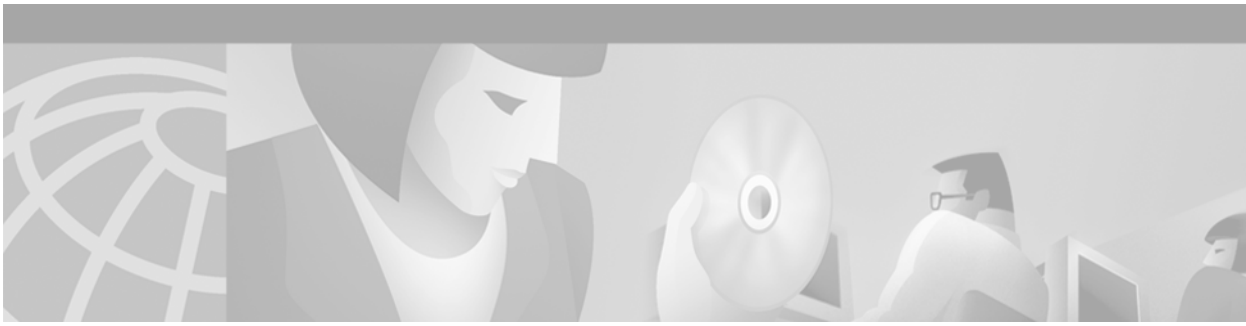

Release Notes for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges

February 16, 2002

These release notes describe features and caveats for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges running firmware version 11.10T1. Firmware version 11.10T1 fixes these defects: CSCdw63011, CSCdw63031, and CSCdw63032.

Contents

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

Introduction

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

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.

Access point and bridge firmware version 11.10T1 fixes defects CSCdw63011, CSCdw63031, and CSCdw63032.

New Features

This section describes new features introduced in firmware version 11.10T. These features are also included in firmware version 11.10T1.

Prevent Attacks on WEP with Enhanced Security

Three new security features prevent sophisticated attacks on your wireless network's WEP keys:

- Message Integrity Check (MIC)—MIC prevents attacks on encrypted packets called bit-flip attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on both the access point or bridge and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof. Click this link for instructions on enabling MIC:

  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350ch4.htm#xtocid10

- Temporal Key Integrity Protocol (TKIP)—Also known as WEP key hashing, this feature defends against an attack on WEP in which the intruder uses the initialization vector (IV) in encrypted packets to calculate the WEP key. WEP key hashing removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. Click this link for instructions on enabling key hashing:

  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350ch4.htm#xtocid11

- Broadcast key rotation—EAP authentication provides dynamic unicast WEP keys for client devices but uses static broadcast, or multicast, keys. When you enable broadcast WEP key rotation, the access point or bridge provides a dynamic broadcast WEP key and changes it at the interval you select. Click this link for instructions on enabling broadcast key rotation:

  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350ch4.htm#xtocid12

Note To use these security features, you must upgrade client devices associated to the access point or bridge to these software versions: Aironet Client Utility version 5.0x, PC card driver version 8.0x for Microsoft Windows , and radio firmware version 4.25.23 or later.

Use RADIUS Accounting to Collect Wireless Network Statistics

Enable accounting on the access point or bridge to send network accounting information about wireless client devices to a RADIUS server on your network. See the "Enabling Wireless Network Accounting" section on page 5-16 of the *Cisco Aironet Access Point Software Configuration Guide* for instructions on enabling accounting.

Use EAP to Authenticate Repeater Access Points and Non-Root Bridges

Set up repeater access points and non-root bridges to authenticate to your network like other wireless client devices. After you provide a network username and password for the repeater or bridge, it authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys. Click this link for instructions on setting up a repeater access point:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350ch4.htm#xtocid18

Click this link for instructions on setting up a non-root bridge:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350brdgs/brscg/br350ch4.htm#xtocid18

Installation Notes

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

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

Installation in Environmental Air Space

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

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

Antenna Installation

For instructions on the proper installation and grounding of external antennas, refer to the National Fire Protection Association's *NFPA 70, National Electrical Code,* Article 810, and the Canadian Standards Association's *Canadian Electrical Code,* Section 54.

Warning **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death.**

Power Considerations

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

Caution Cisco Aironet power injectors are designed for use with 350 series access points and 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 11.10T1.

Version Supported

Your access point must be running firmware version 10.x or later to install firmware version 11.10T1. Your bridge must be running version 11.07 or later to install firmware version 11.10T1.

Upgrading to a New Firmware Release

Determining the Firmware Version

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

Upgrade Procedure

For instructions on installing access point and bridge firmware:

1. Follow this link to the Cisco Aironet documentation home page:

   http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm

2. Follow this path to the product, document, and chapter:
   Aironet 350 Series Wireless LAN Products > Cisco Aironet 350 Series Access Points > Cisco Aironet Access Point Software Configuration Guide > Maintaining Firmware > Updating Firmware

3. Follow this link to the Software Center on Cisco.com and download firmware version 11.10T1:

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

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

Limitations and Restrictions

Removing Power During Firmware Update Can Corrupt Radio Firmware

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

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

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

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

1. All three indicators are 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, then the access point should be configured to use Draft 8 of the 802.1x protocol. Table 1 lists firmware versions for Cisco Aironet products and the draft with which they comply.

Table 1 802.1x Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	Draft 10[1]
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—

Table 1 802.1x Protocol Drafts and Compliant Client Firmware (continued)

Firmware Version	Draft 7	Draft 8	Draft 10[1]
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 or later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later[2]	—	x	x
AP34x/35x 11.07 and later	—	x	x
AP34x/35x and BR35x 11.10T1	—	x	x

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

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

Use the Authenticator Configuration page in firmware version 11.10T1 to select the draft of the 802.1x protocol the access point or bridge radio should use. Follow these steps to set the draft for your access point or bridge:

Step 1 Browse to the Authenticator Configuration page in the access point management system.

a. On the Summary Status page, click **Setup**.

b. On the Setup page, click **Security**.

c. On the Security Setup page, click **Authentication Server**.

Step 2 Use the 802.1x Protocol Version (for EAP authentication) pull-down menu to select the draft of the 802.1x protocol the access point or bridge radio should use. Menu options include:

- Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.
- Draft 8—Select this option if LEAP-enabled client devices that associate with this access point or bridge use radio firmware versions 4.13, 4.16, or 4.23.
- Draft 10—This is the default setting in firmware versions 11.06 and later. Select this option if client devices that associate with this access point or bridge use Microsoft Windows XP EAP authentication or if LEAP-enabled client devices that associate with this access point or bridge use radio firmware version 4.25 or later. The functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1x standard.

Step 3 Click **Apply** or **OK** to apply the setting. The access point or bridge reboots.

Select WEP Key 1 as Transmit Key for EAP Authentication

If you use Network-EAP as the authentication type on your wireless network, you must select key 1 as the transmit key on the access point or bridge AP Radio Data Encryption page. The access point or bridge uses the WEP key you enter in key slot 1 to encrypt multicast 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.

MIB File Compatible with Firmware Version 11.00 and Later

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

Important Notes

This section lists important information about access points and bridges running firmware version 11.10T1.

Cisco Discovery Protocol Re-Enabled for Individual Interfaces on Reboot

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

Caveats

This section lists resolved and open software issues in firmware version 11.10T1.

Getting Bug Information on Cisco.com

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

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

Resolved Caveats

The following caveats have been resolved in firmware version 11.10T1:

- Resolved: CSCdw63011--An error can occur with management protocol processing. Please use this URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw63011

- Resolved: CSCdw63031--An error can occur with management protocol processing. Please use this URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw63031

- Resolved: CSCdw63032--An error can occur with management protocol processing. Please use this URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw63032

The following caveats were resolved in firmware version 11.10T and are also resolved in version 11.10T1:

- Resolved: CSCdw02941—The access point should assign the identifier field in an EAP-SUCCESS, EAP-FAILURE, or EAP-REQUEST packet to the value specified by the server in a way that is consistent with the 802.1X specification.
- Resolved: CSCdu05324—IP Port filters do not block pings. Table B-3 in Appendix B of the *Cisco Aironet Access Point Software Configuration Guide* listed PING as the additional identifier for the echo IP Port filter entry. However, the echo entry does not block standard pings.
- Resolved: CSCdu09909—A large amount of CDP messages can consume the access point's entire memory.
- Resolved: CSCdv10964—The access point sometimes displays an Invalid Value error when you change the configuration through the command-line interface.
- Resolved: CSCdu10993—Cannot access workgroup bridges associated with access point or bridge. When a workgroup bridge (WGB34x or WGB352) was associated to an access point, you could not access the WGB console menus or ping the WGB from a station on the wired LAN connected to the access point's Ethernet port.
- Resolved: CSCdv40899—When a standby access point is disabled, the radio port shuts down on the access point it is set up to monitor.

- Resolved: CSCdv46499—EAP success/fail message sent to the client device might not correspond to the RADIUS response. If the access point receives an ACCESS-Reject packet with an EAP-SUCCESS attribute, the access point should discard the EAP-SUCCESS attribute and should forward a standard EAP-FAILURE packet to the client.
- Resolved: CSCdv46567—Messages used for 802.1X authentication should not be sent to client devices not using 802.1X authentication.
- Resolved: CSCdv56299—When you set the SNMP trap server to CiscoWorks6.0 and restart the access point using the Warm restart system now button on the System Configuration Setup page, the trap server never receives the cold restart trap message.
- Resolved: CSCdv61259—Retransmission of EAP-identifier packets using the same identifier value causes delays, especially if it results in multiple requests being forwarded to the RADIUS server. The EAP identifier should be incremented on retransmission.
- Resolved: CSCdv61274—If an 802.1X client that has successfully authenticated continuously transmits EAPOL-START packets to the access point with no more than 60 seconds between each packet, the access point restarts an authentication timer each time it receives a packet, and the client is never denied access. The access point should block the port after responding to a predefined number of EAPOL-START packets.
- Resolved: CSCdv61291—EAP-Notification responses should not always be forwarded to the server. In an 801.1X authentication process, the final RADIUS-ACCEPT message may include an EAP-NOTIFICATION attribute, which is to be forwarded to the client. EAP requires the client to respond. If the access point forwards the response to the authenticating server, as it forwards all EAP messages, it may cause the server to deny access to the client.
- Resolved: CSCdu66066—If the default disposition of the onlyIP Ethertype filter is set to block, the access point does not allow new associations. Because 802.11 management or control packets (0xe1f0 or 0xe1f1) are defined as Ethertype packets, the access point blocks these packets from devices that are not associated.
- Resolved: CSCdu68659—Web-browser interface sometimes requires multiple logins.
- Resolved: CSCdv70892—Access point should start the authentication process from the beginning when it switches from the primary RADIUS server to a backup server during an authentication.
- Resolved: CSCdv73147—An access point sometimes fails to receive a firmware distribution from another access point because it fails to respond to the distributing access point when the distributing access point is searching for other devices that should receive the firmware.
- Resolved: CSCdv74494—The access point's CDP Entry for in-line power consumption is too high (10W). The CDP entry should be 7W.
- Resolved: CSCdu78436—The Reset All System Factory Defaults button on the System Configuration Setup page does not clear all protocol and MAC address filters.
- Resolved: CSCdv81447—If several Aironet UC4800 client devices are associated to an access point running firmware 11.06 and later, the access point locks up and reboots.
- Resolved: CSCdv88993—Standby access point does not change its role to Access Point/Root when the monitored access point's Ethernet port fails.

Open Caveats

The following caveats have not been resolved for firmware version 11.10T1:

- CSCdw00747—SNMP command can lock administrators out of access point or bridge.

  It is possible to use an SNMP command to remove privileges from all users defined in the access point or bridge User Manager without disabling User Manager. All users are locked out of the access point or bridge management system because User Manager is still enabled but users have lost their privileges. Workaround: Use the **:resetall** command on the command-line interface to reset the access point or bridge to default settings, or bootstrap a valid user configuration file.

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

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

- CSCdw13878—Setting up hot standby when monitored access point's radio is disabled locks up standby access point.

  If the radio is disabled on the monitored access point when you set up the standby access point, the standby access point reports an initialization failure and must be rebooted. Workaround: Make sure the monitored access point's radio is working when you set up the standby access point.

- CSCdw16742—Broadcast key rotation does not work with repeater access points and non-root bridges.

  When broadcast key rotation is enabled on a repeater access point or on a non-root bridge that is authenticated to the network using LEAP, data cannot be passed between the repeater or non-root bridge and the root bridge or access point. Workaround: Do not use broadcast key rotation on a non-root bridge or a repeater access point.

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

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

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

  SNMP community names entered on the Express Setup page have limited access to access point configuration information. To provide full access to the SNMP community you specify on the Express Setup page, use the User Manager pages to assign firmware privilege to the community name. See the *Cisco Aironet Access Point Software Configuration Guide* for complete instructions on using the User Manager.

- CSCdt34104—Filters can be disabled but not edited from the command-line interface.

  You cannot edit MAC address filters with the command-line interface. However, you can use the CLI's Ethernet Protocol Filters and Root Radio Protocol Filters pages to disable filters.

- CSCdu38857—Access point sometimes loads wrong firmware when updating from an FTP server.

  When you update access point firmware through FTP file retrieval in the web-browser interface, the access point searches for any valid firmware files if it does not find the firmware file on the FTP server. If the access point finds a valid firmware file, it uses the alternate file and does not indicate on the web-browser interface that it is loading an alternate firmware image. After you update

firmware through FTP file retrieval in the web-browser interface, verify that the access point loaded the correct firmware version. The access point firmware version number appears in the upper-left corner of most management screens in the web-browser interface.

- CSCdv43046—Spanning Tree Protocol (STP) cannot be disabled on 350 series bridges.

  You cannot disable STP on 350 series bridges, and the standards-based STP used on 350 series bridges is incompatible with the STP used on 340 series bridges. Therefore, if you use both 340 and 350 series bridges on your wireless network, the 350 series bridges should link only to other 350 series bridges, and the 340 series bridges should link only to other 340 series bridges.

- CSCdv86778—Access point or bridge reset to default configuration ignores BOOTP response.

  If you reset an access point or bridge configuration with the **:resetall** command on the command-line interface, the access point or bridge is set by default to receive an IP address using DHCP. If a generic configuration file on your DHCP server sets the newly reset access point or bridge to BOOTP, the access point or bridge ignores the BOOTP response when it reboots and displays a series of error messages.

- CSCdv88113—Enabling Message Integrity Check (MIC) without enabling WEP blocks communication with associated client devices.

  If you enable MIC without enabling WEP, client devices associate to the access point or bridge but cannot pass data. Workaround: always enable WEP when you enable MIC.

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 Cisco Aironet access points and bridges.

Packet Tracing Instructions Added to Software Configuration Guide

The *Cisco Aironet Access Point Software Configuration Guide* now provides instructions for using the packet tracing feature on access points and 350 series bridges. See the "Tracing Packets" section on page 9-32 of the *Cisco Aironet Access Point Software Configuration Guide* for details on packet tracing.

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*

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

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 Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, 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 **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

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

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 user, 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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.