



Release Notes for Cisco Unity Bridge Release 3.0(4)

Published July 26, 2004

These release notes describe download and upgrade instructions, new and changed requirements and support, limitations and restrictions, and open and resolved caveats for Cisco Unity Bridge Release 3.0(4).

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:

- [System Requirements, and Supported Hardware and Software, page 2](#)
- [Determining the Software Version, page 2](#)
- [Important Information from Earlier Cisco Unity Bridge 3.0\(x\) Release Notes, page 4](#)
- [Downloading the Software for a Cisco Unity Bridge Installation or Upgrade, page 4](#)
- [Upgrading to Cisco Unity Bridge 3.0\(4\) from 3.0\(x\), page 5](#)
- [Upgrading to Cisco Unity Bridge 3.0\(4\) from 2.x, page 8](#)
- [New and Changed Requirements and Support—Release 3.0\(4\), page 8](#)
- [New and Changed Functionality—Release 3.0\(4\), page 9](#)
- [Installation and Upgrade Notes, page 9](#)
- [Limitations and Restrictions, page 10](#)
- [Caveats, page 10](#)
- [Cisco Unity Documentation, page 14](#)
- [Obtaining Documentation, page 14](#)
- [Documentation Feedback, page 15](#)



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

- [Obtaining Technical Assistance, page 15](#)
- [Obtaining Additional Publications and Information, page 16](#)

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, page 2](#)
- [Cisco Unity, page 2](#)
- [Cisco Unity Voice Connector for Microsoft Exchange, page 3](#)

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(4) 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 the Required Service Packs and Updates

- 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** Check the *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 to determine whether new Windows 2000 Server or Internet Explorer service packs were qualified for use after Cisco Unity Bridge 3.0(4) was released. If so, download the latest service packs from Microsoft.com. Also download or print the installation instructions.
- Step 3** *Optional:* Download Cisco Security Agent for Cisco Unity Bridge, which is available on the Cisco Unity Bridge Crypto Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/bridg3d>.



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

Because of export controls on strong encryption, the first time you download Cisco Security Agent for Cisco Unity Bridge, you need to fill out a brief questionnaire. Follow the on-screen prompts.

Refer to *Release Notes for Cisco Security Agent for Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html for information on supported configurations, and for download and installation instructions.

- Step 4** Go to the Cisco Unity Bridge Software Download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/unity-bridge>.

- Step 5** Click the following files to download, and follow the on-screen prompts:
- **CiscoUnityBridge3.0.4.exe**
 - **CiscoUnityBridge3.0.4ServicePacks.exe**
- Step 6** Go to the Microsoft Updates for Cisco Unity Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity_msft_updates.
- Step 7** Click the file **English-UpdatesForWin2000-SP4.exe**, and follow the on-screen prompts.
- Step 8** Click the file **English-UpdatesForIE6.exe**, and follow the on-screen prompts.
- Step 9** 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 10** 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(4) 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 five 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.
-

If Windows 2000 Server Service Pack 4 is not already installed on the Bridge server, install it now.

To Install Windows 2000 Server Service Pack 4

-
- Step 1** In the directory to which you extracted CiscoUnityBridge3.0.4ServicePacks.exe, browse to the Win2K_SP4\I386\Update directory, and double-click **Update.exe**.
- Step 2** Follow the on-screen prompts to complete the installation.
- Step 3** Restart the server.
-

To Install the Latest Microsoft Updates

-
- Step 1** Browse to the directory in which you extracted **English-UpdatesForWin2000-SP4.exe**.
- Step 2** Browse to every directory and install every update. To speed the installation, you may want to:
- Install each update at a command prompt by using the /z option, so you do not have to restart the computer after installing each update.
 - Install each update at a command prompt by using the /m option, so the update installs without displaying any dialog boxes.
 - Create a batch file that installs all of the updates at once.

For more detailed information, refer to Microsoft Knowledge Base article 296861, *How to Install Multiple Windows Updates or Hot Fixes with Only One Reboot*.

- Step 3** Restart the Bridge server.
-

To Upgrade to Cisco Unity Bridge 3.0(4) 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, 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 **Bridge** 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** The following message may appear:
- InstallShield needs your permission before it can install or uninstall read-only files. This read-only file was found:
- Read-only file: C:\Program Files\InstallShield Installation
- Information\[unique guid]\layout.bin
- Do you want InstallShield to modify this read-only file?
- If it does, leave the **Always Use This Answer** check box checked, and click **Yes**.
- Step 12** When prompted, remove the disc from the CD-ROM drive (if applicable).
- Step 13** 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(4) 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(4) 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.

See also the “Upgrading from Bridge 2.x to Bridge 3.x: Cisco Unity Bridge Networking Guide” section on page 13 in these release notes for updates to the upgrade chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0*.

New and Changed Requirements and Support—Release 3.0(4)

This section contains information on new and changed support in the Cisco Unity Bridge Release 3.0(4) 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.

Bridge 3.0(4) Is Required When Selected Exchange Updates Are Installed

If you plan to install either of the following Exchange updates on your Exchange servers, you must install or upgrade to Bridge version 3.0(4) before you install the updates:

- Exchange 2003 Service Pack 1.
- Any of the Exchange 2000 post-Service Pack 3 rollups dated April 2004 or later. (The April 2004 rollup is described in Microsoft Knowledge Base article 836488.)

Otherwise, the directory messages sent by the Bridge will have critical attributes stripped by Exchange, which will cause unnecessary CPU usage on the Cisco Unity bridgehead server.

Required Versions of Cisco Unity and the Voice Connector

Bridge version 3.0(4) 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(4) 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(4)

There is no new or changed functionality in Cisco Unity Bridge 3.0(4). See the “[Resolved Caveat—Release 3.0\(4\)](#)” section on page 13 for information on the software fix in the release.

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(4), 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

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(4) 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(4)

Table 1 Cisco Unity Bridge Release 3.0(4) Open Caveats

Caveat Number	Severity	Component	Description
CSCee53623	2	exchvoicegateway	<p>Messages from other voice mail systems delivered via the Unity voice connector are of lower volume than other messages recorded directly to Unity. These messages may arrive via the Bridge. This condition can occur in Unity versions 4.0 or greater using the voice connector.</p> <p>There is no workaround.</p> <p>The Automatic Gain Control feature of Unity adjusts the volume of voice messages as they are recorded. Messages recorded on remote voice mail systems are routed to Unity subscriber mailboxes via the Voice Connector, therefore do not pass through the same audio level processing.</p>

Table 1 Cisco Unity Bridge Release 3.0(4) Open Caveats (continued)

Caveat Number	Severity	Component	Description
CSCee01101	3	bridge	<p>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...</p> <p>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.</p> <p>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).</p> <p>Workaround</p> <p>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.</p> <p>There is no other workaround available for this condition, if message delivery does not resume as described above.</p>
CSCed46178	4	bridge	<p>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.</p> <p>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.</p>

Table 1 Cisco Unity Bridge Release 3.0(4) Open Caveats (continued)

Caveat Number	Severity	Component	Description
CSCee62714	6	bridge	<p>Message delivery fails when an outbound message contains a DTMF or disconnect tone.</p> <p>After playing the # to signal completion of the message, the Bridge should receive an 8. Since it received no response it believes the message was not successfully received and attempts delivery again. Delivery is attempted according to the number of retries configured on the System Settings page of the Bridge Administrator for. If viewed in the BANANA tool, the condition is logged as Expected data not received in the Save Request state.</p> <p>This condition can occur in Cisco Unity when Bridge networking is utilized and the message being transmitted from the Bridge contains a digit (a DTMF tone or a background noise or voice that matches the frequencies of a DTMF tone).</p> <p>This problem is inherent to analog networking. The error condition is detected, resulting in a non-delivery receipt to the Unity sender.</p> <p>Workaround</p> <p>The sender will need to re-record the message and send it again.</p>
CSCef21474	6	bridge	<p>Message delivery fails when an inbound message to Bridge contains a DTMF tone.</p> <p>When viewing the call in the starfish logs on the Bridge server, a digit other than # is received and reported while recording the inbound message. The call is terminated following the receipt of this DTMF tone. Repeated delivery attempts from the Octel result in the same condition until the message is returned undeliverable to the sender. If viewed in the BANANA tool, the condition is logged as Expected data not received in the Audio Terminator state.</p> <p>This condition can occur in Cisco Unity when Bridge networking is utilized and the message being transmitted to the Bridge contains a digit (a DTMF tone or a background noise or voice that matches the frequencies of a DTMF tone). This problem is inherent to analog networking. The error condition is detected resulting in a non-delivery receipt to the sender on the Octel system.</p> <p>Workaround</p> <p>The sender will need to re-record the message and send it again.</p>

Resolved Caveat—Release 3.0(4)

Table 2 Cisco Unity Bridge Release 3.0(4) Resolved Caveat

Caveat Number	Severity	Component	Description
CSCee80858	2	exchvoicegateway	CsBridgeConnector is not able to auto-create Bridge subscribers when the Voice Connector is installed on a server running Microsoft Exchange 2000 SP3 with KB836488 or Microsoft Exchange 2003 SP1.

Documentation Updates

Omissions

This section lists new and additional information that is not included in the current Cisco Unity Bridge documentation. The new and additional information will be incorporated in a future documentation release, or as otherwise noted.

Upgrading from Bridge 2.x to Bridge 3.x: *Cisco Unity Bridge Networking Guide*

In the “Upgrading from Bridge 2.x to Bridge 3.x” chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0*, the instructions document how to install Windows 2000 Server Service Pack 3. After the guide was published, Windows 2000 Server Service Pack 4 was qualified for use with the Bridge and is the recommended service pack. Do the following procedure to install Service Pack 4. (The *Cisco Unity Bridge Networking Guide, Release 3.0* is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/bnet30/index.htm.)

To Install Windows 2000 Server Service Pack 4

-
- Step 1** In the directory to which you extracted CiscoUnityBridge3.0.4ServicePacks.exe (which you downloaded in the “[Downloading the Software for a Cisco Unity Bridge Installation or Upgrade](#)” section on page 4), browse to the **Win2K_SP4\I386\Update** directory, and double-click **Update.exe**.
 - Step 2** Follow the on-screen prompts to complete the installation.
 - Step 3** Restart the server.
-

In addition, the instructions for upgrading from Bridge 2.x to Bridge 3.0 do not mention installing Microsoft updates for Windows 2000 Server or for Internet Explorer 6. Do the following procedure to install the updates that you downloaded in the “[Downloading the Software for a Cisco Unity Bridge Installation or Upgrade](#)” section on page 4.

To Install the Latest Microsoft Updates

-
- Step 1** Browse to the directory in which you extracted **English-UpdatesForWin2000-SP4.exe**.
-

- Step 2** Browse to every directory and install every update. To speed the installation, you may want to:
- Install each update at a command prompt by using the /z option, so you do not have to restart the computer after installing each update.
 - Install each update at a command prompt by using the /m option, so the update installs without displaying any dialog boxes.
 - Create a batch file that installs all of the updates at once.
- For more detailed information, refer to Microsoft Knowledge Base article 296861, *How to Install Multiple Windows Updates or Hot Fixes with Only One Reboot*.
- Step 3** Browse to the directory in which you extracted **English-UpdatesForIE6.exe**.
- Step 4** Repeat [Step 2](#) for the Internet Explorer 6 updates.
- Step 5** Restart the Bridge server.
-

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_inpk/pdi.htm

You can order Cisco documentation in these ways:

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

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

