Release Notes for Cisco Unity-CM TSP Release 7.0(4b)

Revised March 23, 2005

These release notes contain download and installation instructions, and information on new and changed requirements and support, and caveats for Cisco Unity-CM TAPI service provider (TSP) Release 7.0(4b).

The Cisco Unity-CM TSP is used only for the Cisco CallManager and Cisco CallManager Express integrations.

Cisco Unity-CM TSP version 7.0(4b) is available only from the Cisco Unity-CM TSP Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity-cm-tsp.

Note Items in release notes—excluding caveats—may be revised to correct or to clarify information after the initial publication date (the date the software was released). When an item has been changed, the phrase "*Revised <date>*" is included in the text of the item.

Table 1 lists the version combinations of Cisco Unity, Cisco CallManager, and Cisco CallManager Express with which version 7.0(4b) is supported.

Table 1 Supported Version Combinations for Cisco Unity-CM TSP 7.0(4b), Cisco Unity, Cisco CallManager, and Cisco CallManager Express[1]

Cisco Unity-CM TSP	Cisco Unity	Cisco CallManager	Cisco CallManager Express
7.0(4b)	4.0(4), 4.0(3), 4.0(2), 4.0(1), 3.1(6), 3.1(5), 3.1(4), 3.1(3), 3.1(2c), 3.1(2b), 3.1(2), 3.1(1), 3.0(4), 3.0(3), 3.0(2), 3.0(1)	4.1(2), 4.0(2), 4.0(1), 3.3(4), 3.3(3), 3.3(2), 3.3(1), 3.2(3), 3.2(2), 3.2(1), 3.1(4), 3.1(3), 3.1(2), 3.1(1), 3.0(12), 3.0(11), 3.0(10), 3.0(9)	3.0(3), 3.0(2), 3.0(1)

1. Table 1 was revised March 23, 2005.

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

Note For the most current list of all qualified version combinations of the Cisco Unity-CM TSP, Cisco Unity, Cisco CallManager, and Cisco CallManager Express—including combinations qualified since the release of Cisco Unity-CM TSP version 7.0(4b)—and for the version support policy for Cisco Unity and Cisco CallManager, refer to *Compatibility Matrix: Cisco Unity, the Cisco Unity-CM TSP, Cisco CallManager, and Cisco CallManager Express* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/cmptblty/tspmtrx.htm.

Cisco CallManager Support Patch (sp) releases are not listed in Table 1 unless they affect compatibility with Cisco Unity or the Cisco Unity-CM TSP. If not listed, a support patch has the same compatibility as the base release. In addition, rereleased versions—for example, 3.x(xa) rereleased as 3.x(xb)—are assumed to have the same compatibility unless noted.

Cisco Unity service releases (SR) are not listed in Table 1 unless they affect compatibility with Cisco CallManager or the Cisco Unity-CM TSP. If not listed, a service release has the same compatibility as the base release.

Contents

System Requirements

- The Cisco Unity server must be running a version of Cisco Unity from 3.0(1) through 4.0(x).
- An account with local administrator privileges must be used to upgrade the Cisco Unity-CM TSP. Otherwise, no Cisco Unity ports will be available after the upgrade.

- If you are changing the number of voice messaging ports on the Cisco Unity system, you must adjust the ports in Cisco CallManager before installing the Cisco Unity-CM TSP. Refer to the "Changing the Number of Voice Messaging Ports" section in the applicable version of the Cisco CallManager integration guide. Cisco CallManager integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_configuration_guides_list.html.
- If you are setting up a Cisco CallManager integration for the first time, refer to the applicable version of the Cisco CallManager integration guide, instead of using the instructions in these release notes. Cisco CallManager integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_configuration_guides_list.html.

Determining the Software Version

This section contains procedures for determining the version in use for the following software:

- Cisco Unity-CM TSP, page 3
- Cisco Unity, page 3

Cisco Unity-CM TSP

To Determine the Cisco Unity-CM TSP Version in Use by Using the Cisco Unity Telephony Integration Manager

Step 1 On the Windows Start menu of the Cisco Unity server, click **Programs** > **Cisco Unity** > **Manage Integrations**. The UTIM window appears.

Step 2 In the left pane, click the Cisco CallManager integration.

Step 3 In the right pane, click **Properties**. On the Integration tab, the Cisco Unity-CM TSP version appears in the TSP Version field.

To Determine the Cisco Unity-CM TSP Version in Use by Using the AvSkinny.tsp File

Step 1 Browse to the WinNT\System32 directory.

Step 2 Right-click **AvSkinny.tsp**, and click **Properties**.

Step 3 In the Properties window, click the **Version** tab.

Step 4 In the Item Name list, click **Product Version**. The Cisco Unity-CM TSP version appears in the Value window.

Cisco Unity

To Determine the Cisco Unity Version in Use by Using the Cisco Unity Administrator

In the Cisco Unity Administrator, go to the **System > Configuration > Software Versions** page. The Cisco Unity version appears in the Cisco Unity Build Number field.

To Determine the Cisco Unity Version in Use by Using the AvCsMgr.exe File (Version 3.0(4) and Later Only)

Step 1 Browse to the **CommServer** directory.

Step 2 Right-click **AvCsMgr.exe**, and click **Properties**.

Step 3 In the Properties window, click the **Version** tab.

Step 4 In the Item Name list, click **Product Version**. The Cisco Unity version appears in the Value window.

Downloading Cisco Unity-CM TSP Version 7.0(4b)

Cisco Unity-CM TSP version 7.0(4b) is available only from the Cisco Unity-CM TSP Software Download page.

To Download the Cisco Unity-CM TSP

Step 1 Confirm that the Cisco Unity server has at least 6 MB of hard disk space available for the download file and the extracted files.

Step 2 On a computer with a high-speed Internet connection, go to the Cisco Unity-CM TSP Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity-cm-tsp.

Note To access the software download page, you must be logged on to Cisco.com as a registered user.

Step 3 Download the file **CiscoUnityCMTSP7.0.4b.exe** to the directory of your choice.

Step 4 Unzip the file **CiscoUnityCMTSP7.0.4b.exe** to the default directory or to the directory of your choice.

Step 5 Delete the file **CiscoUnityCMTSP7.0.4b.exe** to free hard disk space.

Installing the Cisco Unity-CM TSP

This section contains procedures for installing the Cisco Unity-CM TSP depending on the version of Cisco Unity:

- For a Cisco Unity 4.0(x) System, page 5
- For a Cisco Unity 3.1(x) or 3.0(x) System, page 5

For a Cisco Unity 4.0(x) System

Do the procedure in this section only if you are installing Cisco Unity-CM TSP 7.0(4b) on a Cisco Unity version 4.0(x) system.

Note that if you are changing the number of voice messaging ports on the Cisco Unity system, you must add a voice messaging port to Cisco CallManager for each port that you are connecting to Cisco Unity before you install the Cisco Unity-CM TSP. Refer to the "Changing the Number of Voice Messaging Ports" section in the applicable version of the Cisco CallManager integration guide. Cisco CallManager integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_configuration_guides_list.html.

You can keep the previous voice messaging ports, and the Cisco Unity-CM TSP configuration is automatically retained.

To Install the Cisco Unity-CM TSP on a Cisco Unity 4.0(x) System

Step 1 Stop Cisco Unity (right-click the **Cisco Unity** icon in the system tray, then click **Stop Cisco Unity**).

Step 2 Browse to the directory in which you saved the extracted Cisco Unity-CM TSP files in the "Downloading Cisco Unity-CM TSP Version 7.0(4b)" section on page 4, and double-click **SkinnySetup.exe**.

Step 3 Follow the on-screen prompts.

Step 4 Restart the Cisco Unity server.

For a Cisco Unity 3.1(x) or 3.0(x) System

Do the procedure in this section only if you are installing Cisco Unity-CM TSP 7.0(4b) on a Cisco Unity version 3.1(x) or 3.0(x) system.

Note that if you are changing the number of voice messaging ports on the Cisco Unity system, you must add a voice messaging port to Cisco CallManager for each port that you are connecting to Cisco Unity before you install the Cisco Unity-CM TSP. Refer to the "Changing the Number of Voice Messaging Ports" section in the applicable version of the Cisco CallManager integration guide. Cisco CallManager integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_configuration_guides_list.html.

You can keep the previous voice messaging ports, and the Cisco Unity-CM TSP configuration is automatically retained.

To Install the Cisco Unity-CM TSP on a Cisco Unity 3.1(x) or 3.0(x) System

Step 1 Stop Cisco Unity (right-click the **Cisco Unity** icon in the system tray, then click **Stop Cisco Unity**).

Step 2 Browse to the directory in which you saved the extracted Cisco Unity-CM TSP files in the "Downloading Cisco Unity-CM TSP Version 7.0(4b)" section on page 4, and double-click **SkinnySetup.exe**.

Step 3 Follow the on-screen prompts.

Step 4 In the Cisco Unity-CM TSP dialog box, in the Select Cisco CallManager list, click the Cisco CallManager or Cisco CallManager Express server to which Cisco Unity is connected.

If the Select Cisco CallManager list is empty, click **Add**, enter the IP address of the Cisco CallManager server to which Cisco Unity is connected, then click **OK**.

Step 5 In the Cisco Unity-CM TSP Settings dialog box, verify the information in the following three fields:

- Primary CallManager IP Address
- Number of Voice Ports
- Device Name Prefix (The prefix must match the prefix for the Voice Mail ports. Note that the device name prefix is case-sensitive.)

Step 6 Confirm that the dial numbers in the MessageWaitingOffDN and MessageWaitingOnDN fields match the Cisco CallManager settings on the applicable Cisco CallManager Administration page:

Cisco CallManager version 3.2(1) and later	Settings are on the Features > Voice Mail > Message Waiting page in Cisco CallManager Administration.
Cisco CallManager version 3.1(4) and earlier	Settings are on the Service > Service Parameters page in Cisco CallManager Administration

If the dial numbers are not in the MessageWaiting fields of the Cisco Unity-CM TSP Settings dialog box, enter them.

Step 7 Confirm that the Cisco CallManager Device list displays the correct number of Cisco Unity ports and that the port names match the names of the Voice Mail ports.

Step 8 Click **OK**.

Step 9 In the Cisco Unity-CM Service Provider dialog box, click **Test**.

Step 10 In the Test Configuration and Connection dialog box, click **OK**.

Step 11 If the configuration is correct, the Test Succeeded dialog box appears. Click **OK**, then skip to Step 13.

If incorrect information was entered during configuration, the Error dialog box appears. Errors can be caused by:

- Entering the wrong IP address for the Cisco CallManager server during configuration.
- Entering the wrong device name prefix during configuration.

Step 12 Correct errors in the Service Provider dialog box.

In Windows 2000, on the Start menu, click **Settings > Control Pane > Phone and Modem Options > Advanced > Cisco Unity-CM Service Provider > Settings**.

or

In Windows NT, on the Start menu, click **Settings > Control Panel > Telephony > Telephony Drivers > Cisco Unity-CM Service Provider > Settings**.

Step 13 Restart the Cisco Unity server.

New and Changed Requirements and Support—Release 7.0(4b)

This section contains information about new and changed requirements and support for Cisco Unity-CM TSP Release 7.0(4b) only. Refer to the applicable release notes for information on new and changed functionality in earlier versions of the Cisco Unity-CM TSP. Release notes for all versions of the Cisco Unity-CM TSP are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Version 7.0(4b) Highly Recommended

We highly recommend upgrading to Cisco Unity-CM TSP 7.0(4b) to prevent blue screens that can occur in certain infrequent circumstances.

New and Changed Functionality—Release 7.0(4b)

There is no new functionality in Cisco Unity-CM TSP Release 7.0(4b). See the "Resolved Caveats—Release 7.0(4b)" section on page 11 for software fixes in this release.

Refer to the applicable release notes for information on new and changed functionality in earlier versions of the Cisco Unity-CM TSP. Release notes for all versions of the Cisco Unity-CM TSP are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Installation and Upgrade Notes

Uninstalling the Cisco Unity-CM TSP

It is not necessary to uninstall an earlier version of the Cisco Unity-CM TSP before installing version 7.0(4b). The installation process automatically removes the older Cisco Unity-CM TSP.

Caveats

This section describes only severity 1, 2, and select severity 3 caveats.

If you have an account with Cisco.com, you can use Bug Toolkit to find more information on the caveats in this section, in addition to caveats of any severity for any release. Bug Toolkit is available at the website http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Note that this section contains caveat information for Cisco Unity-CM TSP Release 7.0(4b) only. For caveat information for earlier versions of the Cisco Unity-CM TSP, refer to the applicable release notes. Release notes for all versions of the Cisco Unity-CM TSP are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Open Caveats—Release 7.0(4b)

Table 2 Cisco Unity-CM TSP Release 7.0(4b) Open Caveats

Caveat Number	Severity	Component	Description
CSCef29258	2	telephony	Cisco Unity makes about 100 attempts per minute to toggle an MWI for a phone and logs an event log error/warning for each attempt. The failure (CiscoUnity_TSP source id 127) notes that a collision occurred with an incoming call on the same port. This problem may occur with Cisco Unity 4.0(4). **Workaround** In order to stop Cisco Unity from logging messages to the event log, restart Cisco Unity. However, it is not known how to prevent this problem from occurring in the first place.

CSCee09717	3	telephony	Calls will intermittently fail when the following events occur:
			1. A call arrives from the PSTN via an h.323 gateway to a Cisco CallManager server running 4.01 SR1a.
			2. The directory number is configured to call forward all to Cisco Unity voice mail
			3. The call is transferred or hair-pinned to the PSTN via an h.323 gateway.
			The original PSTN caller continues to hear music on hold although the transfer fails.
			This specific transfer failure is indicated by this sequence of events in detailed CallManager traces:
			`ERROR star_MediaExchangeAgenaOpenLogicalChannel can't find call=`
			followed by:
			`sendErrorToMX,waitForMXPathEstablished_MediaExchangeAgenaOpenLogicalChannelAck,Audio Channel OLCAck with error recd`
			Cisco CallManager version 4.0(1) SR1a, Cisco Unity version 4.0.3, Cisco Unity-CM TSP version 7.0.3b. Transfer destination is an h.323 gateway. The gateway sends an h.245 address in the call_proceeding or the alerting message before Cisco Unity has time to send the second transfer event.
			Workaround
			Configure Cisco Unity to use a supervised transfer and increase the number of rings to wait until transfer is always successful. This number may go as high as 20 rings.

Table 2 Cisco Unity-CM TSP Release 7.0(4b) Open Caveats (continued)

Caveat Number	Severity	Component	Description
CSCee43394	3	telephony	Cisco Unity does not properly recall a supervised transfer. This has been identified as a problem in two cases: • A transfer target subscriber is set for call screening, and when they receive the transfer they press 2 to reject the call. The call rejection does not occur properly. • If Cisco Unity transfers a call to a phone that goes RNA after the phone rings the configured number of times, Cisco Unity hangs up the call instead of pulling the call back to the subscriber mailbox. This problem occurs for Cisco Unity integrations with Cisco CallManager Express. There is no workaround.
CSCee57683	3	telephony	The caller is disconnected when transferring to a subscriber (the caller should receive a busy signal). This problem occurs when the following are true: • Cisco Unity is integrated with Cisco CallManager version 4.0(1) or higher. • The caller is not a subscriber. • The dialed subscriber is set to use release transfers to a non-existent phone. There is no workaround.
CSCee59871	3	telephony	This problem occurs when a caller makes a transfer to a subscriber phone. After the subscriber phone begins to ring, the caller hangs up before the subscriber is able to pick up the phone. The port used to make the call does not become idle for 30 seconds, so that the port cannot be used. This problem occurs with Cisco Unity 4.0(4) and Cisco CallManager 4.0(1) (and with SR2 and SR2a). The subscriber is set for supervised transfers. This set up did work properly with Cisco CallManager 3.3(x) version. There is no workaround. However, it is very unlikely that a user will notice this problem.

Table 2 Cisco Unity-CM TSP Release 7.0(4b) Open Caveats (continued)

Caveat Number	Severity	Component	Description
CSCef10291	3	telephony	Upon clicking the Verify Servers command button for a given Cisco CallManager cluster in UTIM (Cisco Unity Telephony Integrations Manager), the Cisco Unity-CM TSP activity to test connectivity and registration to the Cisco CallManager server is not written in any diagnostics file. The UTIM Verify Servers button makes the Cisco Unity-CM TSP do the same registration process as the Cisco Unity-CM TSP does when connecting to Cisco CallManager when Cisco Unity starts up. As long as the Cisco Unity-CM TSP diagnostics are enabled, that Cisco Unity-CM TSP registration activity at Cisco Unity startup is written to a diagnostic file. The registration caused by the Verify Servers button in UTIM is not written to any diagnostic file, even if the Cisco Unity-CM TSP diagnostics are enabled. This behavior occurs in all conditions. There is no workaround.
CSCef51624	3	telephony	Intermittently, when a call arrives from the PSTN and the caller dials zero so that Cisco Unity will transfer the call to a receptionist IP phone, the call will fail and the IP phone will ring only half a ring. The caller from the PSTN will also hear half a ringback on the transfer. This problem happens for around 50 percent of the transfer calls. The customer has five Cisco CallManager servers in the cluster running 4.0(1) SR2a. The cluster is integrated with Cisco Unity 4.0(4) and Cisco Unity-CM TSP 7.0(4). Cisco CallManager sent a StationSetLamp message to turn off the MWI lamp, and Cisco Unity returned a StationOnHook (ci=0, line=0) message for the SetLamp message, which caused the secondary call drop before the secondary call split completion. The split failure caused the transfer failure. As a possible workaround, assign an alternate extension (four or five digits) to the operator. Create a Cisco Unity call handler that translates the zero entered by the caller to the alternate extension of the operator. Cisco Unity will reach the operator by dialing the alternate extension. Since this defect is sensitive to short dial strings, this workaround should resolve the problem until a more permanent fix is available.
CSCef79341	3	telephony	Under certain conditions, Cisco Unity ports will become “locked” in any given conversation state. This has happened under several different scenarios. Under each of the following scenarios, a call into “play” or “record” can block the conversation from transitionning to its next state: 1. The caller calls Cisco Unity and places Cisco Unity on hold. 2. Subscriber 1 has supervised transfer with confirm enabled. Caller 1 attempts to reach Subscriber 1. Before confirming, Subscriber 1 disconnects. 3. Callers abandoning transfers from IVR into Cisco Unity. This has only been seen with the AvAudio.sys that was distributed in TSP 7.0(4)ES6. There is no workaround.

Resolved Caveats—Release 7.0(4b)

Table 3 Cisco Unity-CM TSP Release 7.0(4b) Resolved Caveats

Caveat Number	Severity	Component	Description
CSCed52913	2	telephony	Cisco Unity RTP stream has jitter with G.729 at 30 and 60 ms, and with G.711 at 30ms
CSCef69851	2	telephony	The Cisco Unity-CM TSP returns a CALL_MWI_FAIL message for nonexistent DNs with Cisco CallManager 4.0(X)
CSCee13192	3	telephony	MAPI/network errors when running CSA and Cisco Unity
CSCef13875	3	telephony	AvAudio bugchecks after upgrading from Cisco Unity 4.0(4.27) to Cisco Unity 4.0(4.33)
CSCef36843	3	telephony	The Cisco Unity-CM TSP does not recover/reset connection correctly

Troubleshooting

For information on troubleshooting the Cisco Unity-CM TSP and the phone system integration, refer to the applicable version of the Cisco CallManager integration guide. The guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_configuration_guides_list.html.

Cisco Unity Documentation

For descriptions and URLs of Cisco Unity documentation on Cisco.com, refer to *Cisco Unity Documentation Guide*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/about/aboutdoc.htm.

Obtaining Documentation

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

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

- 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 1 800 553-NETS (6387).

Documentation Feedback

You can send 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request 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 list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—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.

Severity 2 (S2)—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.

Severity 3 (S3)—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.

Severity 4 (S4)—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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. 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/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html