



Release Notes for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges Running Firmware Version 12.02T1

March 3, 2003

These release notes describe features and caveats for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges running firmware version 12.02T1.

Contents

- [Introduction, page 2](#)
- [Installation Notes, page 2](#)
- [Limitations and Restrictions, page 3](#)
- [Important Notes, page 6](#)
- [Caveats, page 9](#)
- [Troubleshooting, page 12](#)
- [Related Documentation, page 12](#)
- [Obtaining Documentation, page 13](#)
- [Obtaining Technical Assistance, page 14](#)



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Introduction

A Cisco Aironet Access Point is a wireless LAN transceiver that can act as the connection point between wireless and wired networks or as the center point of a standalone wireless network. Cisco Aironet Bridges are wireless LAN transceivers that connect two or more remote networks into a single LAN.

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.

Installation Notes

You can find the latest release of access point and bridge firmware at this 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 350 series 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 340 or 350 series access point or a 350 series bridge to install firmware version 12.02T1.

Version Supported

Your access point must be running firmware version 10.x or later to install firmware version 12.02T1.
Your bridge must be running version 11.07 or later to install firmware version 12.02T1.

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 > Managing Firmware Configurations > Updating Firmware
3. Follow this link to the Software Center on Cisco.com and download firmware version 12.02T1:
<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 chapter 6 in the *Cisco Aironet Access Point Software Configuration Guide* for more information.

Limitations and Restrictions

This section describes limitations and restrictions for 340 and 350 series access points and 350 series bridges.

Cisco Aironet 350 Series Bridges Incompatible with 340 Series Bridges

Cisco Aironet 340 and 350 Series Bridges can be connected to the same LAN segments, but they cannot communicate wirelessly. Although you can disable STP on non-root 350 series bridges, 350 and 340 series bridges are not designed to interoperate. If you use both 340 and 350 series bridges on your network, make sure the 340 series bridges have radio bridge links only to other 340 series bridges, and that 350 series bridges have radio bridge links only to other 350 series bridges.

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 steady 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 should try to reset the unit to factory defaults using the **:resetall** command in the CLI; see chapter 9 of the *Cisco Aironet Access Point Software Configuration Guide* for instructions on resetting the access point. If the unit cannot be reset to defaults, 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 steady green, meaning that the access point is beginning to update the firmware.
2. The middle indicator is steady 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, 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	802.1x-2001
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	—	x	x
AP34x/35x 11.07 and later	—	x	x
AP34x/35x and BR35x 11.21 through 12.02T1	—	x	x



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 11.06 or later 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.

- 802.1x-2001 (formerly 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.

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 and broadcast 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. When you set up a non-root bridge or repeater access point to authenticate as a LEAP client, the bridge or repeater derives a dynamic WEP key and uses it to communicate with the root bridge or access point. Bridges and repeaters not set up for LEAP authentication use static WEP keys when communicating with other bridges and access points.



Note

If you do not use EAP authentication on your wireless network, you can select any WEP key as the transmit key. If you use EAP authentication and you enable broadcast key rotation, you can enable WEP without entering WEP keys.

Important Notes

This section lists important information about access points and bridges running firmware version 12.02T1.

Reboot of Workgroup Bridges Required When Allowing More Than 20

With firmware version 12.02T1, you can select **no** for the *Classify Workgroup Bridges as Network Infrastructure* setting on the AP/Root Radio Advanced page to allow up to 50 workgroup bridges to associate to the access point or bridge. After selecting **no** for this setting, you must reboot workgroup bridges associated to the access point or bridge.

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.

Adding or Deleting Proxy Mobile IP AAPs

If you need to add or delete proxy Mobile IP authoritative access points, you must disable proxy Mobile IP before changing the configuration. Follow these steps.

-
- | | |
|---------------|---|
| Step 1 | Browse to the Setup page. |
| Step 2 | In the Services section, click Proxy Mobile IP . The Proxy Mobile IP Setup page appears. |
| Step 3 | Click General . The Proxy Mobile IP General page appears. |
| Step 4 | Change the Enable Proxy Mobile IP setting to no . |
| Step 5 | Add or delete AAPs as necessary. |
| Step 6 | Change the Enable Proxy Mobile IP setting to yes . |
-

Unexpected Results on Lost Ethernet

When backbone connectivity is lost on an access point running version 12.02T1, the device switches to repeater mode. Switch to Repeater mode is the default setting for this condition. Therefore, if the access point's role in your network is not a repeater access point, make sure you connect it to your wired network before booting it up. If you do not connect the access point to your network, it switches to the repeater mode when it fails to detect the presence of an Ethernet connection. When this occurs, wireless client devices are unable to connect and you cannot correct the problem using a wireless client. The only way you can change the configuration is through a serial connection using the access point's command line interface.

Centralized Authentication Administration System Flow Notes

The following information briefly explains the flow between the access point and its authentication server. This information was inadvertently omitted from the *Cisco Aironet 340 and 350 Series Access Point Software Configuration Guide*.

- The authentication server is initialized to listen for socket requests on the predetermined UDP or TCP ports specified on the Authenticator Configuration page (UDP 1812 for RADIUS servers or TCP 49 for TACAS+ servers).
- The authentication server must be preconfigured with valid usernames and passwords and the shared secret key the server uses for secure authentication between it and the access point.
- No remote server authentication is possible with a new access point unless it has been configured by the user.
- The access point requires the following parameters to access the remote authentication servers, which were described in the procedure above:
 - Remote server authentication—accomplished by configuring or not configuring the authentication server to send requests
 - IP address of the authentication server(s)
 - Secret key to be shared with the authentication server(s)
 - Selection of RADIUS or TACACS+ server indication

- Default UDP or TCP port ID used for authentication
- Timeout value while waiting for a server response

The administrator attempts to log in to the access point using any HTML capable browser on a wireless or wired network. The access point receives the authentication request and checks the local database of users to verify that the request is accompanied by a valid username and password.

If the user is not found on the local list, or if local authentication fails (user found, but incorrect password), the access point determines whether a remote authentication server is configured to handle authentication requests. If it is, the access point sends an authentication request to the first remote authentication server and waits for the server to reply or timeout. This asynchronous request is sent to either a TACACS + or RADIUS server using a client interface and protocol appropriate for the target server. The password for the administrator requesting authentication is encrypted using an MD5 hash function and sent to the server. The password is never sent to the server in clear text.

If the server does not respond, a timeout occurs prompting the access point to check for an additional configured authentication server. If it finds a server, the access point sends an authentication request to that server. Additional servers are contacted until one of the following events occurs:

- A configured server responds accepting or rejecting the request.
- A final timeout occurs on the last configured server.

When the authentication server responds to a successful request, the authorization parameters (described in the Authorization Parameters section below) are extracted and processed to a local database cache entry. This entry is kept in the cache for five minutes and is used to authenticate the user for subsequent authentication requests.

The cache speeds up the administrative configuration process by not forcing the subsequent requests to require a transaction with an authentication server within the five-minute time period. The following applies:

- If the user is accessed using an authentication request within the 5-minute period, the cache timer resets to 5 minutes.
- If the user entry is not accessed within 5 minutes, the next access causes a new server request to be sent to the authentication server so the user and new privileges are cached again.

If the authentication response is a rejection, the server issues a reject response just as if the local database entry was not found. The administrator is also rejected if they exist on the authentication server but do not have administrative capabilities configured.

Authorization Parameters

The following authentication server attribute value (AV) pair is returned to the access point for an administrator login request:

```
This is RADIUS attribute #26, Cisco Vendor ID #9, type #1 --- string.
```

```
Cisco:Avpair = aironet:admin-capability=write+snmp+ident+firmware+admin
```

Any combination of capabilities are returned with this attribute; for example:

```
Cisco:Avpair = aironet:admin-capability=ident+admin
```

```
Cisco:Avpair = aironet:admin-capability=admin
```

The following is an example Livingston RADIUS server users file entry:

```
User password = "aironet"
  Service-Type = Outbound
  cisco-avpair = "aironet:admin-capability=ident+admin"
```

The following is an example TACACS + server users file entry:

```
Service - Aironet
Protocol - Shell
cisco-avpair = "aironet:admin-capability=ident+admin"
```

See Chapter 8 of the *Cisco Aironet 340 and 350 Access Point Software Configuration Guide* or click **Help** on the Authenticator Configuration page for an explanation of the attributes returned by the server.

Caveats

This section lists open and resolved software issues in firmware version 12.02T1.

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/>.

Open Caveats

The following caveats have not been resolved for firmware version 12.02T1:

- CSCdz04380—Incorrect values are advertised for CWMin and CWMax on Voice VLAN.

When a voice VLAN using Cisco IP Phones is configured with default settings (CSMin=31, CWMax=31), the values advertised by the access point in the beacons and probes are CWMin=7 and CWMax=255.

There is no workaround for this caveat.

- CSCdz04708—Early 340 series access points are incompatible with VLAN tagging. Early versions of the 340 series access point are able to set up VLANs, but clients on non-native VLANs will be unable to transmit and receive large packets. The reason for this is because early 340 series access points were limited to a maximum packet data length of 1500 bytes.

You can identify an affected access point by browsing to the Ethernet Identification page and checking the Maximum Packet Data Length parameter. If it is 1500, the failure will occur.

Possible workaround—If you have an early 340 series access point on your network, you can eliminate the problem by setting the Maximum Packet Data Length parameter for all other devices to 1400 bytes.

- CSCdy10787—The access point aborts any configuration containing an unknown MIB variable.

When an access point receives a configuration from another access point that is running a newer firmware version than the receiving access point, the receiving access point aborts the configuration if it encounters a MIB variable that it does not recognize.

Workaround: Upgrade access points to the same firmware version before distributing configurations.

- CSCdy11906—When WEP is enabled and you set all WEP keys to **not set**, WEP is still enabled but the web-browser page indicates that WEP is disabled.

Workaround: To disable WEP, select **no encryption** from the *Use of Data Encryption by Stations* is drop-down menu on the Radio Data Encryption page.

- CSCin18914—IP release or renew not occurring with EAP-TLS+MIC+KH+BWR.

When a client associates with EAP-TLS + 40/128 bit broadcast key + MIC + Keyhash + Broadcast WEP key rotation (10sec), and IP DHCP **release** and **renew** commands are issued, the client releases the IP address, never receives it again, and remains EAP authenticated. A ping from the access point to the client appears to succeed, but does not reveal an IP address. The access point association table shows the IP address for the client as 0.0.0.0.

- CSCdy27831—When you set the default Unicast Address Filter to disallowed, you must reboot the access point for the setting to take effect.
- CSCdy29556—Symbol IP phone continuously associates and authenticates to an access point configured with multiple VLANs.

When a Symbol IP phone is associated to a VoIP VLAN (Symbol extensions enabled), the phone associates to the access point and is authenticated approximately every 2 seconds. The Symbol phone shows a “No Network” error every 1 to 2 minutes.

It also appears that Symbol phones do not work well when using a non-primary SSID. It is possible that the phone does not perform an active probe and therefore does not detect information about the SSID it associated with in the beacon, causing it to reassociate and re-authenticate.

There is no workaround for this caveat.

- CSCdz32333—Repeater bridge link intermittent with LEAP client on non-native VLAN.

An intermittent drop occurs in a bridge link between a root bridge and a non-root bridge acting as a repeater or non-root device. The drop occurs when a client LEAP authenticates and associates with the non-root bridge that is acting as a repeater or non-root device. When the client associates to an SSID that is mapped to the non-native VLAN on the non-root bridge, it subsequently brings down the bridge link between the root and the non-root that is LEAP authenticated as well. The condition is intermittent and does not seem to occur if the VLAN is not enabled or if the client is associated to the root bridge or is using open or WEP authentication to the non-root bridge.

There is no workaround for this caveat.

- CSCdz43069—Symbol phone not working when multicast or FTP traffic is passed.

If an FTP or multicast session is in progress during a Symbol phone session, the phone call may be dropped and the phone may be unable to roam between subnets. If there are no FTP or multicast sessions in progress, the Symbol phone operates normally and is able to roam between subnets.

Workaround: Limit multicast and FTP traffic if using Symbol phones in a proxy Mobile IP environment.

- CSCdz48575—Default lost Ethernet action not appropriate.

See the [“Unexpected Results on Lost Ethernet” section on page 7](#) for a complete explanation of this caveat.

- CSCdz50218—Access point does not update home or foreign agent status when advertisement flags change.

When a local home or foreign agent is disabled on the router, the access point does not detect the change from the the advertisement flags it receives. The access point continues to list the agent addresses on the Statistics page.

Workaround: Disable then enable proxy Mobile IP.

- CSCdz58192—Root bridges with LEAP enabled on the native VLAN must have the security setting matching that set on the Advanced Radio Setup page. If the settings do not match, the bridge link will go down temporarily whenever an infrastructure device authenticates.
- CSCdy73695—When a repeater access point receives packets from a root access point while the repeater is attempting to associate, the repeater sometimes displays this error:

```
00:00:10 (Warning): Station <Root MAC address> Associated with Encryption, then
attempted to send an Unencrypted packet to <Repeater MAC address> (length 74)
```

The error occurs when WEP is not enabled on either the root or the repeater. When an association response is received by the repeater, it no longer displays the error message and is able to successfully pass data. However, if a significant amount of traffic, such as multicast traffic, is being transmitted by the root access point while the repeater is attempting to associate, the repeater may miss the association response from the root access point and never fully associate. In this case, the root access point reports that the repeater is associated and the repeater reports that it is only authenticated. The repeater continues to display warning messages about receiving unencrypted packets and does not recover until it is rebooted.

- CSCdy76093—Proxy Mobile IP with multiple authoritative access points continuously sends update packets.

See the [“Adding or Deleting Proxy Mobile IP AAPs” section on page 7](#) for details and procedures to correct this problem.

- CSCdx81372—Access point does not accept version 11.21-generated .ini file.

If you download the full configuration .ini from an access point running 11.21, upgrade to version 12.02T1, and then attempt to download the .ini file from an FTP server, the following error message displays:

```
*** No Such MIB Variable as Specified on Initialization File Line xxx! for the
following variables:
awcAaaServerAccountingEnabled.x,
awcVoIPvlanId, awcVoIPvlanEnabled,
awcPublicVlanId.
*** Bad Value for MIB Variable awcVlanEncapMode Specified on Initialization File Line
xxx (error 13)!
```

Workaround—When producing .ini files, dump a non-default configuration for version 11.21 instead of a full configuration.

- CSCdw89705—All Ethernet devices behind a client bridge show up as roamed.

When a non-root bridge roams from one root bridge to another, messages might appear in the logs of the root bridges stating that Ethernet devices connected to the non-root bridge and wireless client devices associated to the non-root bridge have roamed.

You can ignore these messages.

Resolved Caveats

The following caveats are resolved in version 12.02T1:

- CSCdz24966—Broadcast key rotation operates correctly with 350 client.
- CSCdz28380—One broadcast key is sent at rotation time when two radios are operating.
- CSCdz42150—Duplicate detection logic changed.
- CSCdz50475—Access point no longer loses WEP keys when hot standby is configured.
- CSCdz55839—DHCP no longer fails after first broadcast WEP key rotation.
- CSCdx80069—Access point buffers traffic correctly in power saving mode.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac>. In the Tools and Utilities section, Select **Wireless Troubleshooting Center**. The Wireless Troubleshooting Center page appears. Choose the link that best suits your troubleshooting needs.

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*
- *Quick Start Guide: Cisco Aironet 350 Series Bridges*
- *Cisco Aironet 350 Series Bridge Hardware Installation Guide*
- *Cisco Aironet 350 Series Bridge Software Configuration Guide*
- *Cisco IOS Solutions Configuration Guide, Version xx.x*
- *Cisco IOS Quality of Service Solutions Command Reference, Version xx.x*
- *Cisco IOS Switching Services Configuration Guide*
- *Cisco Internetworking Design Guide*
- *Cisco Internetworking Technology Handbook*
- *Cisco Internetworking Troubleshooting Guide*

Obtaining Documentation

These 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 this URL:

<http://www.cisco.com>

Translated documentation is available at this URL:

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

You can order Cisco documentation in these 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
- 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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing 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 online 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 with these tasks:

- 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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

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

Cisco TAC inquiries 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.

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

Cisco TAC Web Site

You can use the Cisco TAC Web Site 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 this URL:

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

All customers, partners, and resellers who have a valid Cisco service 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 this URL to register:

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. 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 automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this 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). When you call the center, please have available your service agreement number and your product serial number.

This document is to be used in conjunction 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 © 2003 Cisco Systems, Inc.
All rights reserved.