Release Notes for Cisco Unity Bridge Release 3.0(3)

Published May 28, 2004

These release notes describe download and upgrade instructions, new and changed requirements and support, new and changed functionality, limitations and restrictions, and open and resolved caveats for Cisco Unity Bridge Release 3.0(3).

Access the latest Bridge software upgrades on the Cisco Unity Bridge Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity-bridge.

Contents

These release notes contain the following sections:

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

System Requirements, and Supported Hardware and Software

The following documents list the most current Cisco Unity Bridge requirements and are available on Cisco.com:

- *Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm.
- *Cisco Unity Networking Options Requirements (With Microsoft Exchange)* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/netrq.htm.
- *Recommended and Supported Service Packs and Updates for Use with Cisco Unity and the Cisco Unity Bridge* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/cmptblty/msupdate.htm.

Determining the Software Version

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

Cisco Unity Bridge

To Determine the Cisco Unity Bridge Version in Use

Step 1 On the Bridge server, open the Bridge Administrator.

Step 2 Click **About**. The About Cisco Unity Bridge page displays the Bridge version.

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 is displayed in the Cisco Unity Build Number field.

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

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 is displayed in the Value window.

Cisco Unity Voice Connector for Microsoft Exchange

This section contains two procedures. Do the procedure for your version of Cisco Unity.

To Determine the Voice Connector Version in Use: Cisco Unity 4.0 and Later, Voice Connector 10.0 and Later

Step 1 Log on to the Exchange server on which the Voice Connector is installed.

Step 2 In Windows Explorer or My Computer, browse to the applicable directory:

Exchange 2000 or Exchange 2003	<ExchangeServerPath>\VoiceGateway\Bin
Exchange 5.5	<ExchangeServerPath>\Connect\Voice\Bin

Step 3 Right-click **GwIvc.exe,** and click **Properties**.

Step 4 Click the **Version** tab in the Properties window.

Step 5 In the Item Name box, click **Product Version** to view the product version in the Value box.

To Determine the Voice Connector Version in Use: Cisco Unity 3.0 Through 3.1

Step 1 Log on to the Exchange server on which the Voice Connector is installed.

Step 2 In Windows Explorer or My Computer, browse to the applicable directory:

Exchange 2000	<ExchangeServerPath>\VoiceGateway\Bin\LocalizedFiles\ENU
Exchange 5.5	<ExchangeServerPath>\Voice\Bin\LocalizedFiles\ENU

Step 3 Right-click **SetupRes.dll**, and click **Properties**.

Step 4 In the Properties window, click the **Version** tab to view the File Version.

Important Information from Earlier Cisco Unity Bridge 3.0(x) Release Notes

Changes to the Bridge Networking Option

The Bridge Networking option changed significantly in Cisco Unity version 4.0(3) with Bridge 3.0(1) and provided many new features. Refer to the following documentation for details:

- The "Cisco Unity with Exchange: Bridge Networking Enhancements" item in the "New and Changed Functionality—Release 4.0(3)" section of *Release Notes for Cisco Unity Release 4.0(3)* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/relnote/cu403rn.htm.
- *Release Notes for Cisco Unity Bridge Release 3.0(1)* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/relnote/br301rn.htm.

Downloading the Software for a Cisco Unity Bridge Installation or Upgrade

The software required to install or upgrade to Bridge version 3.0(3) is available for download from the Cisco Software Center website. Use a computer with a high-speed Internet connection.

To Download the Bridge Software and Required Service Packs

Step 1 Confirm that the computer you are using has up to 680 MB of hard disk space for the required software, in addition to the space required for the download files. (The download file sizes appear on the download pages.)

Step 2 Go to the Cisco Unity Bridge Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity-bridge.

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

Step 3 Click the following files to download, and follow the on-screen prompts:

- **CiscoUnityBridge3.0.3.exe**
- **CiscoUnityBridge3.0.3ServicePacks.exe**

Step 4 Go to the Microsoft Updates for Cisco Unity Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity_msft_updates.

Step 5 Click the file **English-UpdatesForWin2000-SP4.exe**, and follow the on-screen prompts.

Step 6 When all downloads are complete, extract the files to separate directories:

a. In Windows Explorer, double-click the file.

b. In WinZip, specify a directory to which the files will be extracted.

Step 7 When you are done extracting the files, delete the downloaded .exe files to free disk space.

If you are installing the Bridge software for the first time, refer to the *Cisco Unity Bridge Installation Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/big/big30/index.htm.

Upgrading to Cisco Unity Bridge 3.0(3) from 3.0(x)

If the system is using virus-scanning software or the Cisco Security Agent for Cisco Unity Bridge, you must disable virus-scanning and Cisco Security Agent services on the Bridge server before upgrading the Bridge software. (You disable the services so that they do not slow down the upgrade or cause the upgrade to fail; you re-enable the services after the upgrade.)

Do the following three procedures, as applicable, in the order listed.

To Disable and Stop Virus-Scanning and Cisco Security Agent Services

Step 1 Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.

Step 2 On the Windows Start menu, click **Programs > Administrative Tools > Services**.

Step 3 Disable and stop each virus-scanning service and the Cisco Security Agent service:

a. In the right pane, double-click the service.

b. On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.

c. Click **Stop** to stop the service immediately.

d. Click **OK** to close the Properties dialog box.

Step 4 When the services have been disabled, close the Services MMC.

To Upgrade to Cisco Unity Bridge 3.0(3) from Version 3.0(x)

Step 1 Log on to the Bridge server by using a Windows 2000 Server Administrator account.

Step 2 Confirm that the account has permission to access the Bridge Administrator:

a. Open the Bridge Administrator.

b. If you are allowed access and can view the Bridge Administrator pages, exit the Bridge Administrator.

Caution If you are denied access to the Bridge Administrator, do not continue or the Bridge Setup program will fail. You must log off, then log back on by using another account that is allowed access to the Bridge Administrator. It is possible that the account was denied access to the Bridge Administrator because it is not in the Access Control List of the <Bridge>\Starfish\Asp directory or does not have Full Control permissions to that directory. Access to the <Bridge>\Starfish\Asp directory may have been restricted when password

protection was added to the Bridge Administrator. (For more information, refer to the "Adding Password Protection to the Bridge Administrator" section in the "Setting Up Cisco Unity and the Bridge for Networking" chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/bnet30/index.htm.)

Step 3 Open the Services Control Panel on the Bridge server, and stop the following two services:

- Digital Networking
- Unity Bridge

The Bridge services will complete the shutdown process when the last in-process message transmission or reception, rather than call, is complete. No additional message transmissions will begin on the in-process calls—either outbound or inbound—once shutdown has been initiated.

Step 4 If you downloaded the Bridge software from the Software Center website, browse to the directory in which the files were extracted.

If you are using the Cisco Unity Bridge CD, insert the disc in the CD-ROM drive, and browse to the **Install** directory.

Step 5 Double-click **Setup.exe**.

Step 6 Click **Next**.

Step 7 In the Choose Destination Location dialog box, change the installation directory, if applicable, and click **Next**.

Step 8 If a device driver service was previously installed for the Brooktrout voice-fax card, a message asks if you want to overwrite the existing service. Click **Yes** twice.

Step 9 In the Select Country dialog box, select the country for which the voice-fax cards will be configured, and click **Next**.

Step 10 Verify the installation settings, and click **Next**.

Step 11 When prompted, remove the disc from the CD-ROM drive.

Step 12 Click **OK** to restart the server.

To Re-enable and Start Virus-Scanning and Cisco Security Agent Services

Step 1 Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.

Step 2 On the Windows Start menu, click **Programs > Administrative Tools > Services**.

Step 3 Re-enable and start each virus-scanning service and the Cisco Security Agent service:

a. In the right pane, double-click the service.

b. On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.

c. Click **Start** to start the service.

d. Click **OK** to close the Properties dialog box.

Step 4 When the services have been re-enabled, close the Services MMC.

Upgrading to Cisco Unity Bridge 3.0(3) from 2.x

Upgrading from Bridge 2.x requires that Cisco Unity be upgraded to version 4.0(3) or later and that the Cisco Unity Voice Connector for Microsoft Exchange 2000 be upgraded to version 11.0(1) or later.

For instructions on upgrading to Bridge version 3.0(3) from Bridge 2.x, refer to the "Upgrading from Bridge 2.x to Bridge 3.x" chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/bnet30/index.htm.

New and Changed Requirements and Support—Release 3.0(3)

This section contains information on new and changed support in the Cisco Unity Bridge Release 3.0(3) time frame only. Refer to the release notes of the applicable version for information about new and changed support with earlier versions of the Bridge. Release notes for all versions of the Bridge are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Required Microsoft Service Pack

Note Before installing any qualified service pack on the Cisco Unity Bridge server, confirm that the manufacturer of any optional virus-scanning software that you plan to install on the Bridge server—or that is already installed—also supports the service pack for use with its product.

Windows 2000 Server Service Pack 4 is required for use with Cisco Unity Bridge 3.0(x).

For the most current list of all supported Microsoft service packs—including service packs qualified since the release of Cisco Unity Bridge version 3.0(3)—refer to *Recommended and Supported Service Packs and Updates for Use with Cisco Unity and the Cisco Unity Bridge* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/cmptblty/msupdate.htm.

Required Versions of Cisco Unity and the Voice Connector

Bridge version 3.0(3) is supported only with Cisco Unity 4.0(3) and later and Cisco Unity Voice Connector for Microsoft Exchange 11.0(1) and later. In installations with multiple Cisco Unity servers, all the servers must be upgraded to Cisco Unity 4.0(3) or later.

Caution If you currently have Bridge 2.x, do not upgrade the Bridge server to version 3.0(3) unless you also plan to upgrade all Cisco Unity servers and the Voice Connector to the required versions. If you upgrade the Bridge server without upgrading Cisco Unity and the Voice Connector, messaging between the Bridge and Cisco Unity will fail. Refer to the "Upgrading from Bridge 2.x to Bridge 3.x" chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0* for information on upgrading the Bridge Networking option, including the Bridge server. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/bnet30/index.htm.

New and Changed Functionality—Release 3.0(3)

This section contains information on new and changed functionality for Cisco Unity Bridge Release 3.0(3) only. Refer to the release notes of the applicable version for information about new and changed functionality in earlier versions of the Bridge. Release notes for all versions of the Bridge are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Cisco Unity Bridge Analog Network and Node Analyzer

The Cisco Unity Bridge Analog Network And Node Analyzer (BANANA) is a stand-alone application that runs on the Bridge server. It is designed to assist with monitoring and troubleshooting analog communication between the Bridge and the Octel nodes in the analog network. It also provides detail and summary information of call activity.

BANANA contains an administration application called the BANANA admin that allows you to control how BANANA:

- Generates test messages to the Octel systems that are networked with the Bridge server.
- Extracts information from the call traces on the Bridge server and presents different views of the data.
- Monitors the call traces for error conditions, and logs warnings or errors to the Windows Event Viewer.

With the BANANA admin, you can also install and configure the BANANA service to do the tasks listed above at configurable intervals.

BANANA is available on the Bridge CD and can be downloaded from http://www.ciscounitytools.com. For more information about installing BANANA and using it for monitoring and troubleshooting, refer to BANANA Help and to the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/bnet30/index.htm.

Full Synchronization of Bridge Subscribers with Octel Node Directories

If the Octel node directory (or directories) on the Bridge server becomes out of sync with Cisco Unity, you can force the Cisco Unity bridgehead server to request that all Bridge servers send their entire Octel node directories to the Cisco Unity bridgehead server, which updates the Bridge subscriber information in Cisco Unity. For large directories, the process of synchronizing Bridge subscriber data with the Octel node directories may take several hours to complete. Subscribers can still send and receive messages while the directories are synchronizing.

To Synchronize Bridge Subscribers with Octel Node Directories

Step 1 On the Cisco Unity bridgehead server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Administration - Full synchronization of Bridge Subscribers with Octel Node Directories**.

Step 4 In the **New Value** list, click **1**, then click **Set**.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

Note that the setting Administration - Full synchronization of Bridge Subscribers with Octel Node Directories was added to the Advanced Settings Tool after the release of Cisco Unity 4.0(3). The setting is in the version of the Advanced Settings Tool shipped with Cisco Unity 4.0(4). The latest version of the Advanced Settings Tool can be downloaded from http://www.ciscounitytools.com.

Timeout Settings on Systems Settings Page

The following settings have been added to the Systems Settings page in the Bridge Administrator:

- Inbound DTMF – First Digit Timeout: Enter a number from 10000 to 99000 for the maximum time to wait in milliseconds for the first digit of an analog protocol response from the remote system. The default is 30000 milliseconds.
- Inbound DTMF – Inter-Digit Timeout: Enter a number from 1000 to 99000 for the maximum time to allow in milliseconds between digits of an analog protocol response from the remote system. The default is 2500 milliseconds.

We recommend that you use the default settings unless the Bridge is experiencing message delivery problems with the Octels. For detailed troubleshooting information, refer to the "Troubleshooting Bridge Networking" chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/bnet30/index.htm.

Installation and Upgrade Notes

For detailed information on installing the Cisco Unity Bridge, refer to the *Cisco Unity Bridge Installation Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/big/big30/index.htm.

For detailed information on configuring Bridge Networking, refer to the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/bnet30/index.htm.

Verifying Logon Account Access to the Bridge Administrator

Before upgrading the Bridge software to version 3.0(3), confirm that the account that you log on to the Bridge server with has permission to access the Bridge Administrator. If you are denied access to the Bridge Administrator, do not continue or the Bridge Setup program will fail. You must log off, then log back on by using another account that is allowed access to the Bridge Administrator.

It is possible that the account was denied access to the Bridge Administrator because it is not in the Access Control List of the <Bridge>\Starfish\Asp directory or does not have Full Control permissions to that directory. Access to the <Bridge>\Starfish\Asp directory may have been restricted when password protection was added to the Bridge Administrator. (For more information, refer to the "Adding Password Protection to the Bridge Administrator" section in the "Setting Up Cisco Unity and the Bridge for Networking" chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/bnet30/index.htm.)

Limitations and Restrictions

Refer to the "Notable Behavior" section in the "About Bridge Networking" chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/bnet30/index.htm.

Caveats

This section describes 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 caveat 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 Bridge Release 3.0(3) only. Refer to the release notes of the applicable version for caveat information for earlier versions of the Bridge. Release notes for all versions of the Bridge are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Open Caveats—Release 3.0(3)

Table 1 Cisco Unity Bridge Release 3.0(3) Open Caveats

Caveat Number	Severity	Component	Description
CSCed46178	4	bridge	Queue Status page in the Bridge Administrator shows negative numbers for an Octel Node in the Normal, Urgent, and/or Lines in Use Columns. This has been seen on a Bridge server that was sending and receiving messages to Octel Nodes on multiple ports. As messages are transmitted, the counts on the Queue Status page are not properly updated, resulting in the negative numbers displayed on the screen. There is no workaround. Note, however, that the negative numbers do not indicate problems on the Bridge server; messages are still transmitted to the Octel nodes properly and it is only the counts on the Queue Status Viewer page that are inaccurate.

Table 1 Cisco Unity Bridge Release 3.0(3) Open Caveats (continued)

Caveat Number	Severity	Component	Description
CSCee01101	3	bridge	If a new outbound message is sent, the Bridge receives the message and queues it for delivery. The call log indicates that the new message is ready for delivery with the line: Date/Time,New Outgoing Message,UnityNode,OctelNode... However no calls are initiated to deliver the message, even when the Octel node schedule is active and the interval for sending messages has elapsed. The starfish logs note only "No Callout Activity was started." And there are no event log messages indicating a problem with the message. This can occur on a Cisco Unity Bridge 3.0(x) server, if the system time is manually changed to an earlier time (into the past). **Workaround** In some cases when the system time reaches the latest time previously set on the server message delivery will resume. For example if the system time was 4pm and reset to 2pm, then when the system time again reaches 4pm and the message delivery interval is exceeded, the Bridge will begin delivering the queued messages. There is no other workaround available for this condition, if message delivery does not resume as described above.

Resolved Caveats—Release 3.0(3)

Table 2 Cisco Unity Bridge Release 3.0(3) Resolved Caveats

Caveat Number	Severity	Component	Description
CSCed16197	4	bridge	Bridge-Max voice name length should be enforced on the Bridge
CSCed17947	3	bridge	Bridge-Unity subs with apostrophe in name can not be added
CSCed41856	3	documentation	The Bridge License File wizard fails if Windows 2000 locale is set to anything other than English (United States). All Bridge software including the Bridge License File wizard requires that the Regional Options in Windows Control Panel be set as follows: • The locale must be English (United States). • The language settings must be Western Europe and United States.
CSCed43302	3	bridge	NIC/TCPIP init slow - Bridge DigN svc needs restart after boot
CSCed46693	3	bridge	Bridge-Retry voicename retrieval when call fails on first attempt
CSCed88069	2	bridge	Bridge - port locks under heavy load conditions

Cisco Unity Documentation

For descriptions and URLs of Cisco Unity documentation on Cisco.com, refer to *About Cisco Unity Documentation*. 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

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

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/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 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.

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

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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be 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/

- 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://cisco.com/univercd/cc/td/doc/pcat/

- *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