



Release Notes for Cisco Unity Bridge Release 3.0(6)

Published May 6, 2005

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(6).

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 to Note from Earlier Cisco Unity Bridge 3.0\(x\) Release Notes, page 3](#)
- [Downloading the Software for a Cisco Unity Bridge Installation or Upgrade, page 4](#)
- [Upgrading to Cisco Unity Bridge 3.0\(6\) from 3.0\(x\), page 5](#)
- [Upgrading to Cisco Unity Bridge 3.0\(6\) from 2.x, page 8](#)
- [New and Changed Requirements and Support—Release 3.0\(6\), page 8](#)
- [New and Changed Functionality—Release 3.0\(6\), page 9](#)
- [Installation and Upgrade Notes, page 11](#)
- [Limitations and Restrictions, page 11](#)
- [Caveats, page 12](#)
- [Cisco Unity Documentation, page 14](#)
- [Obtaining Documentation, page 15](#)
- [Documentation Feedback, page 16](#)
- [Cisco Product Security Overview, page 16](#)



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

- [Obtaining Technical Assistance, page 17](#)
- [Obtaining Additional Publications and Information, page 18](#)

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* 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.
-

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

This section contains information worth noting from the release notes of Cisco Unity Bridge versions earlier than 3.0(6). 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) 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.

Downloading the Software for a Cisco Unity Bridge Installation or Upgrade

The software required to install or upgrade to Bridge version 3.0(6) 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(6) 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 **CiscoUnityBridge3.0.6.exe**, and follow the on-screen prompts.
- Step 6** Return to the Cisco Unity Bridge Software Download page.
- Step 7** Click the file **CiscoUnityBridge3.0.6ServicePacks.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:
- In Windows Explorer, double-click the file.
 - 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*. The Domino version of the guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/big/dom/index.htm. The Exchange version of the guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/big/ex/index.htm.

Upgrading to Cisco Unity Bridge 3.0(6) from 3.0(x)

If the Windows fax service is running or enabled on the Bridge server, you must disable it to prevent it from interfering with the Brooktrout software before upgrading the Bridge software. In addition, 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 six procedures, as applicable, in the order listed.

To Disable the Windows Fax Service

- Step 1** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 2** In the right pane, double-click **Fax Service**.
- Step 3** In the Fax Service Properties dialog box, click the **General** tab.
- Step 4** In the Startup Type list, click **Disabled**.
- Step 5** Click **OK** to close the Fax Service Properties dialog box.
- Step 6** Close the Services MMC.

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 in which you extracted CiscoUnityBridge3.0.6ServicePacks.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(6) 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/ex/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 appears, 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(6) 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(6) from Bridge 2.x, refer to the “Upgrading from Bridge 2.x to Bridge 3.x” chapter of the *Cisco Unity Bridge Networking Guide (With Microsoft Exchange), Release 3.0* at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/ex/index.htm.

New and Changed Requirements and Support—Release 3.0(6)

This section contains information on new and changed support in the Cisco Unity Bridge Release 3.0(6) 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/voicewsw/ps2237/prod_release_notes_list.html.

Cisco Security Agent for Cisco Unity Bridge Version 1.1(4)

Cisco Security Agent for Cisco Unity Bridge version 1.1(4) is qualified for use with Cisco Unity Bridge 3.0(x). The application combines host intrusion detection and prevention, malicious mobile code protection, and operating system integrity assurance.

For requirements and other information on using Cisco Security Agent for Cisco Unity Bridge, refer to *Release Notes for Cisco Security Agent for Cisco Unity Bridge, Release 1.1(4)* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bsecagent/bsa114rn.htm.

For information on the full Cisco Security Agent product, refer to the product website at <http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html>.

Required Versions of Cisco Unity with IBM Lotus Domino

Bridge version 3.0(6) is supported only with Cisco Unity 4.0(5) and later with Domino. In installations with multiple Cisco Unity servers, all the servers must be upgraded to Cisco Unity 4.0(5) or later.

Required Versions of Cisco Unity with Microsoft Exchange and the Voice Connector for Exchange

Bridge version 3.0(6) is supported only with Cisco Unity 4.0(3) and later with Exchange and Cisco Unity Voice Connector for Microsoft Exchange 2000 version 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 the Bridge server is running version 2.x, do not upgrade to version 3.0(6) 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 (With Microsoft Exchange), 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/ex/index.htm.

New and Changed Functionality—Release 3.0(6)

This section contains information on new and changed functionality for Cisco Unity Bridge Release 3.0(6) 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.

Acceptance of Requests to Push Mailbox Information to the Bridge

By default, the Bridge will attempt to retrieve name information for remote Octel subscribers when needed. Some remote systems may also provide the capability to push name information to other nodes; Cisco Unity Bridge version 3.0(6) provides the capability to accept this mailbox information and update the Bridge directory and the Bridge subscriber directory in Cisco Unity. Although the Bridge can now accept push requests from other nodes, it will not attempt to push mailbox information to other nodes.

The Accept Remote Push check box on the System Settings page in the Bridge Administrator allows you to specify acceptance of remote name pushes from Octel nodes. By default, this box is unchecked, and thus the Bridge will reject an attempt by the remote node to push mailbox information (but the call will proceed and the remote node will be able to continue with any additional tasks).

When the Accept Remote Push check box is checked, the Bridge will accept all administrative name push requests from any remote node, and will process the directory information even if the recorded name is not included in the transmission. If the mailbox information sent by the remote node does not match any existing mailbox in the Bridge directory, a new usage-based entry is added to the directory. If the information pertains to a mailbox that already exists in the Bridge directory, the Bridge will modify the directory entry; if the text name is blank or no recorded name is transmitted, the corresponding field will be removed from the directory entry.

Note that, before enabling this feature, you should be familiar with the voice messaging system models, versions, configuration, and subscriber population of each remote node that may push mailbox information to the Bridge, to ensure that any increased call processing and directory activity related to acceptance of non-solicited mailbox information by the Bridge does not delay or block message delivery or result in a larger Bridge subscriber directory than your Cisco Unity and Cisco Unity Bridge deployment was designed to support. Refer to the documentation for the particular model of each remote voice messaging system for additional information on support for and mechanisms used in pushing mailbox information via Octel analog networking.

Enable Extended Absence Notification Setting Added to the Bridge Administrator

Cisco Unity Bridge version 3.0(5) included the ability to notify Cisco Unity subscribers when an Octel recipient has enabled an extended-absence greeting, and to indicate whether or not the message was accepted in such a case. In version 3.0(6), the Enable Extended Absence Notifications check box has been added to the Digital Networking page in the Bridge Administrator to enable this feature. (Previously, the feature was enabled by editing a configuration file and restarting the Digital Networking service.)

This functionality requires that you enable the Bridge server to send the notification. You do not need to restart the Digital Networking service when using the check box to enable the notification.

Note that when the Bridge is used in conjunction with Cisco Unity with Exchange, the functionality also requires that all Cisco Unity servers are running version 4.0(4) or later, and that you install Cisco Unity Voice Connector for Microsoft Exchange 2000 version 11.0(2) or later.

Retrieving or Confirming Octel Serial Numbers

The GetSN command-line utility has been added for Cisco Unity Bridge version 3.0(6). This utility allows you to retrieve or confirm the serial number of a remote Octel location.

The utility is located in the <Bridge>\Starfish\bin directory, and it must be run from this directory. You must stop the Unity Bridge service prior to running the utility. To get the serial number of an Octel system, run GetSN and specify the phone number for the system on the command line. Commas can be used in the dial string to specify a pause. For example:

```
GetSN 9,5552900
```

Silence Detection and Trimming for Audio Received from Remote Systems

Delays inherent in the analog transmission of audio and control messages can cause noticeable amounts of silence to be added to recordings made by the Bridge. In version 3.0(6) and later, the Bridge automatically detects and trims leading and trailing silence on both recorded names and recorded voice messages that are received from remote systems via the Octel analog network.

Alternatively, the Silence Trimmer tool can be used to remove silence from recordings that are stored on a Cisco Unity server (for example, the recorded names stored on the bridgehead server). This utility requires Cisco Unity version 4.0(2) or later; because it does not run on the Bridge server, it can be used in deployments where earlier versions of the Bridge are in use. However, the utility acts only on existing audio files, and therefore will not affect recordings that are made after the utility is run. The utility is available at http://ciscounitytools.com/App_SilenceTrimmer.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*. The Domino version of the guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/big/dom/index.htm. The Exchange version of the guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/big/ex/index.htm.

For detailed information on configuring Bridge Networking, refer to the *Cisco Unity Bridge Networking Guide, Release 3.0*. The Domino version of the guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/dom/index.htm. The Exchange version of the guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/ex/index.htm.

Verify Logon Account Access to the Bridge Administrator Before an Upgrade

Before upgrading the Bridge software to version 3.0(6), 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 (With Microsoft Exchange), Release 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/ex/index.htm.)

Windows Fax Service Must Be Disabled Prior to Installing or Upgrading Bridge Software

If the Windows fax service is running or enabled while you are attempting to install or upgrade the Bridge software to version 3.0(6), you will see an error indicating that you must stop and disable the service. You disable the Windows fax service to prevent it from interfering with Brooktrout software.

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*. The Domino version of the guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/dom/index.htm. The Exchange version of the guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/bnet/ex/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(6) 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(6)

Table 1 Cisco Unity Bridge Release 3.0(6) 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 1 Cisco Unity Bridge Release 3.0(6) Open Caveats (continued)

Caveat Number	Severity	Component	Description
CSCeg19346	3	bridge	<p>The Cisco Unity Bridge is taking calls and processing messages successfully from remote Octels, but messages sent from Cisco Unity outbound to remote Octels are not being delivered. The Queue Status page of the Bridge Administrator shows that the messages are queued to be delivered to the remote Octels, but calls are not being placed to deliver them.</p> <p>This behavior was observed on Cisco Unity Bridge 3.0(5). The delivery of messages queued for remote Octels appears to have stopped at the same time as the system clock fell back from 2:00am to 1:00am 10/31/04 transitioning from daylight savings time to standard time. The behavior occurred only on one of many Bridges under the exact same conditions. It is believed this is due to a problematic time window that can occur whenever the system time of the Bridge server is rolled backwards for any reason. The likelihood of the problem occurring is unknown at this time.</p> <p>Workaround</p> <p>Try to stop the Unity Bridge service via the Windows Services MMC. If the service will not stop (that is, the stop request times out), make sure there are no calls in process by using the Line Status page of the Bridge Administrator.</p> <p>If there are calls in progress, let them finish, then refresh the Windows Services MMC to see if the service is stopped. If there are no calls in progress, and the Windows Services MMC still shows the Unity Bridge service is in a Stopping state:</p> <ol style="list-style-type: none"> 1. Open the Windows Task Manager. 2. Click the Processes tab. 3. Click Starfish.exe. 4. Click End Process. 5. In the warning dialog box, click Yes to terminate the process. 6. Exit the Windows Task Manager. <p>The Unity Bridge service should restart within 60 seconds. If the Unity Bridge service does not restart within 60 seconds, or if the initial shutdown request via Windows Services MMC was successful, manually restart the Unity Bridge service.</p> <p>Within a few minutes, delivery of outbound messages to remote Octel servers should resume as normal. Monitor the Bridge Administrator Queue Status page to verify that the number of queued messages is decreasing.</p>

Table 1 Cisco Unity Bridge Release 3.0(6) Open Caveats (continued)

Caveat Number	Severity	Component	Description
CSCeg61174	3	bridge	<p>The Cisco Unity Bridge License wizard freezes when you are browsing for a license file to add, and you select the My Documents directory, which is immediately below Desktop.</p> <ol style="list-style-type: none"> 1. Open the Windows Task Manager. 2. Click the Processes tab. 3. Click CiscoLicFileWiz.exe. 4. Click End Process. 5. In the warning dialog box, click Yes to terminate the process. 6. Exit the Windows Task Manager. <p>Move the license file to a location other than the My Documents directory. Rerun the Cisco Unity Bridge License wizard and select the license file from the new location.</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>

Resolved Caveats—Release 3.0(6)

Table 2 Cisco Unity Bridge Release 3.0(6) Resolved Caveats

Caveat Number	Severity	Component	Description
CSCef39470	3	bridge	Bridge: Deletion of Octel Node stalls callout process
CSCef77936	3	bridge	Apostrophe in name causes failure with mbupload
CSCef90550	3	bridge	Bridge: SIT Intercept tone not recognized appropriately
CSCeg45985	3	bridge	Bridge-Sent time on messages one hour too early
CSCef21474	6	bridge	Message delivery fails when inbound message to Bridge contains DTMF tone

Cisco Unity Documentation

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

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

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

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_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/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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



Tip

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

<http://www.cisco.com/techsupport>

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

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



Note

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

Submitting a Service Request

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

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

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

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

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

Definitions of Service Request Severity

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

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

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

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

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

<http://www.ciscopress.com>

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

<http://www.cisco.com/packet>

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

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

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

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

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)

© 2005 Cisco Systems, Inc. All rights reserved.

