## New Features

This section describes new features in firmware version 8.80.

### Key Hashing Support

Firmware version 8.8 supports key hashing. When a WEP key is used to encrypt and decrypt transmitted data, each packet includes an initialization vector (IV), a 24-bit field that changes with each packet. The RC4 Key Scheduling Algorithm creates the IV from the base WEP key. A flaw in the WEP implementation of RC4 allows the creation of “weak” IVs that give insight into the base key. A hacker can exploit this flaw by gathering packets encrypted with the same key and using the weak IVs to calculate the base key.

By hashing the base key with the IV to create a new key for each packet, WEP key hashing removes the predictability that an intruder relies on to determine the WEP key by exploiting the IVs. Key hashing is implemented in the radio firmware on both the transmitter and recipient of encrypted packets.

### Message Integrity Check Support

Firmware version 8.80 supports message integrity check (MIC). The use of MIC thwarts an active attack designed to determine the WEP key used to encrypt intercepted packets. This active attack is a combination of a bit-flipping and replay attacks, which proceed as follows:

1. A Hacker intercepts a WEP-encrypted packet.
2. The hacker flips bits in packets and recalculates ICV CRC32.
3. The hacker transmits the bit-flipped frame with known IV to the access point.
4. The access point accepts and forwards the frame because the CRC32 is correct.
5. Layer 3 device rejects the frame and sends a predictable response.
6. The access point encrypts the response and sends it to the hacker.
7. The hacker uses the response to derive the WEP key (stream cipher)

When MIC support is implemented on the root AP of a cell, all associated radio devices in that cell are instructed by the AP to start using MIC when transmitting data. No MIC configuration is required on those devices associated to the root AP. Then each device in that cell transmitting a packet adds a few bytes (the MIC) before encrypting and transmitting that packet. When the recipient receives the packet, it decrypts it and checks the MIC. If the MIC is intact and unmodified, the recipient accepts the packet. If the MIC is not intact and has been modified, the recipient discards the packet.

Because MIC is activated on the access point, not on the client device, there is no effective way to have a MIC “setting” on the workgroup bridge.

## MIC Errors

When MIC is enabled on the root access point in cell, a workgroup bridge produces and displays MIC Failed errors which do not affect the unit's functionality. These MIC errors are produced under the following conditions:

- At initial powerup and association with the root access point
- When using the root access point's HTML interface under the following scenario:
  - If you wait approximately 10 minutes and then browse to the access point's Association screen and click the MAC address of an associated workgroup bridge, a MIC error is generated. This MIC error also appears on associated clients screens.
  - If you wait approximately 10 minutes in the Associations screen. a MIC error is generated when you exit the screen. The MIC error also appears on the associated clients screens.

This situation is believed to be related to the access point code.



**Warning**

**Users should be aware that using MIC may reduce throughput by 80% Therefore, if throughput is an issue, users should consider not activating MIC on an access point that serves workgroup bridges.**

## Support for 802.1x Protocol Draft 10

Firmware version 8.80 uses 802.1x protocol draft 10. If your workgroup bridge uses Extensible Authentication Protocol (EAP) to log onto a network, the access point with which the workgroup bridge associates must use 802.1x protocol draft 10 also.

Table 1 lists firmware versions for Cisco Aironet products and the 802.1x protocol draft with which they comply.

**Table 1 802.1x Protocol Drafts and Compliant Client Firmware**

Firmware Version	Draft 7	Draft 8	Draft 10
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 8.65	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later <sup>1</sup>	—	x	x
AP34x/35x 11.07 and later	—	x	x
AP34x/35x and BR35x 11.08T	—	x	x

1. The default draft setting in access point firmware version 11.06 and later is Draft 10.

Use the Authenticator Configuration page in access point firmware version 11.06 to select the draft of the 802.1x protocol the access point radio should use. Follow these steps to set the draft for your access point:

- 
- Step 1** Browse to the Authenticator Configuration page in the access point management system.
- On the Summary Status page, click **Setup**.
  - On the Setup page, click **Security**.
  - 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 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 use radio firmware versions 4.13, 4.16, or 4.23, or if workgroup bridges associating with this access point use firmware version 8.58 or earlier.
  - Draft 10—This is the default setting in access point and workgroup bridge firmware versions 11.06 and later. Select this option if client devices that associate with this access point or workgroup bridge use Microsoft Windows XP EAP authentication, if LEAP-enabled client devices that associate with this workgroup bridge use radio firmware version 4.25 or later, or if workgroup bridges associating with this access point use firmware version 8.65 or later.
- Step 3** Click **Apply** or **OK** to apply the setting. The access point reboots.
- 

## Installation Notes

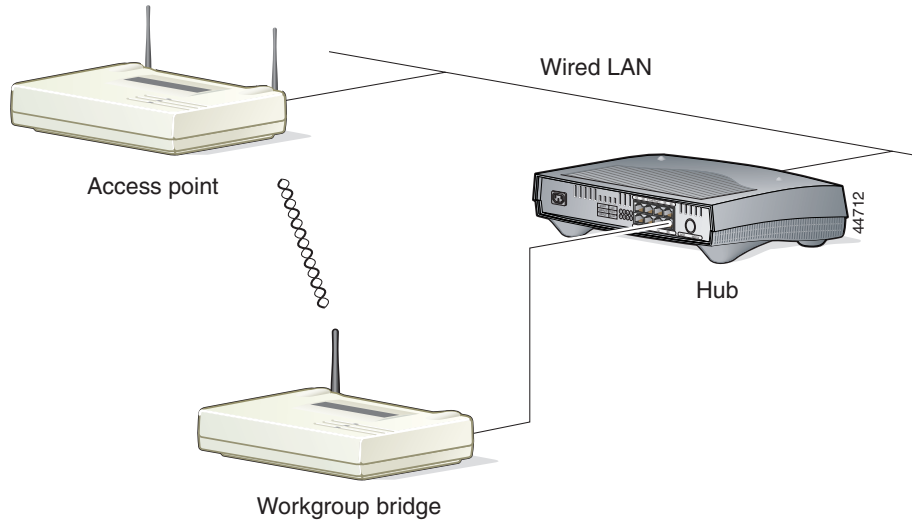
### Verify Mounting Hole Measurement

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.

### Bridge Loop May Occur with Incorrect Network Topology

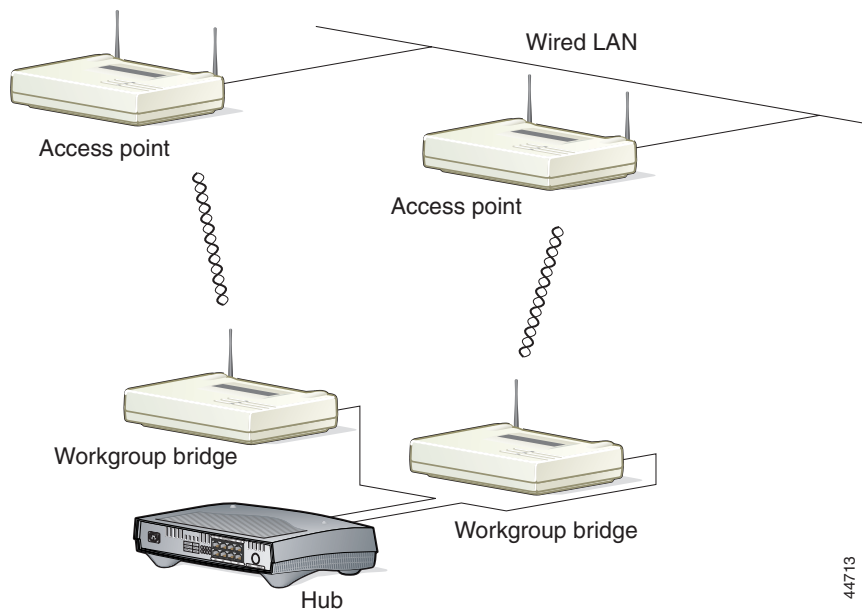
If the workgroup bridge is connected to the wired LAN and is communicating with an access point on the same LAN, a network problem known as a *bridge loop* can occur. Avoid a bridge loop by disconnecting the workgroup bridge from the wired LAN immediately after you configure it. Figure 1 shows the network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

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



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 loop occurs.

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



## Caveats

This section describes open and resolved caveats for firmware version 8.80.

## 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

There are no open caveats associated with version 8.80. However, MIC errors are received under certain conditions that do not affect workgroup bridge functionality. For details, see the “MIC Errors” section on page 4.

## Resolved Caveats

The following caveats were resolved in firmware version 8.80:

- CSCdv07929—Distribute Configuration feature fails to distribute configuration to other units
- CSCdu10993—Cannot access workgroup bridge console menus or ping the device when the workgroup bridge is associated with an access point
- CSCdu811478—The workgroup bridge’s web browser interface prompts you for a password on logout

## 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.

## Documentation Updates

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

### Stale Out Time Setting

The workgroup bridge’s management system includes a Wired LAN stale out time setting on the Configuration>Ethernet page. Use this setting to control the number of seconds 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 unplug the Ethernet cable from the workgroup bridge and plug it back in, the workgroup bridge removes all devices from its association table and re-learns them regardless of the stale out 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

The following sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at the following URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 through an annual subscription.

### Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](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, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the “Leave Feedback” at the bottom of the Cisco Documentation home page.

You can e-mail your comments to [bug-doc@cisco.com](mailto: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:

Cisco Systems  
Attn: Document Resource Connection  
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 by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

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

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.





Copyright © 2001, Cisco Systems, Inc.  
All rights reserved.