



Release Notes for Cisco Aironet 1200 Series Access Points Running VxWorks Firmware Version 12.05

September 27, 2004

These release notes describe caveats for Cisco Aironet 1200 Series Access Points running VxWorks firmware version 12.05. This release note also contains important information about the device.

Contents

- [Introduction, page 2](#)
- [Installation Notes, page 2](#)
- [Limitations and Restrictions, page 5](#)
- [Important Notes, page 8](#)
- [Caveats, page 11](#)
- [Troubleshooting, page 13](#)
- [Related Documentation, page 13](#)
- [Obtaining Documentation, page 13](#)
- [Obtaining Technical Assistance, page 15](#)



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

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

Introduction

Cisco Aironet Access Points are wireless LAN transceivers that can act as the connection point between wireless and wired networks or as the center point of a standalone wireless network. In large installations, the roaming functionality provided by multiple access points enables wireless users to move freely throughout a facility while maintaining uninterrupted access to the network.

Your 1200 series access point can contain two radios: a 2.4-GHz radio in an internal mini-PCI slot and a 5-GHz radio module in an external, modified cardbus slot. The access point supports only one radio of each type. You can configure the radios separately using different settings on each radio.

The access point uses a browser-based management system, but you can also configure the access point using a terminal emulator, a Telnet session, or Simple Network Management Protocol (SNMP).

Installation Notes

You can find the latest release of access point firmware at this URL:

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

Installation in Environmental Air Space

The 1200 series access points are suitable for use in environmental air space in accordance with Section 300-22(c) of the *National Electrical Code*.

**Note**

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

**Caution**

The Cisco Aironet Power Injector has a smaller operating temperature range (32 to 104°F; 0 to 40°C) than the 1200 series 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 install the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death.

Power Considerations

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



Caution

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



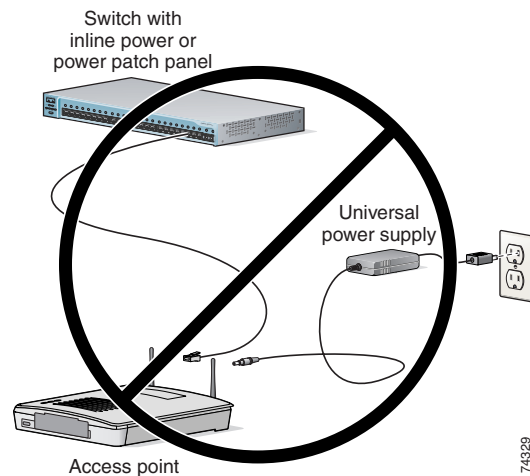
Caution

Cisco Aironet Power Injectors are designed for use with 1200 series access points only. *Do not use the power injector with any other Ethernet-ready device.* Using the power injector with other Ethernet-ready devices can damage the equipment.

Use Only One Power Option

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

Figure 1 Improper Power Configuration Using Two Power Sources



Operating 5-GHz Radio Requires Power Injector or Power Module

Only the 1200 series power injector and the 1200 series power module can support operation of the 5-GHz radio in the access point. Currently, switches with inline power and power patch panels do not provide enough power for operation of the 5-GHz radio.

Access Point Requires 1200 Series Universal Power Supply and Power Injector

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

System Requirements

You must have a 1200 series access point to install firmware VxWorks version 12.05.

Version Supported

Your access point must be running VxWorks firmware version 11.40T or later to install VxWorks firmware version 12.05.

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.

Upgrade Procedure

Follow these steps to install access point firmware:

- Step 1** Follow this link to the Software Center on Cisco.com and download VxWorks firmware version 12.05:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
- Step 2** Select **Option #1: Aironet Wireless Software Selector**. The Aironet Wireless Software Selector window appears.
- Step 3** Click the drop-down menu to view the valid values for the Product Type field.
- Step 4** Click **Access Point**.
- Step 5** Click **Submit**. The Step 2 of 3 page appears.
- Step 6** Click the drop-down menu to view the valid values in the Model Number field.
- Step 7** Click **1200 Series: VxWorks Software for Aironet 1200 (802.11a/802.11b)**.
- Step 8** Click **Submit**. The Step 3 of 3 page appears.
- Step 9** To download the current release, click the **(VxWorks Software for Aironet 1200) Release 12.05 with Cisco Wireless Security Suite** radio button.
- Step 10** Click **Submit**. The software selector displays the categories you selected and lists the available download methods.
- Step 11** Review your selections. If you want to change anything, use your browser's back button to return to the previous software selector page.

- Step 12** When you are ready to download the firmware, go to the Standard Installation section and click **Access Point Bundle**. The Aironet Software Selector encryption authorization form appears.
- Step 13** Complete the required fields on the authorization form and check the boxes indicating agreement with the download agreement.
- Step 14** Type your name exactly as you entered it in the First Name and Last Name fields.
- Step 15** Click **Submit**. The Software Download Software License Agreement page appears.
- Step 16** Review the license agreement and click **Accept**. The File Download window appears.
- Step 17** Click **Save** and select a location at which to save the file.

**Note**

To upgrade firmware from a file server, you must enter settings on the access point's FTP Server Setup page. Refer to Chapter 10 in the *Cisco Aironet 1200 Series Access Point Software Configuration Guide* for more information.

Limitations and Restrictions

This section describes limitations and restrictions for 1200 series access points.

Removing Power During Firmware Update Can Corrupt Radio Firmware

When you update the firmware on an access point, allow the unit to finish its start-up sequence before removing power.

**Caution**

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) is red continuously, and the following error message appears when the access point starts up:

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

The access point should recover from this error automatically.

You can safely shut off 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 continuously green, meaning that the access point is beginning to update the firmware.
2. The middle indicator is continuously green and the top and bottom indicators are off, indicating that the access point is updating the radio firmware.

When the middle indicator blinks or the top and bottom indicators blink, you can shut off 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 version 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 and later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later ¹	—	x	x
AP34x/35x 11.07 and later	—	x	x
AP12xx 11.40T and later	—	x	x

1. The default draft setting in access point VxWorks firmware version 11.06 and later is 802.1x-2001.

Use the Authenticator Configuration page to select the draft of the 802.1x protocol the access point 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:

- 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) drop-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.
 - 802.1x-2001 (formerly Draft 10)—This is the default setting. Select this option if client devices that associate with this access point use Microsoft Windows XP EAP authentication or if LEAP-enabled client devices that associate with this access point use radio firmware version 4.25 or later.
- Step 3** Click **Apply** or **OK** to apply the setting. The access point 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 AP Radio Data Encryption page. The access point 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 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 uses a dynamic WEP key to encrypt unicast messages to EAP-enabled clients. When you set up a repeater access point to authenticate as a LEAP client, the repeater derives a dynamic WEP key and uses it to communicate with the root access point. Repeaters not set up for LEAP authentication use static WEP keys when communicating with other 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.

MIB File Compatible with VxWorks Firmware Version 11.00 and Later

The access point MIB file (AWCVX-MIB) is supported only by access point VxWorks 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>.

Hot Standby Mode and Radio Diagnostics Availability

The hot standby feature is available on dual mode access points. To make the feature operational, both radios must be set to the hot standby mode.

The Carrier Test and Antenna Alignment radio diagnostics tool are available only for an access point's 2.4-GHz radio.

Important Notes

This section lists important information about access points running VxWorks firmware version 12.05.

SQL Worm Virus Vulnerability

In certain situations, the access point could be affected by the SQL Worm virus. The signature of this worm appears as high volumes of UDP traffic to port 1434. Symptoms on Cisco devices include but are not limited to high CPU usage and traffic drops on the input interfaces.

The worm has been referenced by several names including *Slammer*, *Sapphire*, and *MS SQL*.

Cisco has prepared a security notice containing details about this virus and how to eliminate it. The document is on Cisco.com at the following link:

<http://www.cisco.com/warp/public/707/cisco-sn-20030125-worm.shtml>

Cisco Aironet Software Requires Completion of Encryption Authorization Form

In order to access Cisco Aironet software from the Software Center on Cisco.com, you must now fill out a form to receive authorization to download encrypted software. Registered Cisco.com users are required to fill out the form only once, but 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 located at the following URL:

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

Adding or Deleting Proxy Mobile IP AAPs

If you need to add or delete proxy Mobile IP authoritative access points (AAPs), 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**.
-

Error Message Appears for Access Points with One Radio

When you install VxWorks firmware version 12.05 in an access point with one radio, an error message appears. If your access point contains only the internal 2.4-GHz radio, this error message appears:

```
** Failed to Load Driver for device entry #3.
```

If your access point contains only the external 5-GHz radio, this error message appears:

```
** Failed to Load Driver for device entry #2.
```

You can ignore these messages. The errors do not appear if your access point contains two radios.

Installing a 5-GHz Radio May Require Updating Firmware

If you upgrade a 2.4-GHz access point by adding a 5-GHz radio module, you must ensure that the firmware is updated prior to installing the radio, otherwise the access point fails to recognize the new radio. In order to install the 5-GHz radio module, the access point must be running VxWorks version 11.54T or later in a VxWorks-based access point or IOS Release 12.2(8)JA or later in an IOS-based access point.

Enabling Broadcast Key Rotation on One Radio Enables It on Both Radios

If you enable Broadcast Key Rotation on one of the radios in a dual-radio access point, Broadcast Key Rotation is automatically enabled on the other radio.

Set Flow Control to None or Xon/Xoff When Using Terminal Emulator

The terminal emulator flow control setting for 1200 series access points (**none** or **Xon/Xoff**) differs from the flow control setting for 340 and 350 series access points (**none**, **Xon/Xoff**, or **Hardware**).

To use a terminal emulator to open the 1200 series access point's command-line interface (CLI), use these settings for the terminal emulator connection:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- No flow control or Xon/Xoff

Reboot of Workgroup Bridges Required When Allowing More Than 20

With VxWorks firmware version 12.05, you can select **no** for the Classify Workgroup Bridges as Network Infrastructure setting on the AP/Root Radio Advanced page to allow up to 20 workgroup bridges to associate to the access point. When you select **no** for this setting, you must reboot workgroup bridges associated to the access point.

The “Reliable multicast messages from the access point to workgroup bridges” setting limits reliable delivery of multicast messages to approximately 20 Cisco Aironet Workgroup Bridges that are associated to the access point. The default setting, *disabled*, reduces the reliability of multicast delivery to allow more workgroup bridges to associate to the access point.

Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

The performance cost of reliable multicast delivery—duplication of each multicast packet sent to each workgroup bridge—limits the number of infrastructure devices, including workgroup bridges, that can associate to the access point. To increase beyond 20 the number of workgroup bridges that can maintain a radio link to the access point, the access point must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the access point cannot confirm whether multicast packets reach the intended workgroup bridge, so workgroup bridges at the edge of the access point's coverage area might lose IP connectivity. When you treat workgroup bridges as client devices, you increase performance but reduce reliability.

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 relevant interfaces by default. However, if you disable CDP for one of the individual interfaces, the access point re-enables CDP for that interface when it reboots. If you disable CDP completely, the access point does not re-enable CDP on reboot.

Symbol IP Phone Issues

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 authenticate.

Symbol phones may disconnect and be unable to roam between subnets when the access point passes multicast or FTP traffic. If there are no FTP or multicast sessions in progress the Symbol phone operates normally and is able to roam between subnets. To work around this issue, limit multicast and FTP traffic if you are using Symbol IP phones in a proxy Mobile IP environment.

Caveats

This section lists resolved and open software issues in VxWorks firmware version 12.05.

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 VxWorks firmware version 12.05:

- CSCdz30285—The *Configuring the Cisco Wireless Security Suite* application note is incorrect. The screen capture in section 3.1 of this document shows Add AAA Server, which is incorrect as the Aironet device is a client of the ACS, not a server.
Workaround: Call the TAC for setup instructions.
- CSCdy49857—VxWorks event descriptions in documentation are incomplete. Events displayed on the Event Log page are not described in the software configuration guides for 350 and 1200 series devices.
- CSCea66593—Access point reboots sporadically because of a protection violation in tRcv_awc0. Reboots can occur within a 2 to 3 hour period or remain on line for several days and occur based on a protection violation of data accessed associated with task tRcv_awc0. There is no workaround for this caveat.
- CSCef74550—802.11b clients start reauthentication when an 802.11a client is configured. When a user makes a change to the 802.11a radio, the 802.11b radio reauthenticates. There is no workaround for this caveat.

Resolved Caveats

The following caveats are resolved in VxWorks firmware version 12.05:

- CSCec84851—Unexpected packet errors no longer occur during EAP process.
- CSCee22526—TCP stack has been improved to eliminate TCP vulnerabilities.
- CSCee00894—Non-Cisco clients no longer remain in the access point association table after disassociating.
- CSCef23633—The access point no longer locks up and reboots during certain VLAN configuration changes.

Other Caveats

The following is a status of caveats published in the release notes for previous VxWorks versions that were not resolved in version 12.05:

- CSCdz04380—Incorrect values are advertised for CWMin and CWMax on Voice VLAN.
This caveat is postponed. The issue is to be resolved in a future maintenance release for VxWorks access points and will advertise the CWMin and CWMax values as defined by IEEE 802.11e.
- 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.
This caveat is closed. Disable encryption by changing the WEP setting instead of removing the key.
- CSCdy20169—The access point sometimes displays a warning message when booted.
This caveat is a duplicate of CSCdy72691, which was resolved in an early version.
- CSCdy27831—Access point must be rebooted after setting Ethernet Unicast Filter to disallowed.
This caveat is closed.
- CSCdy29556—Symbol IP phone continuously associates and authenticates to an access point configured with multiple VLANs.
This caveat is closed. See “[Symbol IP Phone Issues](#)” section on page 10 for additional information.
- CSCea39261—SQL Worm virus vulnerability affects access point.
Follow the instructions in the Cisco Security Notice at this link to reduce your vulnerability:
<http://www.cisco.com/warp/public/707/cisco-sn-20030125-worm.shtml>
Follow the instructions in the “[SQL Worm Virus Vulnerability](#)” section on page 8.
- CSCdz43069—Symbol phone not working when multicast or FTP traffic is passed.
This caveat is closed. See “[Symbol IP Phone Issues](#)” section on page 10 for additional information.
- CSCdy73695—An error is displayed when a repeater access point receives packets from a root access point while attempting to associate.
This caveat is closed due to lack of severity.
- CSCdy76093—Proxy Mobile IP with multiple authoritative access points continuously sends update packets.
This caveat is closed.
- CSCdx35804—RADIUS attributes in documentation is incomplete or inaccurate.
This caveat is being investigated.
- CSCdw89705—All Ethernet devices behind a client bridge show up as roamed.
This caveat is closed. No further action is planned.
- CSCea49176—PEAP requires users to change password results in failed logon.
Cisco has been unable to reproduce this caveat.
- CSCin46049—Client is always forced to EAP-associate with multiple VLANs.
This defect is unreproducible and has been archived.
- CSCin45850—A valid access point is not reporting a rogue access point in its logs when an invalid RADIUS server IP address is used in the rogue AP.
This caveat is closed.

- CSCin46851—After roaming from its home network to the foreign network, the mobile node fails to reach the home or foreign agent but associates to the authoritative access point on the foreign network. The mobile node must fully reauthenticate to reach the entire network.

This caveat is unreproducible and has been archived.

Troubleshooting

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

Related Documentation

Use the following documents with this document:

- *Quick Start Guide: Cisco Aironet 1200 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1200 Series Access Point Radio Upgrade Instructions*
- *Cisco Aironet 1200 Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1200 Series Access Point Software Configuration Guide*
- *Cisco IOS Solutions Configuration Guide*
- *Cisco IOS Quality of Service Solutions Command Reference*
- *Cisco IOS Switching Services Configuration Guide*

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

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

Documentation CD-ROM

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

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

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/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, 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. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments 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

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com 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

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

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: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing 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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, 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 website. Some services on the Cisco TAC website require 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://tools.cisco.com/RPF/register/register.do>

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

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

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 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.

Obtaining Additional Publications and Information

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

- 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://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. 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/go/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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

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