



Release Notes for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges Running VxWorks Firmware Version 12.04

November 10, 2003

These release notes describe features and caveats for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges running VxWorks firmware version 12.04.

Contents

- [Introduction, page 2](#)
- [Installation Notes, page 2](#)
- [Limitations and Restrictions, page 4](#)
- [Important Notes, page 7](#)
- [Caveats, page 9](#)
- [Troubleshooting, page 11](#)
- [Related Documentation, page 11](#)
- [Obtaining Documentation, page 12](#)
- [Documentation Feedback, page 13](#)
- [Obtaining Technical Assistance, page 13](#)
- [Obtaining Additional Publications and Information, 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>

Invalid Console Message on Reboot

When upgrading to 12.04 from an earlier version, the following console message appears when the system reboots:

```
Inflating EnterpriseAP Sys 12.03...
```

The message is invalid and should be ignored.

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 VxWorks firmware version 12.04.

Version Supported

Your access point must be running VxWorks firmware version 10.x or later to install VxWorks firmware version 12.04. Your bridge must be running version 11.07 or later to install VxWorks firmware version 12.04.

Upgrading to a New Firmware Release

Determining the VxWorks Firmware Version

The VxWorks 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 instructions to install access point and bridge firmware:

- Step 1** Follow this link to the Software Center on Cisco.com and download VxWorks firmware version 12.04:
<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 arrow to view the valid values for the Product Type field.
- Step 4** Click **Access Point** or **Wireless Bridge**.
- Step 5** Click **Submit**. The Step 2 of 3 page appears.
- Step 6** Click the drop-down arrow to view the valid values in the Model Number field.

- Step 7** Select the model number of your access point or bridge:
 - a. 340 or 350 series for access points
 - b. 340, 350, or 4800 series for bridges
- Step 8** Click **Submit**. The Step 3 of 3 page appears.
- Step 9** To download the current release, click the **Current Release (Recommended)** 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** or **Wireless Bridge 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 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.



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 or bridge) lights continuously 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 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 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	—

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

Firmware Version	Draft 7	Draft 8	802.1x-2001
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 ¹	—	x	x
AP34x/35x 11.07 and later	—	x	x
AP34x/35x and BR35x 11.21 through 12.04	—	x	x
AP12xx 11.40T and later	—	x	x

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



Note

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

Use the Authenticator Configuration page in VxWorks 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) drop-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 VxWorks firmware version 12.04.

MAC Address Filtering

Version 12.04 has added a new method of MAC address filtering. The filter is based on whether or not the address is a client. A new "Client Disallowed" button on the Address Filters page allows users to determine whether or not a client having a specific MAC address is allowed to associate to the access point. Using the "Client Disallowed" feature prevents clients from assuming sensitive MAC addresses on the user's network.

Setting ACS Session Timeout

Version 12.04 has added a MAC authentication timeout featurette which is used in conjunction with MAC authentication caching. It enables administrators to control MAC authentication session time in seconds by configuring the ACS with RADIUS attribute Session-Timeout (27). When the session time expires, the access point deauthenticates the client and removes the cached MAC authenticated entry. When the client re-associates, the access point performs a MAC authentication operation with the ACS.

**Note**

This featurette addresses resolved caveats CSCec08844, CSCec35327, and CSCeb61728.

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

Reboot of Workgroup Bridges Required When Allowing More Than 20

With VxWorks firmware version 12.04, 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 or bridge. After selecting **no** for this setting, you must reboot workgroup bridges associated to the access point or bridge.

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 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 (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**.
-

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.

Hot Standby Not Supported on 350 Series Bridges

Although the hot standby feature appears on the menu, hot standby is not supported on 350 series bridges.

Caveats

This section lists open and resolved software issues in VxWorks firmware version 12.04.

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 12.04:

- 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.

- CSCec60688—The access point sometimes drops all client associations and stops communicating through both the radio and Ethernet ports.

Workaround: Disable DNS on the access point.

Resolved Caveats

The following caveats are resolved in VxWorks firmware version 12.04:

- CSCea44315—Intermittent AWCO stop/start no longer causes wireless clients to disassociate.
- CSCea47390—Access point no longer crashes on task 0x97d2d8 “tThttpd.”
- CSCea51324—Enabling MIC on a 350 series bridge no longer blocks communication.
- CSCea65900—TFTP downloads no longer cause the access point to crash.
- CSCeb27772—The access point no longer crashes due to excess memory consumed by maintaining the association table.
- CSCeb55765—The auto channel-select feature now works as expected.
- CSCeb58467—A long If-Modified-Since header no longer causes a Buffer overflow in Trivial HTTP (THTTPd).
- CSCeb61648—The access point now sends accounting request packets when a client attempts a double LEAP login.
- CSCeb61728, CSCeb87616, CSCec00332, CSCeb73542—The access point no longer hangs when too many client devices associate to it.
- CSCeb75140—The access point no longer stops sending beacons unexpectedly.
- CSCeb76379—When a client that has been assigned to a VLAN disassociates and then reassociates to the access point, the client no longer has to wait to be reassigned to the correct VLAN.
- CSCeb82272—Client devices using EAP-SIM can now log off from a connection to an access point and successfully log back in.
- CSCeb84020—Bridge links are now stable when the non-root bridge is configured to authenticate to the root bridge using LEAP authentication.
- CSCeb85983—Non-root bridges no longer hang when they lose association with the root bridge.
- CSCec20567—Non-root bridges now reassociate after losing connectivity to the root bridge.
- CSCec53509—You can now define client MAC addresses that are not allowed to associate to the access point.
- CSCin46604—The Solicitations Sent counter on the authoritative access point now increments correctly by 1.
- CSCin46620—Resetting All System Factory Defaults now deletes existing VLAN numbers.
- CSCin46639—When configured to do so, the access point now switches to repeater mode when Ethernet link is down.
- CSCeb61728—The access point no longer hangs and reboots when an abnormally large number of clients are associated.
- CSCec50480—The non-root bridge no longer loses association with the root bridge when using LEAP.

Other Caveats

The following is a status of caveats published in the release notes for previous VxWorks versions that were not resolved in version 12.04:

- CSCeb79415—The access point association table does not display a client name, device type, or software version for Cisco 7920 phones that associate to the access point.

This caveat has been closed because Cisco 7920 phones do not support Aironet Extensions. The access point displays values for the client name, device, type, and software version fields in the association table only for client devices that support Aironet Extensions.

- 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 has been closed.

- CSCin46049—Client is always forced to EAP-associate with multiple VLANs.

Cisco has been unable to reproduce this caveat.

- 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.

Cisco has been unable to reproduce this caveat.

- CSCea64908—Voice stream is interrupted when using Spectralink IP phones or Cisco 7920 wireless IP phones with 350 series access points.

There is no workaround for this caveat and Cisco will not be addressing it in future releases.

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 Internetworking Design Guide*
- *Cisco Internetworking Technology Handbook*
- *Cisco Internetworking Troubleshooting 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 annual or quarterly subscriptions through the online Subscription Store:

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

Click Subscriptions & Promotional Materials in the left navigation bar.

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, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

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

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

Opening a TAC Case

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

TAC Case Priority Definitions

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

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

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

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

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

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 general networking, training and certification titles. Both new and experienced user will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/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/index.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 © 2003 Cisco Systems, Inc. All rights reserved.

 Printed in the USA on recycled paper containing 10% postconsumer waste.