Release Notes for Cisco Aironet 1200 Series Access Points Running Firmware Version 12.01T1

January 20, 2003

These release notes describe caveats for Cisco Aironet 1200 Series Access Points running firmware version 12.01T1. This release note also contains important information about the device.

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 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 the 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 one radio of each type, but it does not support two 2.4-GHz or two 5-GHz radios. 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

Cisco Aironet 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 subject 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.

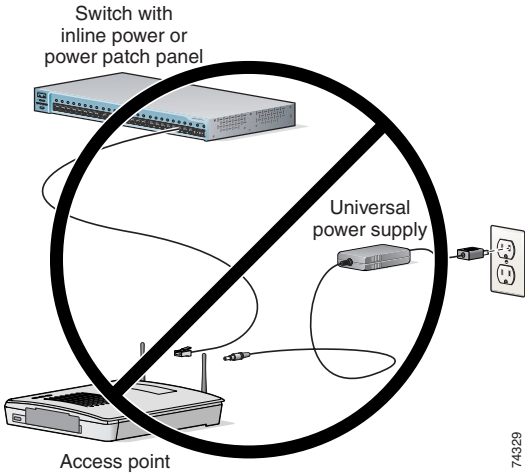
Caution The nominal voltage for 1200 series access points is 48 VDC, and the access point is operational up to 60 VDC. Voltage higher than 60 VDC can damage the equipment.

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 version 12.01T1.

Version Supported

Your access point must be running firmware version 11.40T or later to install firmware version 12.01T1.

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 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 1200 Series Wireless LAN Products > Cisco Aironet 1200 Series Access Points > Cisco Aironet 1200 Series Access Point Software Configuration Guide > Managing Firmware and Configurations > Updating Firmware

3. Follow this link to the Software Center on Cisco.com and select the **Cisco Aironet 1200 Series** link to download firmware version 12.01T1:

   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 FTP Server Setup page. Refer to the "Updating from a File Server" section on page 10-5 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. 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 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 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 remove power.

EAP Authentication Requires Matching 802.1x Protocol Drafts

Note This section applies to wireless networks set up to use LEAP. If you do not use LEAP on your wireless network, you can skip this section.

Wireless client devices use Extensible Authentication Protocol (EAP) to log onto a network and generate a dynamic, client-specific WEP key for the current logon session. If your wireless network uses WEP without EAP, client devices use the static WEP keys entered in the Aironet Client Utilities.

If you use Network-EAP authentication on your wireless network, your client devices and access points must use the same 802.1x protocol draft. For example, if the radio firmware on the client devices that will associate with an access point is 4.16, the access point should be configured to use Draft 8 of the 802.1x protocol. Table 1 lists firmware versions for Cisco Aironet products and the draft with which they comply.

Table 1 802.1x Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	802.1x-2001
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 and later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—

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

Firmware Version	Draft 7	Draft 8	802.1x-2001
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 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) pull-down menu to select the draft of the 802.1x protocol the access point radio should use. Menu options include:

- Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.
- Draft 8—Select this option if LEAP-enabled client devices that associate with this access point use radio firmware versions 4.13, 4.16, or 4.23.
- 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 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.

Hot Standby Mode and Radio Diagnostics Available for 2.4-GHz Radio Only

Hot Standby mode is available only for the 2.4-GHz radio in access points that contain two radios. Hot Standby mode is not available for 5-GHz radios. Also, the Carrier Test and Antenna Alignment radio diagnostics tool are available only for the access point's 2.4-GHz radio.

Important Notes

This section lists important information about access points running firmware version 12.01T1.

Adding or Deleting Proxy Mobile IP AAPs

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

Step 1 Browse to the Setup page.

Step 2 In the Services section, click **Proxy Mobile IP**. The Proxy Mobile IP Setup page appears.

Step 3 Click **General**. The Proxy Mobile IP General page appears.

Step 4 Change the Enable Proxy Mobile IP setting to **no**.

Step 5 Add or delete AAPs as necessary.

Step 6 Change the Enable Proxy Mobile IP setting to **yes**.

Unexpected Results on Lost Ethernet

When backbone connectivity is lost on an access point running version 12.01T1, the device switches to repeater mode. Switch to Repeater mode is the default setting for this condition. Therefore, if the access point's role in your network is not a repeater access point, make sure you connect it to your wired network before booting it up. If you do not connect the access point to your network, it switches to the repeater mode when it fails to detect the presence of an Ethernet connection. When this occurs, wireless client devices are unable to connect and you cannot correct the problem using a wireless client. The only way you can change the configuration is through a serial connection using the access point's command line interface.

Error Message Appears for Access Points with One Radio

When you install firmware version 12.01T1 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.

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 firmware version 12.01T1, you can select **no** for the *Classify Workgroup Bridges as Network Infrastructure* setting on the AP/Root Radio Advanced page to allow up to 50 workgroup bridges to associate to the access point. When you select **no** for this setting, you must reboot workgroup bridges associated to the access point.

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 CDP-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.

Caveats

This section lists resolved and open software issues in firmware version 12.01T1.

Getting Bug Information on Cisco.com

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

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

Open Caveats

The following caveats have not been resolved for firmware version 12.01T1:

- CSCdy03381—One access point radio on dual-mode access points sometimes fails to restart after a warm reset.

  Workaround: Perform a cold reboot of the access point if one of the radios does not restart.
- CSCdz04380—Incorrect values are advertised for CWMin and CWMax on Voice VLAN.

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

  There is no workaround for this caveat.
- CSCdz50218—Access point does not update home or foreign agent status when advertisement flags change.

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

  Workaround: Disable and then enable proxy Mobile IP.
- CSCdy10787—The access point aborts any configuration containing an unknown MIB variable.

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

  Workaround: Upgrade access points to the same firmware version before distributing configurations.
- CSCdy11906—When WEP is enabled and you set all WEP keys to **not set**, WEP is still enabled but the web-browser page indicates that WEP is disabled.

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

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

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

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

- CSCdz48575—Default lost Ethernet action not appropriate.

  See the "Unexpected Results on Lost Ethernet" section on page 7 for a complete description of this caveat.

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

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

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

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

  There is no workaround for this caveat.

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

  See the "Adding or Deleting Proxy Mobile IP AAPs" section on page 7 for details and procedures to correct this problem.

- CSCdy20169—When a 1200 series access point boots, it sometimes displays this warning:

  ```
  (Warning) Routine "pktRouterRcvRtn" is unable to Take the forwardTbl Guard semaphore
  ```

  You can ignore this message.

- CSCdy27831—When you set the default Unicast Address Filter to disallowed, you must reboot the access point for the setting to take effect.

- CSCdy29556—Symbol IP phone continuously associates and authenticates to an access point configured with multiple VLANs.

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

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

There is no workaround for this caveat.

- CSCdy73695—When a repeater access point receives packets from a root access point while the repeater is attempting to associate, the repeater sometimes displays this error:

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

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

- CSCdx81372—Access point does not accept version 11.56-generated .ini file.

  If you download the full configuration .ini from an access point running 11.56, upgrade to version 12.01T1, and then attempt to download the .ini file from an FTP server, the following error message appears:

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

  Workaround—When producing .ini files, dump a non-default configuration for version 11.56 instead of a full configuration.

- CSCdz58192—Root bridges with LEAP enabled on the native VLAN must have the security setting matching that set on the Advanced Radio Setup page. If the settings do not match, the bridge link will go down temporarily whenever an infrastructure device authenticates.

Resolved Caveat

The following caveat is resolved in version 12.01T1:

- CSCdz66748 (CSCdz60229)—Access points are no longer vulnerable to a denial of service (DoS) when support for the Secure Shell (SSH) server is enabled. Malformed SSH packets directed at the access point no longer cause a reload of the device.

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*

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

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

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

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

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

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

Cisco TAC Web Site

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

http://www.cisco.com/tac

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

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

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

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

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

Cisco TAC Escalation Center

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

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

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

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

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