



Release Notes for Cisco Unity Bridge Release 3.0(5)

Published August 31, 2004

These release notes describe download and upgrade instructions, new and changed requirements and support, new and changed functionality, limitations and restrictions, open and resolved caveats, and documentation updates for Cisco Unity Bridge Release 3.0(5).

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](#)
- [Downloading the Software for a Cisco Unity Bridge Installation or Upgrade, page 3](#)
- [Upgrading to Cisco Unity Bridge 3.0\(5\) from 3.0\(x\), page 5](#)
- [Upgrading to Cisco Unity Bridge 3.0\(5\) from 2.x, page 7](#)
- [New and Changed Requirements and Support—Release 3.0\(5\), page 7](#)
- [New and Changed Functionality—Release 3.0\(5\), page 8](#)
- [Installation and Upgrade Notes, page 12](#)
- [Limitations and Restrictions, page 12](#)
- [Caveats, page 12](#)
- [Documentation Updates, page 15](#)
- [Cisco Unity Documentation, page 17](#)
- [Obtaining Documentation, page 17](#)
- [Documentation Feedback, page 18](#)



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 18](#)
- [Obtaining Additional Publications and Information, page 19](#)

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 directory **<ExchangeServerPath>\VoiceGateway\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 3.1(3) Through 3.1(6)

-
- 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 directory **<ExchangeServerPath>\VoiceGateway\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.
-

Downloading the Software for a Cisco Unity Bridge Installation or Upgrade

The software required to install or upgrade to Bridge version 3.0(5) 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(5) 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 file **CiscoUnityBridge3.0.5.exe**, and follow the on-screen prompts.
 - Step 6** Return to the Cisco Unity Bridge Software Download page.
 - Step 7** Click the file **CiscoUnityBridge3.0.5ServicePacks.exe**, and follow the on-screen prompts.
 - Step 8** Go to the Microsoft Updates for Cisco Unity Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity_msft_updates.
 - Step 9** Click the file **English-UpdatesForWin2000-SP4.exe**, and follow the on-screen prompts.
 - Step 10** Return to the Microsoft Updates for Cisco Unity Software Download page.
 - Step 11** Click the file **English-UpdatesForIE.exe**, and follow the on-screen prompts.
 - Step 12** 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 13** 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(5) 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:
- In the right pane, double-click the service.
 - On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.
 - Click **Stop** to stop the service immediately.
 - 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 CiscoUnityBridge3.0.5ServicePacks.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** Browse to the directory in which you extracted **English-UpdatesForIE.exe**.
- Step 4** Repeat [Step 2](#) for the Internet Explorer updates.
- Step 5** Restart the Bridge server.

To Upgrade to Cisco Unity Bridge 3.0(5) 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 the account is allowed access and can view the Bridge Administrator pages, exit the Bridge Administrator.



Caution If the account is 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 access was denied because the account 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(5) 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(5) 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 16 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(5)

This section contains information on new and changed support in the Cisco Unity Bridge Release 3.0(5) 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/voicew/ps2237/prod_release_notes_list.html.

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

If you plan to install either of the following Exchange updates on your Exchange servers and you are currently using Bridge version 3.0(3) or earlier, you must install or upgrade to Bridge 3.0(4) or later 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(5) 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(5) 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(5)

This section contains information on new and changed functionality for Cisco Unity Bridge Release 3.0(5) 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.

Automatic Gain Control Applied to Messages Sent from the Bridge to Cisco Unity

The Automatic Gain Control (AGC) feature of Cisco Unity adjusts the volume of voice messages as they are recorded, compensating for variations in the level of the incoming audio signal. The AGC provides subscribers with consistent message-playback levels through the normalization of recordings, and it is enabled by default in Cisco Unity versions 3.1(2c) and later.

Prior to the AGC implementation in Bridge 3.0(5), the volume level of messages recorded on the Bridge from Avaya Octel subscribers was often noticeably lower than messages recorded directly on a Cisco Unity server. Adding the functionality to Bridge 3.0(5) makes the volume level of messages from Octel and Cisco Unity subscribers consistent. Before the Bridge sends messages from Octel to Cisco Unity, the gain level is set to the same default level that Cisco Unity uses.

Error Handling Added for Problematic Outbound Analog Messages

There are many reasons why the analog delivery of an outbound message can fail, for example, a bad connection caused by an interruption on the line or poor line quality. However, message-delivery failure can also occur as a result of problems delivering one particular message. New settings have been added to the System Settings page in the Bridge Administrator that allow you to control how long the Bridge attempts to deliver a particular message before returning it to the sender as undeliverable. (See the [“Fields Added to System Settings Page in Bridge Administrator”](#) section on page 11 for details.)

The specific condition for which the new Max Play Attempts Per Message setting is applicable is the following sequence of events:

1. A message being transmitted from the Bridge contains a tone (a DTMF tone or a background noise or voice that matches the frequencies of a DTMF tone or disconnect tone).
2. Detection of the tone by the Octel during recording causes the Octel to disconnect the call, causing the message transmission to fail.
3. The Octel does not deliver the incomplete message transmission to the recipient.
4. When the Bridge completes playing the message, it receives no response from the Octel.
5. The Bridge requeues the message at the front of the outgoing analog queue for delivery to the Octel.

Because the problematic tone is in the voice message itself, the unsuccessful sequence will repeat each time the Bridge attempts delivery of the message to the Octel. When this condition occurs, text similar to the following will be displayed in the Starfish logs on the Bridge server and in the call details displayed by the Cisco Unity Bridge Analog Network and Node Analyzer (BANANA) each time delivery of the message is attempted:

```

Playing Voice
Playing <Message Path>
Playing completed
Playing #
Received
Encountered communication problems with this Node
Completed delivering Messages
Received
Call Out Completed

```

After playing the # to signal completion of the message, the Bridge expects to receive DTMF tone 8 from the Octel. If viewed in BANANA, the condition is logged as “Expected data not received” in the “Save Request” state.

In Bridge 3.0(4) and earlier, the failure condition was not explicitly tracked. Each failure in the sequence caused the “Bad Connection” count for the Octel node to be incremented by 1. As successive attempts to deliver the message failed, any subsequent messages received by the Bridge from Cisco Unity for delivery to the Octel node were placed behind this message in the outbound analog queue. Eventually, when the threshold for “Attempts on Bad Connection” as configured on the System Settings page was reached, the entire outgoing analog queue for the Octel node was returned as undeliverable to Cisco Unity.

In Bridge 3.0(5) and later, the failure condition is explicitly tracked per message. Each time message delivery is unsuccessful due to this condition, the “Max Play Attempts Per Message” for a particular message is incremented by 1. As successive attempts to deliver the message fail, subsequent messages received by the Bridge from Cisco Unity for delivery to the Octel node are placed behind the message in the outbound analog queue. When the threshold for “Max Play Attempts Per Message” as configured on the System Settings page is reached for the message, only the message is returned as undeliverable to Cisco Unity. Any other messages in the analog outgoing queue for the Octel node are retained in the queue, and the next delivery attempt to the Octel node resumes with the next message in the queue.

See the considerations for “Max Play Attempts Per Message” in [Table 1 on page 11](#) for details on the new setting.

Event Viewer Warnings Enhanced

When the Bridge is unable to deliver a message to an Octel, the Bridge returns a nondelivery receipt (NDR) to the sender and logs warnings to the Event Viewer Application log. With Bridge 3.0(5), the Event Viewer warnings have been enhanced to provide details that were previously available only by using BANANA or by examining the Starfish or VPIM logs on the Bridge server.

The Bridge detects the following conditions and logs warnings in the Event Viewer:

- When the message sent from Cisco Unity contains a serial number that the Bridge does not recognize. Each Cisco Unity subscriber account must have a serial number and legacy mailbox ID in order to exchange messages with Octel subscribers. When a Cisco Unity subscriber sends a message to an Octel subscriber, the serial number of the Cisco Unity subscriber is added to the header of the message. The Bridge will not deliver a message when the serial number in the message header does not match a serial number of a Unity Node configured on the Bridge.
- When any of the analog delivery thresholds configured on the System Settings page has been hit. (The System Settings thresholds are: Attempts if Busy, Attempts on No Answer, Attempts on Bad Connection, Max Play Attempts Per Message, Max Retention Time - Normal, and Max Retention Time - Urgent.)
- When the message recording is in an invalid WAV file format (either the message was recorded using a codec that cannot be converted by the Bridge, or the WAV attachment contains no voice data).
- When the mailbox of the Octel recipient is full.
- When the recipient mailbox does not exist on the Octel node.

Failed Directory for SMTP Messages Added

On the Digital Networking page in the Bridge Administrator, you can enter a number in the field Retention Days for Temporary SMTP Messages so that copies of SMTP messages transmitted to and from the Bridge are saved for the specified number of days. Previously, copies of messages that were successfully delivered and copies of messages that could not be delivered were saved in the same directory, which made troubleshooting message delivery problems difficult.

With Bridge 3.0(5), messages that the Bridge could not deliver to Cisco Unity are stored in <Bridge Path>\Vpim\Internet\Out\Failed. Outbound messages that the Bridge successfully delivered are still stored in <Bridge Path>\Vpim\Internet\Out\Tmp. The Retention Days for Temporary SMTP Messages setting applies to both the Failed and Tmp directories. Note that when the Bridge saves a message to the Failed directory, it also logs a message in the Event Viewer Application log.

The Retention Days for Temporary SMTP Messages setting also controls the number of days that inbound messages from Cisco Unity are stored in the <Bridge Path>\Vpim\Xcode\Inbound\Tmp directory on the Bridge server. A <Bridge Path>\Vpim\Xcode\Inbound\Failed directory is also created, although it is not utilized at this time.

Fields Added to System Settings Page in Bridge Administrator

The System Settings page in the Bridge Administrator allows you to configure various aspects of the analog transmissions. [Table 1](#) lists considerations regarding the new fields on the System Settings page.

Table 1 Considerations for New Fields on the System Settings Page

Field	Considerations
Max Play Attempts Per Message	<p>Enter a number from 1 to 15 for the number of times that the Bridge will play a message when the Octel does not send the expected response that indicates the message was received OK. If the Bridge does not get the expected response from the Octel after playing the message the specified number of times, the Bridge stops trying to deliver the message, logs an error in Event Viewer, and returns an NDR to the sender. The default value is 5.</p> <p>The counter for Max Play Attempts Per Message is on a per-message basis. The counter is reset to 0 when the message is either successfully transmitted or returned as undeliverable.</p> <p>Note that when the counter for Max Play Attempts Per Message is incremented, the counter for Attempts on Bad Connection is also incremented. Therefore, you should set the number for Max Play Attempts Per Message to be less than the number set for Attempts on Bad Connection so that only the problematic message is returned as undeliverable. (When the Attempts on Bad Connection threshold is hit, all messages queued for delivery to the node are returned to the senders.)</p>
Max Retention Time - Normal	<p>Enter a number from 1 to 48 for the number of hours that a normal priority message is queued on the Bridge for analog delivery before being returned to the sender as undeliverable. If the Bridge cannot send the message within the specified time period, the Bridge stops trying to deliver the message, logs an error in Event Viewer, and returns an NDR to the sender.</p> <p>The default value is 48 hours. However, you may want to lower this setting so that a problematic message is returned as undeliverable before the Attempts on Bad Connection threshold is hit (which results in all messages queued for delivery to the node to be returned to the senders). By doing so, the Bridge can handle situations where a particular message is causing a transmission failure.</p>
Max Retention Time - Urgent	<p>Enter a number from 1 to 48 for the number of hours that an urgent message is queued on the Bridge for analog delivery before being returned to the sender as undeliverable. If the Bridge cannot send the message within the specified time period, the Bridge stops trying to deliver the message, logs an error in Event Viewer, and returns an NDR to the sender.</p> <p>The default value is 12. However, you may want to lower this setting so that a problematic message is returned as undeliverable before the Attempts on Bad Connection threshold is hit (which results in all messages queued for delivery to the node to be returned to the senders). By doing so, the Bridge can handle situations in which a particular message is causing a transmission failure.</p>

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(5), confirm that the account with which you log on to the Bridge server has permission to access the Bridge Administrator.



Caution

If the account is 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.

If access is denied, it is possible that the account 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 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 Bridge Release 3.0(5) 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(5)

Table 2 Cisco Unity Bridge Release 3.0(5) Open Caveats

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>
CSCef20968	3	bridge	<p>A remote node communicating with the Bridge places multiple calls in succession that appear to have errors when viewed via the BANANA utility in Cisco Unity Bridge versions 3.0(x).</p> <p>A currently unknown condition on the remote node causes the first call for delivery of a multiple-recipient message to disconnect after delivering the message successfully to the first recipient. Subsequent calls from the remote node will continue to deliver the message for each recipient.</p> <p>There is no workaround.</p>

Table 2 Cisco Unity Bridge Release 3.0(5) Open Caveats (continued)

Caveat Number	Severity	Component	Description
CSCef39470	3	bridge	<p>Voice messages from Cisco Unity subscribers to subscribers on remote Octel systems are not being delivered. The Queue Status page of the Bridge server shows messages queued for delivery to Octel Nodes, but the Bridge does not appear to be attempting outbound calls. Delivery schedules for the Octel Nodes have been checked and are such that the delivery of these messages should have been attempted at least once. Inbound message delivery calls from remote Octel nodes are successfully processed.</p> <p>This behavior has been observed on a Bridge server after a previously active Octel Node profile on the Bridge server has been recently deleted.</p> <p>Workaround</p> <p>On the Octel Node profile on the Bridge for each node for which outbound analog messages are queued, verify that Octel Node delivery schedules are active and configured such that the message delivery should be attempted.</p> <p>Use BANANA to confirm that there are actually no outbound calls being attempted, i.e. that the conditions aren't actually that the Bridge is attempting outbound calls but without success.</p> <p>Reboot the Bridge server. This will resynchronize the Bridge callout process with the current Octel Node database and the messages should be delivered.</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>
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 Caveats—Release 3.0(5)

Table 3 Cisco Unity Bridge Release 3.0(5) Resolved Caveats

Caveat Number	Severity	Component	Description
CSCee53623	2	bridge	Audio delivered to Unity via Voice Connector has varied volume level.
CSCef27921	3	bridge	Bridge: detect and discard null WAV attachment from Unity.
CSCee62714	6	bridge	Message delivery fails when an outbound message contains a DTMF or disconnect tone.

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.

Enabling the Bridge Server to Send Extended-Absence Delivery Receipts: *Cisco Unity Bridge Networking Guide*

For Cisco Unity 4.0(4) subscribers to receive delivery receipts when the extended-absence greeting for an Octel subscriber is enabled and the mailbox is accepting messages, you need to modify the Vpim configuration file on the Bridge server, then restart the Digital Networking service. The procedure in the *Cisco Unity Bridge Networking Guide, Release 3.0* omits the step of restarting the Digital Networking service.

The procedure appears in the following sections and chapters of the *Cisco Unity Bridge Networking Guide, Release 3.0* (available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/bnet30/index.htm):

- In the “Finishing the Setup” section in the “Setting Up Cisco Unity and the Bridge for Networking” chapter.
- In the “Upgrading from Bridge 2.x to Bridge 3.x” chapter.
- In the “Upgrading from Cisco Unity 4.0(3) with Bridge 3.x” chapter.

The following version of the procedure includes all of the steps.

To Enable the Bridge to Send Extended-Absence Delivery Receipts (Cisco Unity 4.0(4) Only)

-
- Step 1** On the Bridge server, make a backup copy of the file <Bridge Path>\Vpim\Vpim.cfg.
- Step 2** Open the file <Bridge Path>\Vpim\Vpim.cfg with Notepad.
- Step 3** Search for **EnableExtAbsenceNotifications**. You should see text similar to:

```
[config]
POP3_SERVER_ID=
ESMTP_SERVER_ID=
```

```
InetRecvProtocol=1
POP3_POLL_INTERVAL_MS=600000
OUTDIAL_INTERVAL_MS=600000
CALLX_IN_POLL_INTERVAL_MS=30000
PROXY_MAILBOX_MESSAGE=IMCEAOMNI-AvVoiceMessage
PROXY_MAILBOX_DIRECTORY=IMCEAOMNI-AvVoiceAddress
EnableExtAbsenceNotifications=0
SMTP_PORT=25
```

- Step 4** Go to the line containing **EnableExtAbsenceNotifications=0**, and change the **0** to a **1**.
- Step 5** Save and close the file.
- Step 6** Restart the Digital Networking service for the setting to take effect:
- On the Windows Start menu, click **Programs > Administrative Tools > Services**.
 - In the right pane, right-click **Digital Networking**, and click **Restart**.
 - Close the Services console.
-

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 CiscoUnityBridge3.0.5ServicePacks.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.
-

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 any updates that you downloaded.

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-UpdatesForIE.exe**.
- Step 4** Repeat [Step 2](#) for the Internet Explorer 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.