



Troubleshooting Bridge Networking

Overview: Bridge Troubleshooting

See the following sections for information about troubleshooting message delivery and directory synchronization problems that occur between Cisco Unity and the Bridge:

- [Configuration Problems, page 6-1](#)
- [Overview of Troubleshooting Logs, Traces, and Tools, page 6-3](#)
- [Messages Are Not Delivered from Cisco Unity to Octel, page 6-5](#)
- [Messages Are Not Delivered from Octel to Cisco Unity, page 6-24](#)
- [Directory Messages Are Not Processed, page 6-44](#)

Configuration Problems

If you have just configured Cisco Unity and the Bridge for networking, and you encounter problems, review the following list to verify that your configuration follows all of these basic guidelines. If needed, go to the [“Messages Are Not Delivered from Cisco Unity to Octel”](#) section on page 6-5 or the [“Messages Are Not Delivered from Octel to Cisco Unity”](#) section on page 6-24 as applicable for detailed troubleshooting steps.

Verify the following:

1. The Cisco gateway is supported. The only supported Cisco gateways are those listed in the “Supported Cisco Gateways” section of *Cisco Unity Bridge System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm.
2. The DTMF duration and interdigit timing settings for Cisco CallManager and gateways have been set to 100 milliseconds. (Any value within the range of 80 and 100 milliseconds is fine.) In some versions of Cisco CallManager, the default value for the H225 DTMF Duration parameter is 300 milliseconds, which causes problems for the Bridge. Refer to the applicable Cisco documentation for details on locating and changing the applicable parameters in Cisco CallManager and the gateways.
3. The Octel server(s) are supported. The only supported Octel servers are those listed in *Cisco Unity Bridge System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm.

4. The Octel server(s) are running a supported protocol. The Octel servers must be running Octel analog networking. Neither Octel digital networking nor the VOICENET protocol is supported by the Bridge.
5. The name of the Bridge server can be resolved. If there are name resolution problems, you need to reconfigure DNS or add a reference to the Bridge server in the HOSTS file on the server on which the Voice Connector is installed and/or on the server that sends outbound SMTP messages to the Bridge server. See the [“Configuring the Bridge and Testing the Configuration”](#) section on page 2-16 for more information.
6. The license file is installed on the Bridge server. See the [“Obtaining a License File for the Bridge Server”](#) section on page 3-4 and the [“Installing the License File Wizard and the License File”](#) section on page 3-12.
7. The Active Directory schema is extended. Confirm that the schema was successfully extended by checking the log file that ADSchemaSetup creates on the desktop.
8. The correct version of the Voice Connector is installed. The Voice Connector for Exchange 2000 is the only Voice Connector supported for Bridge Networking. Voice Connector version 11.0(1) or later is required with Cisco Unity Bridge 3.0. Also verify that the Voice Connector settings are correctly configured, as described in the [“To Verify Voice Connector Settings”](#) section on page 6-19.
9. A Cisco Unity server is configured as the bridgehead. If ConfigMgr has not been run on a Cisco Unity server:
 - The CsBridgeConnector service will fail to start.
 - The Bridge-related pages and fields in the Cisco Unity Administrator will not be accessible.See the [“Designating the Bridgehead Server”](#) section on page 2-10.
10. Search scopes include the Cisco Unity bridgehead server. The Subscriber and Blind Addressing search scopes (which are set on the Network > Primary Location > Addressing Options page in the Cisco Unity Administrator) must be set to either the dialing domain or global level. This must be done for each Cisco Unity server in the network. The search scopes for the auto-attendant and directory handlers (which are configured separately) must also include the Cisco Unity bridgehead server.
11. Each Bridge delivery location is correctly configured.
12. Each Unity node and Octel node on the Bridge server is correctly configured. To verify the serial number of an Octel node based on the phone number of the node, see the [“Optional: Gathering or Confirming Octel Node Serial Numbers \(Bridge 3.0\(6\) or Later\)”](#) section on page 2-5.
13. The correct serial number and legacy mailbox ID is assigned to each Cisco Unity subscriber.
14. The Active Directory Connector is correctly configured. In organizations where Exchange 5.5 co-exists with either Exchange 2000 or Exchange 2003, the Connection Agreements for the Active Directory Connector must be carefully configured. If users on the Exchange 5.5 server experience problems addressing messages to Bridge subscribers, confirm that the Active Directory Connector is configured correctly.

Overview of Troubleshooting Logs, Traces, and Tools

This section provides a summary of the logs, traces, and other tools available for troubleshooting message delivery and directory synchronization problems between Cisco Unity and the Bridge. For descriptions of the tools, see the following sections:

- [Tools for Troubleshooting Communication Problems Between the Bridge and the Octel Nodes, page 6-3](#)
- [Tools for Troubleshooting Communication Problems Between the Bridge and Cisco Unity, page 6-4](#)
- [Tools for Troubleshooting Problems with the Voice Connector, page 6-5](#)
- [Tools for Troubleshooting Problems in Exchange, page 6-5](#)
- [Tools for Troubleshooting Directory Synchronization Problems on the Cisco Unity Server, page 6-5](#)

Details on when and how to use the troubleshooting tools are in the following sections:

- [Messages Are Not Delivered from Cisco Unity to Octel, page 6-5](#)
- [Messages Are Not Delivered from Octel to Cisco Unity, page 6-24](#)
- [Directory Messages Are Not Processed, page 6-44](#)

Tools for Troubleshooting Communication Problems Between the Bridge and the Octel Nodes

This section provides a summary of the logs, traces, and other tools available for troubleshooting communication problems between the Bridge and the Octel nodes.

- **Bridge Analog Network And Node Analyzer (BANANA)**—BANANA is a stand-alone application that runs on the Bridge server. It is designed to assist with monitoring and troubleshooting analog communication between the Bridge and Octel nodes in the analog network. It also provides detail and summary call activity information. BANANA monitors and parses the call traces described below, and presents the data in a format that makes the call traces easier to understand. BANANA is available on the Bridge CD. We recommend that you install it.
- **Call Traces**—(Also referred to as the Starfish logs or SFLOGs.) The files are located on the Bridge server in the <Bridge Path>\Starfish\Log directory. To obtain information about messages coming from or going to Octel servers through the Bridge voice-fax card(s), you increase the Call Tracing Level on the System Settings page in the Bridge Administrator. The log records actions that the Bridge service attempts, notes whether those actions are completed successfully, and records the reasons for failed actions. Within the Log directory are files named SFLOG.YYYYMMDD.LOG, where YYYY is the year, MM is the month, and DD is the day. Each file contains log entries for one hour of the day; the filename indicates which hour. The directory also contains the log file SFLOG.LOG, to which the Bridge server adds current entries, and which is then saved to the applicable hour log. Log files that are older than 24 hours are overwritten.

Each entry in the log files begins with the word “SFLOG,” followed by a number, the date and time, the line number used by the call, and an action. For example:

```
SFLOG 1396 1700 2002/11/26-22:59:18.384 00000008 Line 3: Call Out Process Initiated for Node 80200 Window Type 0
SFLOG 1396 1700 2002/11/26-22:59:18.384 00000008 Line 2: Call Out Process Initiated for Node 80200 Window Type 0
SFLOG 1396 1700 2002/11/26-22:59:22.960 00000100 Line 3: Call Status = Answer
```

In the example log above, a call went out on line 3, another call went out on line 2, and then the Octel answered the call that was initiated on line 3. Although you can use Notepad to view the call traces, we recommend that you use BANANA instead. BANANA parses the logs and presents them in a format that allows you to more easily follow the progress of a call.

- **Call Queue Logs**—Call Queue log files are located on the Bridge server in the <Bridge Path>\Starfish\Log directory. The Call Log Retention setting on the Systems Settings page allows you to specify the number of days that logs are saved. A separate file is used for each day. Files are named CallLog_YYYYMMDD.LOG where YYYY is the year, MM is the month and DD is the day. Call logs are used by the Bridge Traffic Analyzer for generating reports on Bridge activity.
- **Line Status Page**—The Line Status page in the Bridge Administrator allows you to monitor status information for the phone lines of the Bridge server as it communicates with Octel servers. It also allows you to enable or disable specific phone lines for the Bridge server.
- **Queue Status Page**—The Queue Status page in the Bridge Administrator allows you to monitor status information in the outbound message queue on the Bridge server.
- **Bridge Traffic Analyzer**—The Bridge Traffic Analyzer is a report generation utility that reads the call queue log files on the Bridge server and generates a graph and a summary table that can be saved as a comma-separated value (CSV) file. The Bridge Traffic Analyzer is available in Tools Depot on the Cisco Unity server, or you can download it from <http://www.CiscoUnityTools.com>. This tool typically is used for monitoring purposes and not for troubleshooting. However, if messages are not getting delivered in a timely manner, this tool will help you understand Bridge port utilization. See the “[Bridge Traffic Analyzer](#)” section on page 5-4 for more information.
- **Event Viewer**—The Bridge services record errors and warnings to the Windows Event Viewer application log. The Windows Event Viewer on the Bridge server should be one of the first places you look when troubleshooting.

Tools for Troubleshooting Communication Problems Between the Bridge and Cisco Unity

- **Event Viewer**—The Bridge services record errors to the Windows Event Viewer application log.
- **Temporary SMTP Messages**—On the Bridge Administrator Digital Networking page, set Retention Days For Temporary SMTP Messages to a non-zero value. Subsequently, temporary SMTP messages are stored on the Bridge server in the following directories:
 - <path>\VPIM\Xcode\Inbound\Tmp—Messages from Cisco Unity are stored in this directory. If messages appear in this directory, you know that messages are getting to the Bridge from Cisco Unity.
 - <path>\VPIM\Internet\Out\Tmp directory—Messages to Cisco Unity are stored in this directory. If messages appear in this directory, you know that messages from Octel have made it this far.
- **VPIM Traces**—Trace files are located on the Bridge server in the <path>\VPIM\Trace directory. Increase the Tracing Level on the Digital Networking page in the Bridge Administrator to obtain information about messages coming from or going to Cisco Unity. Within the Trace directory are the files VPIM.mmdtttt.LOG. Each file contains log entries for one hour of the day; the filename indicates which hour.
- **VPIM Message Log**—Related to the VPIM Traces is the log file VpimMsg.log, which is located on the Bridge server in the <path>\VPIM\MsgLog directory. The Bridge server adds current entries, and saves the applicable hour trace file. Log files that are older than 24 hours are overwritten.

Tools for Troubleshooting Problems with the Voice Connector

- **Voice Connector Log File**—The Voice Connector logs are located on the Exchange server on which the Voice Connector is installed in the directory <ExchangeServerPath>\VoiceGateway\LogFiles. The files are named in the format GwIvc_<YyMmDd>.log, where Yy is the year, Mm is the month, and Dd is the day.
- **Event Viewer**—The Voice Connector service records some errors to the Windows Event Viewer logs on the Exchange server on which it is installed.

Tools for Troubleshooting Problems in Exchange

- **Exchange Message Tracking Tool**—This tool is available in the Exchange System Administrator.
- **Exchange SMTP Logging**—You enable SMTP logging from within the Exchange System Administrator.

Tools for Troubleshooting Directory Synchronization Problems on the Cisco Unity Server

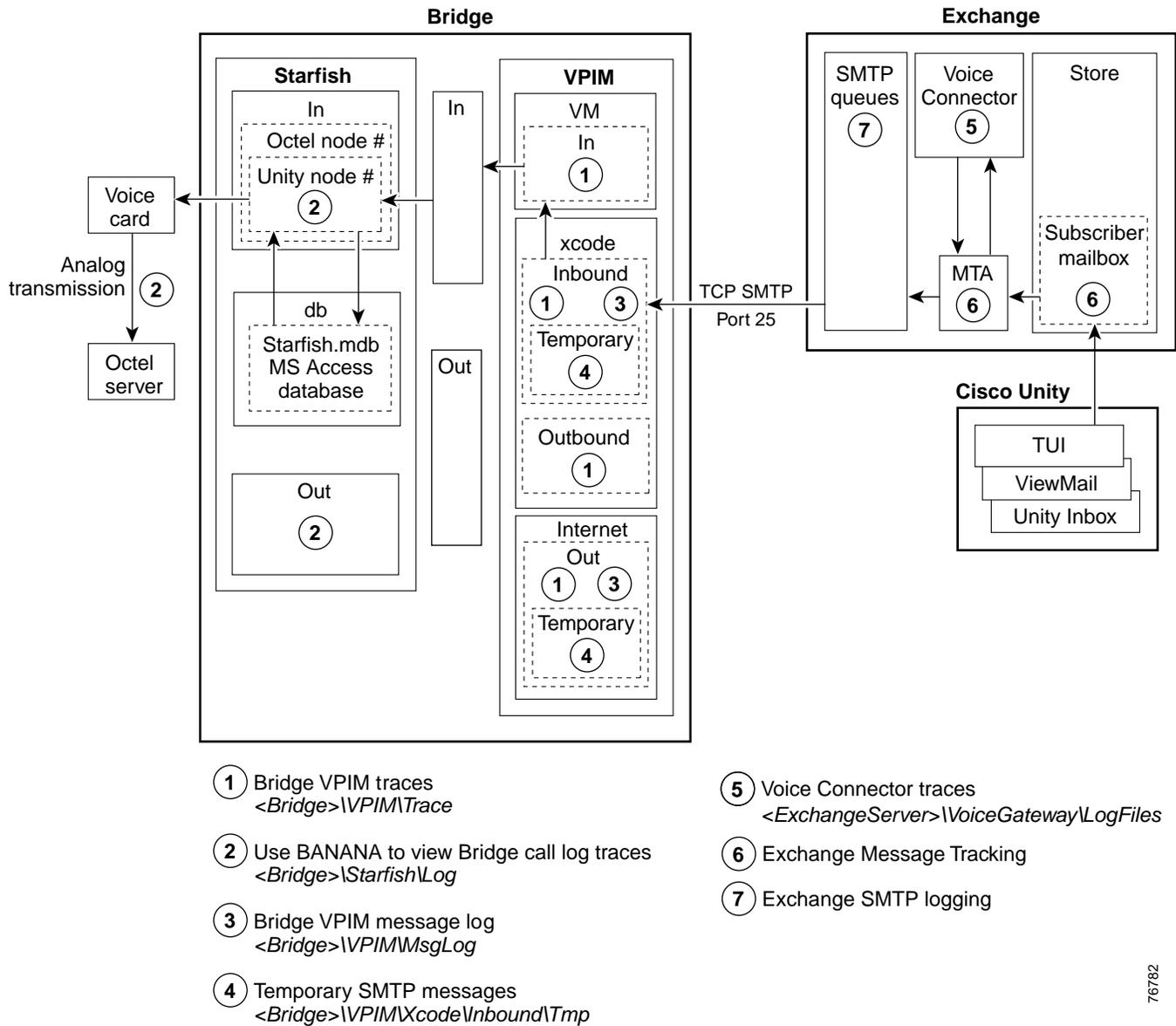
- **Event Viewer**—The CsBridgeConnector service, which is responsible for keeping the directories on the Bridge and Cisco Unity synchronized, logs several errors to the Windows Event Viewer application log on the Cisco Unity bridgehead server (that is, the Cisco Unity server that is configured for networking with the Bridge).
- **Sent/Received vCard Data**—This data, which can help you troubleshoot directory synchronization problems, is located on the Cisco Unity server in \CommServer\MsgArchive.
- **CsBridgeConnector Traces**—Use the Unity Diagnostic tool to set the applicable CsBridgeConnector macro traces to troubleshoot directory synchronization problems. This tool is available on the Windows Start menu (click Programs > Cisco Unity > Unity Diagnostic Tool).

Messages Are Not Delivered from Cisco Unity to Octel

This section provides troubleshooting information to help you determine why voice messages from Cisco Unity are not received on an Octel system. When a Cisco Unity subscriber sends a voice message to an Octel subscriber, the message is passed by Cisco Unity to the Exchange MTA, which hands the message over to the Voice Connector. The Voice Connector converts the message to VPIM format (with proprietary extensions) and hands it back to Exchange to be sent to the Bridge via SMTP.

[Figure 6-1](#) illustrates at a high level the message flow from Cisco Unity to Octel, and the troubleshooting logs, traces, and tools that you can use to determine where the problem is along the path. For simplicity, the illustration shows messages originating from subscriber mailboxes. This is true when subscribers use ViewMail for Outlook or the Cisco Unity Inbox to send messages, but when subscribers use the TUI, the messages originate from the Exchange partner server.

Figure 6-1 Troubleshooting Message Flow from Cisco Unity to Octel



76782

Bridge In and Out Directories

Note the Bridge\In and Bridge\Out directories in [Figure 6-1](#).

Conceptually, these directories divide the Bridge into the SMTP side and the analog side. The Unity Bridge service controls messages on the analog side, and the Digital Networking service controls messages on the SMTP side. Bridge\In and Bridge\Out are transitional directories. Messages from Cisco Unity are delivered to the Bridge\In directory by the Digital Networking service, where they are picked up by the Unity Bridge service for delivery to the Octels. In the other direction, messages from the Octels are delivered to the Bridge\Out directory by the Unity Bridge service, where they are picked up by the Digital Networking service for delivery to Cisco Unity via Exchange. If either service is stopped for some reason, messages will queue up as shown in the following table.

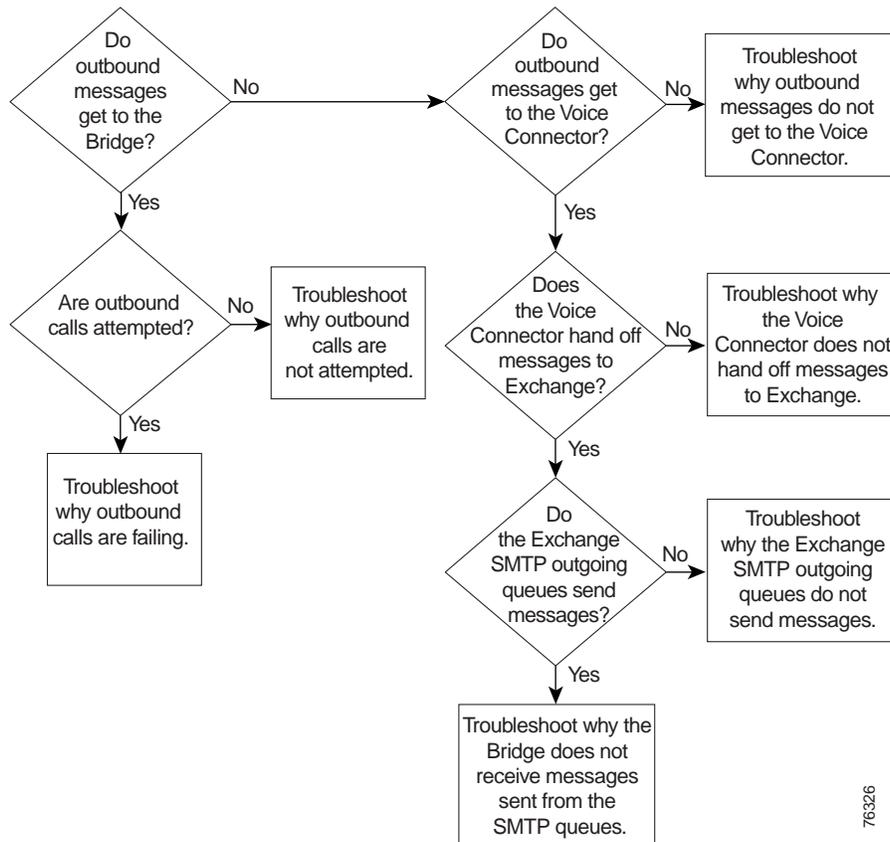
Table 6-1 Messages Queue Up When the Unity Bridge Service and/or the Digital Networking Service Stop

Digital Networking Service	Unity Bridge Service	Messages from Cisco Unity to the Octels...	Messages from the Octels to Cisco Unity...
Running	Not Running	Will queue up in the Bridge\In directory until the Unity Bridge service starts and picks them up.	Will queue up on the Octel servers.
Not Running	Running	Will be stuck in the Exchange SMTP outgoing queues.	Will queue up in the Bridge\Out directory until the Digital Networking service starts and picks them up.
Not Running	Not Running	Will be stuck in the Exchange SMTP outgoing queues.	Will queue up on the Octel servers.

Troubleshooting Why Messages Are Not Delivered from Cisco Unity to Octel

Figure 6-2 illustrates the troubleshooting process at a high level.

Figure 6-2 Troubleshooting Why Messages Are Not Delivered from Cisco Unity to Octel



76326

The following list provides an overview of the troubleshooting steps. Detailed procedures and troubleshooting steps follow the list.

1. Enable the various logs and traces as described in the [“Enabling Logs and Traces” section on page 6-8](#).
2. If you are tracking down problems with messages that have already been sent, skip to the next step to begin troubleshooting. Otherwise, send a test message from a Cisco Unity subscriber to a remote Octel subscriber. Make a note of the serial number of the receiving Octel node.
3. [Do Messages from Cisco Unity Get to the Bridge?](#) If messages do not get to the Bridge, skip to Step 6.
4. [Are Outbound Calls Attempted?](#) If outbound calls are not attempted, go to the [“Troubleshooting Why Outbound Calls Are Not Attempted” section on page 6-12](#).
5. Determine why calls from the Bridge to the Octels are failing. Go to the [“Troubleshooting Why Outbound Calls Are Failing” section on page 6-13](#).
6. [Do Outbound Messages Get to the Voice Connector?](#) If the Voice Connector does not receive messages, go to the [“Troubleshooting Why Outbound Messages Do Not Get to the Voice Connector” section on page 6-19](#).
7. [Does the Voice Connector Hand Off Messages for Pickup by the SMTP Service?](#) If the Voice Connector does not hand off messages, go to the [“Troubleshooting Why the Voice Connector Does Not Hand Off Messages to Exchange” section on page 6-20](#).
8. [Do the Exchange SMTP Outgoing Queues Attempt to Send Messages?](#) If the Exchange SMTP queues do not send messages, use Exchange message tracking and look for messages with a Recipient address beginning with either “OMNI:” or “IMCEAOMNI-.” Otherwise, go to the [“Troubleshooting Why the Bridge Does Not Receive Messages Sent from the Exchange SMTP Queues” section on page 6-22](#).
9. Reset the logs and traces as described in the [“After You Finish Troubleshooting” section on page 6-23](#).

Enabling Logs and Traces

Before you begin sending test messages to track down the problem, do all of the following procedures to enable the applicable logs, traces, and other troubleshooting tools:

- [To Install BANANA, page 6-8](#)
- [To Enable Troubleshooting Logs and Traces on the Bridge Server, page 6-9](#)
- [To Increase the Voice Connector Logging Level, page 6-9](#)
- [To Enable Message Tracking in Exchange 2000, page 6-10](#)
- [To Enable SMTP Logging in Exchange 2000, page 6-10](#)

To Install BANANA

If you have not already done so during the Bridge Networking setup, install the Bridge Analog Network And Node Analyzer (BANANA).

-
- Step 1 Disable virus scanning services and the Cisco Security Agent service, if applicable.
 - Step 2 Insert the Cisco Unity Bridge compact disc in the CD-ROM drive, and browse to the **BANANA** directory.

- Step 3 Double-click **setup.exe**.
- Step 4 Click **OK** at the welcome screen.
- Step 5 If applicable, change the directory where BANANA will be installed.
- Step 6 Click the **Installation** button.
- Step 7 If applicable, change the program group where BANANA will appear.
- Step 8 Click **Continue**.
- Step 9 If a Version Conflict message box is displayed warning that a file being copied is not newer than the file on your system, click **Yes** to keep the existing file.
- Step 10 When the installation is done, click **OK**.
- Step 11 Enable virus-scanning and the Cisco Security Agent services, if applicable



Note The most up-to-date version of BANANA is available at <http://www.CiscoUnityTools.com>. When you start BANANA, it checks the Cisco Unity Tools website to see if a newer version is available, and if so, prompts you about upgrading.

To Enable Troubleshooting Logs and Traces on the Bridge Server

- Step 1 In the Bridge Administrator, go to the **Digital Networking** page and set Retention Days For Temporary SMTP Messages to the number of days that you want to retain the messages.
 - Step 2 Set the Tracing Level to **Flow**.
 - Step 3 Click **Save**.
 - Step 4 Go to the **System Settings** page, and set the Call Tracing Level to **Verbose**.
 - Step 5 Click **Save**.
-

To Increase the Voice Connector Logging Level

- Step 1 Log on to the Exchange server on which the Voice Connector is installed.
 - Step 2 On the Windows Start menu, click **Programs > Microsoft Exchange > Exchange System Manager**.
 - Step 3 In the left-hand pane, expand the **Connectors** container.
 - Step 4 Right-click **Exchange 2000 Voice Connector (<Server name>)**, and select **Properties**.
 - Step 5 Click the **Advanced** tab.
 - Step 6 In the Logging Level list, click **Information**.
 - Step 7 Click **OK**.
 - Step 8 In the Windows Services applet, right-click **Exchange 2000 Voice Connector (<Server name>)**, and select **Restart**.
-

To Enable Message Tracking in Exchange 2000

You need to enable message tracking on each Exchange server that participates in message delivery: the Exchange server (or servers) on which the Voice Connector is installed, and the Exchange server on which the Cisco Unity subscriber mailbox is located.

-
- Step 1 Open the Exchange System Manager. (On the Windows Start menu, click **Programs > Exchange > Exchange System Manager**.)
 - Step 2 Right-click the Exchange server on which you want to enable message tracking, and select **Properties**.
 - Step 3 Check the **Enable Message Tracking** check box.
 - Step 4 Click **OK**.
 - Step 5 Repeat [Step 1](#) through [Step 4](#) for each Exchange server that participates in message delivery.
-

To Enable SMTP Logging in Exchange 2000

-
- Step 1 Open the Exchange System Manager.
 - Step 2 In the left-hand pane, expand **Servers > <Server where Voice Connector is installed> > Protocols > SMTP**.
 - Step 3 Right-click the Default SMTP Virtual Server (or any other SMTP Connector that is routing mail) and select **Properties**.
 - Step 4 Check the **Enable Logging** check box.
 - Step 5 In the Active Log Format list, click **NCSA Common Log File Format**.
 - Step 6 Click **Properties** and enter the location for the log file.
 - Step 7 Click **OK** twice and close the Exchange System Manager.
-

Do Messages from Cisco Unity Get to the Bridge?

To Determine Whether Outbound Messages Get to the Bridge

-
- Step 1 On the Bridge server, browse to the **Bridge\Vpim\Xcode\Inbound\Tmp** directory.
Messages are saved in this directory when the Retention Days For Temporary SMTP Messages field on the Digital Networking page in the Bridge Administrator is set to a value greater than zero.
 - Step 2 If there are messages in this directory, SMTP messages are being successfully sent from Exchange to the Bridge server. Go to the [“Are Outbound Calls Attempted?”](#) section on page 6-11.
 - Step 3 If messages do not get to the Bridge, go to the [“Do Outbound Messages Get to the Voice Connector?”](#) section on page 6-18.
-

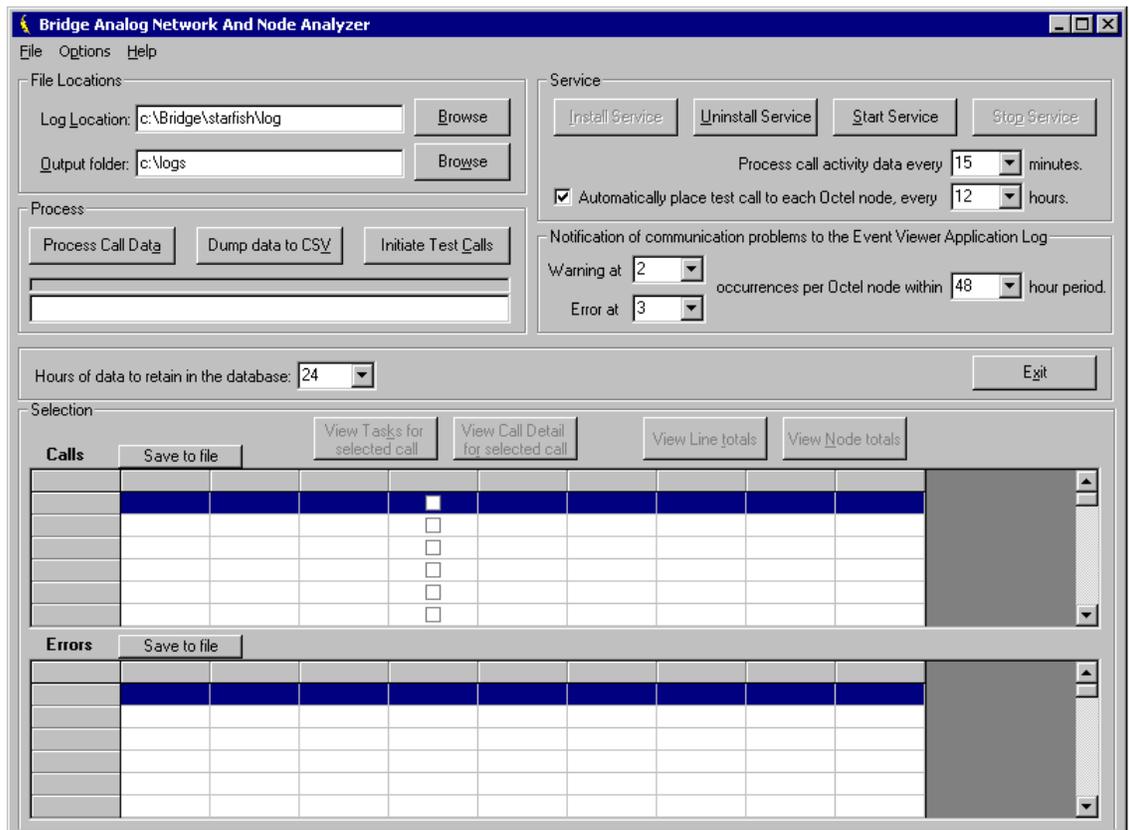
Are Outbound Calls Attempted?

To determine whether calls are attempted, you use BANANA admin to view the call traces. To obtain the needed information from the call traces, the Call Tracing Level field on the System Settings page in the Bridge Administrator must be set to Verbose or Debug. Logs for analog activity are stored in this directory, one log per hour, for a period of 24 hours. The current log is named sflog.log. The logs for the previous 24 hours are named sflog.mmddtttt.log, where mm=month, dd=day, and tttt=time of day in hours and minutes (on a 24-hour clock).

When the call traces are processed by BANANA, it stores all necessary data in its bdgdata.mdb database. Although the call traces from which the data is extracted are retained for only 24 hours, BANANA will retain the data for up to 14 days (configurable to the hour) as long as BANANA processes call traces—either manually or automatically—at least once per 24 hours.

To Determine Whether Calls Are Attempted

Step 1 On the Windows Start menu on the Bridge server, click **Programs > BANANA > BANANA admin**.

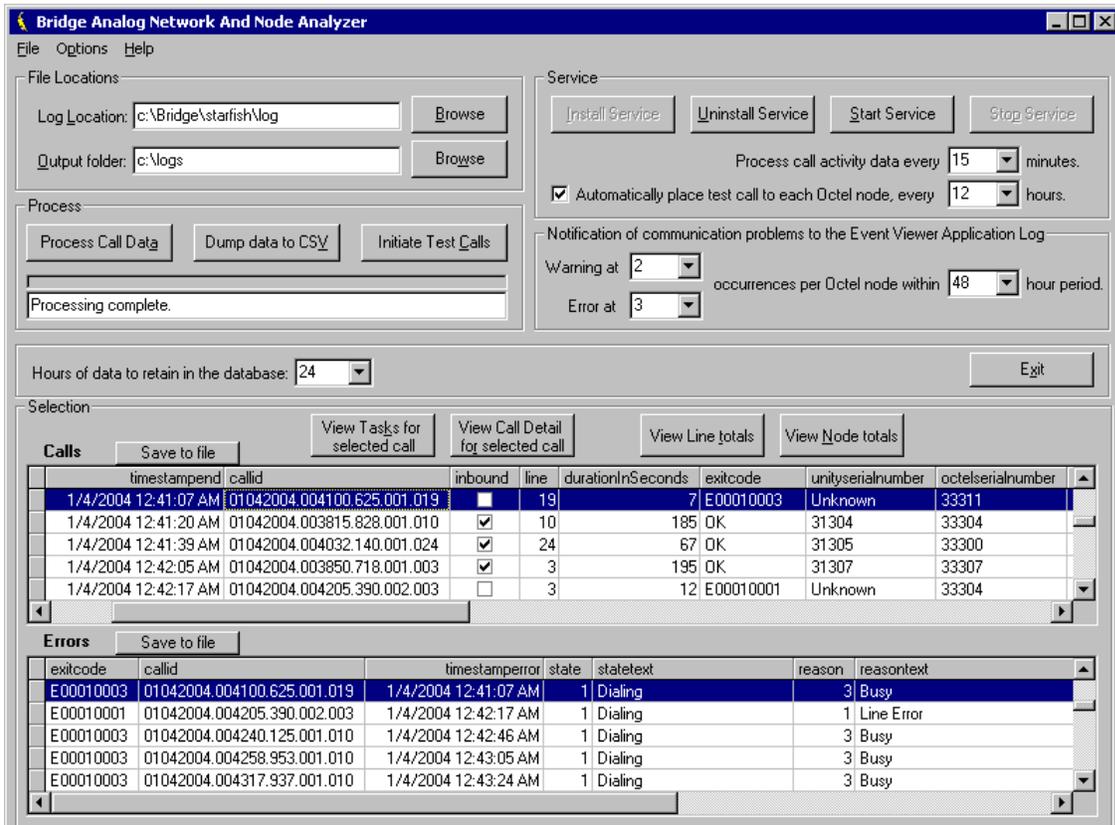


Step 2 If you have not already done so, set the Log Location and Output Folder location as described in the following sub-steps. If you have already set the locations, skip to [Step 3](#).

- a. In the Files Location section, if the path for the Log Location is set to d:\Bridge\Starfish\Log, skip to step b. Otherwise, enter or browse to the directory where the analog call traces are stored. This directory can be identified by the presence of files with names that begin with SFLOG.

- b. If desired, change the location of the Output Folder. This is the directory in which BANANA stores the logs and CSV files that it generates.

Step 3 Click **Process Call Data**. BANANA processes the log file, and then populates the Calls and Errors grids. Depending on the amount of data in the log file, this could take several minutes.



Step 4 In the Calls grid, click the **Inbound** column header to sort the calls by inbound and outbound. Inbound calls are indicated with a check mark.

If you want to see whether a specific call was attempted, and there are numerous calls in the grid, you may want to sort the calls by the TimeStampBegin column or the OctelSerialNumber column.

Refer to the “Viewing Data in the BANANA admin Interface” section of the BANANA Help for more information.

Step 5 If you do not see any outbound calls, or if you were looking for a specific outbound call and do not see it, go to the [“Troubleshooting Why Outbound Calls Are Not Attempted”](#) section on page 6-12.

Otherwise, go to the [“Troubleshooting Why Outbound Calls Are Failing”](#) section on page 6-13.

Troubleshooting Why Outbound Calls Are Not Attempted

- Is the Octel node delivery schedule active?—In the Bridge Administrator, go to the Octel Node configuration page for each node. Confirm that the settings in the Message Delivery Windows section of the page indicate that the delivery schedule is active.

- Is the Unity Bridge service running?—On the Bridge server, open the Services Control Panel and confirm that the Unity Bridge service is running.
- Are any lines enabled?—In the Bridge Administrator, go to the Line Status page to view the status for each line.
- Is only one line enabled?—In the Bridge Administrator, go to the Line Status page to view the status for each line. The Bridge will not dial out when only one line is enabled.
- Are all ports busy with incoming calls?—In the Bridge Administrator, go to the Line Status page to view the status for each line.
- Is there a problem with the Bridge analog card(s) or drivers?—On the Bridge server, open the Windows Event Viewer Application log, and look for warnings and errors related to the cards and drivers.
- Are lines retired?—In the Bridge Administrator, go to the Line Status page to view the status for each line. On the Bridge server, you can also open the Windows Event Viewer Application log, and look for warnings and errors related to retired lines (for example, “Retired for callouts”). If line retirements occur, plug an analog phone into the lines going to the Bridge. Confirm that you get dial tone when you go off hook.

When a problem occurs that prevents the Bridge from initiating an outgoing analog call on a particular analog port—for example, a line cord is not plugged in or there is no dial tone from the phone system—and when the same problem occurs on the same port four times in succession, the Bridge will retire that port and log the following warning in the Windows Event Viewer Application log: “Line X: Retired for callouts.” This port will then be unavailable for outgoing calls. However, if the same port receives an incoming call and the connection is successful, the port will be put back into service for both incoming and outgoing calls, and another warning will appear in the Application Event Viewer: “Line X: Callouts re-started.” This allows the Bridge to resolve the situation automatically if the condition clears up, or at the minimum allows the port to continue to receive incoming calls even if the problem initiating outgoing calls persists.

If all enabled analog lines on the Bridge server become retired due to these conditions, another warning will appear in the Application Event Viewer: “No lines are available for placing outgoing callouts.” As soon as at least one port receives an incoming call and becomes available, another warning will appear in the log: “Line(s) are once again available for outgoing calls.”

If these warnings appear frequently in the Application Event Viewer log, the analog lines connected to the Bridge server should be checked to see what problems may be occurring. After resolving any issues with the lines, any ports currently retired can be returned to service either by calling into the retired ports to trigger an automatic return to service, or by restarting the Unity Bridge service from the Services Control Panel.

Troubleshooting Why Outbound Calls Are Failing

When the Bridge uses a Cisco gateway connected to Cisco CallManager for analog connectivity with the Octels, verify that:

- The Cisco gateway is supported. The only supported Cisco gateways are those listed in the “Supported Cisco Gateways” section of *Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30sysrq.htm.
- The DTMF duration and interdigit timing settings for Cisco CallManager and gateways have been set to 100 milliseconds. (Any value within the range 80 and 100 milliseconds is fine.) In some versions of Cisco CallManager, the default value for the H225 DTMF Duration parameter is 300

milliseconds, which causes problems for the Bridge. Refer to the applicable Cisco documentation for details on locating and changing the applicable parameters in Cisco CallManager and the gateways.

If the above steps do not resolve the problem, refer back to BANANA admin, as described below.

In the Calls grid of the BANANA admin, click the ExitCode column header to sort the calls by exit code. Calls that completed successfully are indicated with “OK” in the ExitCode column. Calls that did not complete successfully have an error code (a number beginning with an “E”) listed in the ExitCode column.

For each call in the Calls grid that encountered an error, a record exists in the Errors grid. This record provides specific details regarding the condition under which the call was terminated, including the state of the protocol that was in process, and the reason the call could not be completed. When you click a call with an error code in the Calls grid, the corresponding record is highlighted in the Errors grid. The record in the Errors grid lists the exit code, call state, and reason for the call failure.

Calls									
timestamp	callid	inbound	line	durationInSeconds	exitcode	unityserialnumber	octelserialnumber		
1/18/2004 11:00:17 PM	01042004.005927.312.001.023	<input type="checkbox"/>	23	1288850	E00090006	31300	33305		
1/18/2004 11:02:01 PM	01042004.005321.937.001.021	<input checked="" type="checkbox"/>	21	1289320	E00120007	31305	33305		
1/18/2004 11:05:25 PM	01042004.004444.515.001.017	<input type="checkbox"/>	17	1290041	E00280999	31305	33305		
1/4/2004 12:05:00 AM	01042004.000350.125.001.001	<input type="checkbox"/>	1	70	OK	31300	33305		
1/4/2004 12:09:43 AM	01042004.000843.406.001.021	<input type="checkbox"/>	21	60	OK	31300	33305		

Errors							
exitcode	callid	timestamp	error	state	statetext	reason	reasontext
E00300999	01042004.005959.578.001.004	1/18/2004 11:00:03 PM	30	Call Out Process Initiated		999	Unknown
E00090006	01042004.005927.312.001.023	1/18/2004 11:00:17 PM	9	Message Header Response		6	Received DTMF String Longer T
E00200007	01042004.005854.640.001.010	1/18/2004 11:00:30 PM	20	Admin Request		7	Received DTMF String Shorter T
E00120007	01042004.004823.375.001.001	1/18/2004 11:00:32 PM	12	Text Name Confirmation		7	Received DTMF String Shorter T
E00120007	01042004.004822.343.001.024	1/18/2004 11:00:59 PM	12	Text Name Confirmation		7	Received DTMF String Shorter T

The following table maps error codes to configuration problems, and to other problems that result in outbound call failures.

Table 6-2 Configuration and Other Problems That Result in Outbound Call Failures

Error Code	Description
E00010001	A Line Error occurs when the Bridge detects a line problem after going off hook and prior to dialing a phone number. The most common cause of this condition is failure to receive dial tone on the line. Plug an analog phone into the source of one of the analog lines and verify that you hear dial tone, and can successfully dial a phone number.
E00010003	The Bridge detected a busy condition after dialing the specified phone number for this node. On busy analog networks, this condition can occur occasionally. However, repeated failures to contact the remote node because of busy line conditions can result in messages not being delivered in a timely manner. Repeated failures can also result in the messages being returned to the Cisco Unity senders, when the number of retries exceeds the Attempts If Busy setting on the Bridge System Settings page. Confirm that the phone number specified for the node being called is correct by dialing the phone number from a regular phone. If you verify that the phone number is correct, but continue to experience busy conditions with this node, contact the system administrator of this Octel system to see if there is a reason the system is often unavailable.

Table 6-2 Configuration and Other Problems That Result in Outbound Call Failures (continued)

Error Code	Description
E00010004	The Bridge detected ringing on the line after dialing the specified phone number for this node, but the call was never answered. Confirm that the phone number specified for the node being called is correct, by dialing the phone number from a regular phone and verifying that the expected voice mail system answers.
E00020005	Verify that: <ul style="list-style-type: none"> The Octel server(s) are supported. The only supported Octel servers are those listed in “Supported Voice Messaging Systems” section of the <i>Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software</i>, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm. The Octel server(s) are running a supported protocol. The Octel servers must be running Octel analog networking. Neither Octel digital networking nor the VOICENET protocol is supported by the Bridge.
E00030005	On an outbound call, after the Bridge sends the BD handshake tones, it expects to receive the CDD handshake response. When an outbound call from the Bridge is answered, but no CDD is received, this may indicate: <ul style="list-style-type: none"> That the call was not answered by an Octel that supports the Octel Analog Networking feature. Check the phone number for the Octel Node profile of the serial number that the Bridge was attempting to contact. Poor line quality. If the line quality is such that the audio being sent to the Bridge is not clear, this is usually the first state in which you will observe problems. To determine what the Bridge may be experiencing when calling this number, plug an analog phone into the source of one of the analog lines and dial the phone number as configured for this Octel Node. Failure to detect call progress, such as ringback or busy tone, on the analog line. If the Bridge is able to place a call successfully, but receives no further indication of the call progress within 20 seconds, it will assume the call has been answered and begin to send the BD wake up tones. If the call has not actually been answered, you may receive this error. To determine what the Bridge may be experiencing when calling this number, plug an analog phone into the source of one of the analog lines and dial the phone number as configured for this Octel Node. Also verify that: <ul style="list-style-type: none"> The Octel server(s) are supported. The only supported Octel servers are those listed in “Supported Voice Messaging Systems” section of the <i>Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software</i>, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm. The Octel server(s) are running a supported protocol. The Octel servers must be running Octel analog networking. Neither Octel digital networking nor the VOICENET protocol is supported by the Bridge.
E00050005	On an outbound call from the Bridge to an Octel, after the Bridge sends the BD handshake tones and receives the CDD handshake response, it sends a string of 18 DTMF digits, including the serial number of the Octel that the Bridge is attempting to communicate with. If no response is received from the Octel, it is possible that the serial number sent from the Bridge did not match the serial number of the Octel that answered the call. Verify that the serial number and phone number for the Octel Node profile are correct.
E00070005	If observed repeatedly, this may indicate that the remote system does not have a location profile configured for the Unity Node serial number that the Bridge server is using. When the Bridge sends the session header, this packet includes the Unity Node serial number that the Bridge is calling as. If the remote system requires this serial number to be configured on a location profile, and it does not have one matching the serial number that the Bridge used in the session header, the remote system will disconnect without sending the session header response. Note that not all systems that support Octel analog networking require confirmation of the calling serial number at this stage. Also note that E00070005 will also be the exitcode if the remote system did not receive all of the session header DTMF digits as sent by the Bridge, even if location profiles on both systems are configured correctly.

Table 6-2 Configuration and Other Problems That Result in Outbound Call Failures (continued)

Error Code	Description
E00160010	Confirm that the Octel node with which the Bridge communicates supports the fax feature.
E00160099	Confirm that all gateway and phone system devices between the Octel and the Bridge support fax transmission.
E00010017	<p>Upon dialing the phone number of the remote system, the Bridge received intercept tones from the phone service provider, indicating the number dialed is out of service. The Bridge counts this condition against the Attempts If Busy threshold configured on the System Settings page. When the number of retries exceeds the Attempts If Busy setting, all messages queued for delivery to this remote system will be returned to the Cisco Unity senders as non-deliverable.</p> <p>Confirm that the phone number specified for the node being called is correct by dialing the phone number from a phone.</p>

Error Handling Added for Problematic Outbound Analog Messages (Cisco Unity Bridge 3.0(5) and Later)

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. In Cisco Unity Bridge 3.0(5) and later, the Max Play Attempts Per Message setting was added to the System Settings page in the Bridge Administrator to allow you to control how long the Bridge attempts to deliver a particular message before returning it to the sender as undeliverable. (See the [“System Settings” section on page 10-1](#) for more information on the Max Play Attempts Per Message setting.)

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.

Event Viewer Warnings (Cisco Unity Bridge 3.0(5) and Later)

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) and later, 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.

Do Outbound Messages Get to the Voice Connector?

If messages do not reach the Bridge, the next step is to determine whether the messages get to the Voice Connector, by examining the Voice Connector log file. Following are the logs (with source code line numbers and file names deleted) for a successfully processed Cisco Unity to Bridge voice message, with the logging level set to Information:

```
08/12/03 16:23:08 094C INFO (hr=0) Add into message Queue.
MessageID=0000000004F9AC27C1A55247823664517E7EAA73010041B30F180DECD
F49ACE42AA5 B1221887000000035CCA0000
08/12/03 16:23:08 094C INFO (hr=0) **** [OUT] Processing message of class
[ENVELOPE.IPM.NOTE] ****
08/12/03 16:23:08 094C INFO (hr=0) Target Address (OMNI:902_81000)
08/12/03 16:23:08 094C INFO (hr=0) Bridge Type Recipient
08/12/03 16:23:08 094C INFO (hr=0) CAvOmniDelivery SendOutOmniMessage: !!!!! Processing
Outgoing OMNI Voice message !!!!!
08/12/03 16:23:08 094C INFO (hr=0) CAvADUserHomedServer object created for given thread-!!
08/12/03 16:23:08 094C INFO (hr=0) Get Octel Information for User: /O=ORG/OU=FIRST
ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=F09LAST000
08/12/03 16:23:08 094C INFO (hr=0) GC Server: \\jdc9.jdc9dom.ecsbu-lab-sea.cisco.com
08/12/03 16:23:08 094C INFO (hr=0) Forest Root Path: GC://MyGCserver.cisco.com
08/12/03 16:23:08 094C INFO (hr=0) Search String: (&(objectCategory=user)
(legacyExchangeDN=/O=ORG/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/
CN=F09LAST000))
08/12/03 16:23:08 094C INFO (hr=0) CAvOmniOutMessage:: (MESSAGE) Sender
(/O=ORG/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=F09LAST000).
MailBox Id= 91000,Octel Node= 99991
08/12/03 16:23:08 094C INFO (hr=0) Search String: (&(objectCategory=ciscoEcsbuUMLocation)
(ciscoEcsbuDtmfId=902))
08/12/03 16:23:08 094C INFO (hr=0) Delivered file to SMTP via C:\Program Files\Exchsrvr\
Mailroot\vs1\pickup\OMN7C.tmp
08/12/03 16:23:08 094C INFO (hr=0) Remove from message Queue. Message ID=
0000000004F9AC27C1A55247823664517E7EAA73010041B30F180DECD F49ACE42AA5
B1221887000000035CCA0000
```

The line containing “!!!! Processing Outgoing OMNI Voice message !!!!!” indicates that the Voice Connector is receiving messages. The lines containing “Delivered file to SMTP” and “Remove from message queue” indicate that processing was successfully completed. If there are problems with processing, there will be error messages in the log between the “!!!! Processing Outgoing OMNI Voice message !!!!!” and “Delivered file to SMTP” lines.

Examine the Voice Connector log file as described in the [“To Determine Whether the Voice Connector Receives Messages”](#) section on page 6-18. Note that the Voice Connector logging level must be set to Information (or Function) as described in the [“To Increase the Voice Connector Logging Level”](#) section on page 6-9.

To Determine Whether the Voice Connector Receives Messages

-
- Step 1 Log on to the Exchange server on which the Voice Connector is installed.
 - Step 2 Browse to the directory <ExchangeServerPath>\VoiceGateway\LogFiles.
 - Step 3 Open the Voice Connector log file **GwIvc_<Date>.log**. The <Date> will be rendered as YyMmDd, where Yy in the year, Mm is the month, and Dd is the day.



Note Be sure to open the correct log file. In this directory, you will also find a Voice Connector performance log file called GwIvc_perf_ YyMmDd.log, which cannot be used in this procedure.

- Step 4** Search for a line containing **!!!!!! Processing Outgoing OMNI Voice Message !!!!!!**
- Step 5** The presence of this line confirms that the Voice Connector is receiving messages. Go to the [“Does the Voice Connector Hand Off Messages for Pickup by the SMTP Service?”](#) section on page 6-20.
- The absence of this line indicates that the Voice Connector is not receiving messages. Go to the [“Troubleshooting Why Outbound Messages Do Not Get to the Voice Connector”](#) section on page 6-19.
-

Troubleshooting Why Outbound Messages Do Not Get to the Voice Connector

- Is the Voice Connector service running?—On the Exchange server on which the Voice Connector is installed, open the Services Control Panel and confirm that the Exchange 2000 Voice Connector service is running.
- Are there errors in Event Viewer?—On the Exchange server on which the Voice Connector is installed, in the Windows Event Viewer system and application logs, look for warnings or errors.
- Are the Exchange route group connectors configured properly?—If the Voice Connector is not installed in the same routing group as the mailbox of the subscriber who sent the message, verify that Exchange route group connectors are properly set up to route messages between the groups.
- Are test messages delivered to subscribers homed on the Exchange server on which the Voice Connector is installed?—Send a test message from the subscriber who sent a message that was not delivered to another subscriber whose mailbox is on the same server on which the Voice Connector is installed.
- Are the Voice Connector settings correct?—Do the [“To Verify Voice Connector Settings”](#) procedure on page 6-19 to verify the settings.

To Verify Voice Connector Settings

- Step 1** On the Exchange server on which the Voice Connector is installed, in the Exchange System Manager under the Connectors subtree, right-click **AvExchangeIVC_<Machine name>**, and select **Properties**.
- Step 2** Click the **Address Space** tab and confirm that a type **OMNI** is listed with an Address of ***** and a Cost of **1**.
- Step 3** Confirm that the Connector Scope is set to **Entire Organization**.
- Step 4** Determine whether the messages are still in the process of being routed, or if they are routing incorrectly within the Exchange network. Use Exchange Message Tracking to view the recent tracking history of messages within the network. Look for messages with a recipient of “[OMNI:...]” or “IMCEAOMNI-...”.
-

Does the Voice Connector Hand Off Messages for Pickup by the SMTP Service?

If a line containing “!!!!!! Processing Outgoing OMNI Voice message !!!!!!” appears in the GwIvc_<date>.log file, do the following procedure. The presence of this line indicates that the Voice Connector is receiving messages from Exchange and is processing them, so the next step is to determine whether the Voice Connector sends the messages back to Exchange to be sent out via the Exchange SMTP queues.

To Determine Whether the Voice Connector Hands Off Messages to Exchange

-
- Step 1** In the GwIvc_<Date>.log file, locate the line containing **!!!!!! Processing Outgoing OMNI Voice Message !!!!!!**
- Step 2** Within the next 5 to 20 lines—the placement varies depending on whether the logging level is set to Information or Function—look for separate lines containing each of the following messages, which indicate who the message is from:
- ...INFO...Get Octel Information for User:**
...INFO...Mailbox Id=...Octel Node=...
- Step 3** Within the next few lines, look for a line containing each of the following messages:
- ...INFO...Delivered File to SMTP**
...INFO...Remove from Message Queue
- Step 4** The presence of the lines specified in [Step 3](#) indicates that the Voice Connector is forwarding these messages on to the SMTP server via Exchange. Continue with the [“Do the Exchange SMTP Outgoing Queues Attempt to Send Messages?”](#) section on page 6-21.

If the lines specified in [Step 3](#) are not present, the Voice Connector is not sending messages back to Exchange. Continue with the [“Troubleshooting Why the Voice Connector Does Not Hand Off Messages to Exchange”](#) section on page 6-20.

Troubleshooting Why the Voice Connector Does Not Hand Off Messages to Exchange

- Are there errors in the Event Viewer?—On the Exchange server on which the Voice Connector is installed, in the Windows Event Viewer system and application logs, look for warnings or errors. In particular:
 - Look for warnings or errors that indicate that messages have been returned because of invalid attachments.
 - Look for warnings that include the text “ciscoEcsbuRemoteNodeID for current user not found” or “ciscoEcsbuLegacyMailbox for current user not found.” These messages indicate that the Cisco Unity subscriber who sent the message does not have the Octel Serial Number (ciscoEcsbuRemoteNodeId) or Legacy Mailbox values defined that are necessary for processing voice messages to and from the Cisco Unity Bridge server (in Cisco Unity version 4.0(3) and later).
 - Look for warnings that include the text “Address Message: Unknown Error, Check GwIvc_<Date>.log.” These warnings may indicate that the Bridge server address and node ID have not been properly defined on the Primary Location page in the Cisco Unity Administrator.
- Are messages stuck in the MTS-IN and MTS-OUT queues? Do one of the following procedures, as applicable.

To View the MTS-IN and MTS-OUT Queues in Exchange 2000

- Step 1** Log on to the Exchange server on which the Voice Connector is installed.
 - Step 2** Start Exchange System Manager. (On the Start menu, click **Programs > Microsoft Exchange > System Manager**.)
 - Step 3** Look for **AvExchangeIVC_<Machine name>** or **Exchange 2000 Voice Connector (<Servername>)** under the Connectors subtree for your site.
 - Step 4** Look in the MTS-IN and MTS-OUT queues to see if any messages appear to be stuck.
 - Step 5** Restart the Exchange 2000 Voice Connector service by using the Services Control Panel.
 - Step 6** Confirm that the SMTP service is running in the Services Control Panel.
-

To View the Voice Connector Queue in Exchange 2003

- Step 1** Log on to the Exchange server on which the Voice Connector is installed.
 - Step 2** Start Exchange Systems Manager. (On the Start menu, click **Programs > Microsoft Exchange > System Manager**.)
 - Step 3** Expand the **Servers** container, and then expand the server on which the Voice Connector is installed.
 - Step 4** Within the server container, click **Queues**. You should see AvExchangeIVC<Server name> listed in the pane on the right.
 - Step 5** Double-click **AvExchangeIVC<Server name>**.
A queue window opens.
 - Step 6** Click **Find Now** to see all of the messages that are in the queue.
-

Do the Exchange SMTP Outgoing Queues Attempt to Send Messages?

If the Voice Connector successfully processes messages and hands them off to Exchange, but messages still do not leave the Exchange SMTP outgoing queue, this indicates a problem with Exchange. Although some troubleshooting steps are provided below, you may need to refer to your Exchange documentation. (In particular, refer to the “Troubleshooting” chapter of the *Microsoft Exchange 2000 Server Resource Kit*, which is available online through the Microsoft TechNet website.)

To Determine Whether the Exchange SMTP Outgoing Queues Attempt to Send Messages

- Step 1** Check the SMTP log files to see whether the SMTP server is attempting to send messages to the Bridge server. If it is attempting but failing to send the messages, look for a 4xx or 5xx code indicating what the cause of the failure is.
- Step 2** In the Exchange System Manager, for each server in the organization, expand the **<Server>\Protocols\SMTP\Default SMTP Virtual Server\Queues** subtree.
- Step 3** Look for messages that appear to be stuck. Messages addressed from the Voice Connector to the Bridge will have a Recipient address like **<mailbox>@<bridge server address>** or **directory@<bridge server address>**.

- Step 4** If the SMTP server is attempting to send messages, but the Bridge does not receive them, go to the [“Troubleshooting Why the Bridge Does Not Receive Messages Sent from the Exchange SMTP Queues”](#) section on page 6-22.
-

Troubleshooting Why the Bridge Does Not Receive Messages Sent from the Exchange SMTP Queues

Do the following procedure to determine if the fully qualified domain name of the Bridge server is entered correctly.

To Verify That the Domain Name of the Bridge Server Is Entered Correctly

- Step 1** In the Cisco Unity Administrator, go to the **Bridge Delivery Location** page for the applicable remote Octel server on the Cisco Unity bridgehead server.
- Step 2** Confirm that the name in the Bridge Server Full Computer Name field on the Bridge Delivery Location page of the Cisco Unity Administrator exactly matches the Bridge Server Full Computer Name field on the Digital Networking page in the Bridge Administrator on the Bridge server.
- Step 3** Confirm that both settings match the Full Computer Name of the Bridge server as listed in the Windows System Control Panel on the Network Identification tab on the Bridge server.
- Step 4** In a command prompt window on the Exchange/SMTP server, enter the command **nslookup <Bridge Server>** where <Bridge Server> is the fully qualified domain name of the Bridge server as entered in the locations above.

If the returned response is **Non-Existent Domain**, check the configuration of the DNS zones in which the servers are located. Make any necessary changes so that the fully-qualified domain name of the Bridge is recognizable from the zone in which the Exchange/SMTP server is located.

- Confirm that Exchange/SMTP servers used for relaying messages outside of the organization are not restricted from relaying messages to unknown servers, or if they are restricted, that relaying messages to the Bridge server IP address is explicitly allowed. Depending on your network configuration, you may need to manually enter a DNS MX record for the Bridge in order to allow SMTP message delivery to it, but usually this is not necessary.
- If there is a firewall between the Bridge and the SMTP relay server, confirm that SMTP traffic is allowed on port 25.
- Check to see whether e-mail leaving your Exchange organization is re-routed to a smart host, non-Exchange corporate SMTP relay server, secure e-mail server, or any other traffic filtering server that may not route SMTP messages to the Bridge server. If so, an Exchange SMTP connector can be configured to send only those message addressed to the Bridge server directly to the Bridge without being re-routed. Do the following procedure.

To Configure an Exchange SMTP Connector to Route Messages Addressed to the Bridge Server Directly to the Bridge



Caution

Consult the Exchange administrator for your organization before doing this procedure. Misconfiguration of the SMTP connector could result in problems routing other SMTP mail for the organization.

-
- Step 1** On the Exchange server on which the Voice Connector is installed, open the Exchange System Manager. (The SMTP connector must be created on the Exchange server on which the Voice Connector is installed.)
- Step 2** Expand the tree in the left pane to view the Connectors directory. On some servers the Connectors directory will be in the Organization root. On others, most notably where multiple Routing Groups are being used, you will need to be sure to select the Connectors directory under the Routing Group in which the Voice Connector is installed.
- Step 3** Right-click **Connectors** and select **New > SMTP Connector**.
- Step 4** On the General tab, enter a meaningful name.
- Step 5** On the General tab, select **Forward All Mail Through this Connector to the Following Smart Hosts**. In the field below, enter the IP address of the Bridge server enclosed in square brackets (for example: [10.10.255.1]).
- Step 6** On the General tab, click **Add**.
- Step 7** Select the server on which the Voice Connector is installed, and click **OK** to set this as the bridgehead server for the SMTP connector.
- Step 8** Click the **Address Space** tab.
- Step 9** On the Address Space tab, click **Add**.
- Step 10** Select **SMTP** and click **OK**.
- Step 11** In the E-Mail Domain field, enter the fully qualified domain name of the Bridge server. The name should match the following:
- The Full Computer Name of the Bridge server as listed in the Windows System Control Panel on the Network Identification tab on the Bridge server.
 - The Cisco Unity Bridge Domain Name in the Digital Networking page in the Bridge Administrator.
 - The Bridge server address entered in the Cisco Unity Administrator on the Primary Location page on the Cisco Unity bridgehead server (the server licensed for the Bridge).
- Step 12** Leave the value in the Cost field set to 1, and click **OK**.
- Step 13** Click **OK** to complete the configuration of the SMTP connector.
- Step 14** Send a test voice message from Cisco Unity to an Octel recipient to see whether the message arrives at the Bridge.
- Step 15** Send a test e-mail to an outside address to verify that e-mail still works.
-

After You Finish Troubleshooting

When finished troubleshooting, you should reset most of the logs and traces back to their defaults. However, leave the call tracing level on the System Settings page in the Bridge Administrator set to Verbose, as this call tracing level is required by BANANA.



Caution

Logs and traces that you enable on the Bridge server, on the Exchange server on which the Voice Connector is installed, and on the Cisco Unity server can take up a great deal of hard disk space. Disable the logs and traces when you finish troubleshooting, with the exception of the call traces (also referred to as the starfish logs) on the Bridge server.

Reset the following logs and traces:

- In the Bridge Administrator, on the Digital Networking page:
 - Reset the Retention Days For Temporary SMTP Messages back to 0 (zero). (These messages consume significant hard disk space, so you should always configure this setting to zero unless you are troubleshooting and also monitoring hard disk consumption.)
 - Reset the Tracing Level back to None. (Typically, these logs do not consume significant hard disk space, so you may choose to leave the Tracing Level set to Flow.)
- In the Exchange System Manager:
 - Reset the Voice Connector Logging Level back to Warning. (You may choose to leave these logs set to the Information level, which provides more detail than the Warning level. With logging at the Information level, you should monitor the hard disk space consumed by the log files. You may need to adjust the Log Recycle Days setting or set a limit for the hard disk space allowed for the logs.)
 - Disable Exchange message tracking. (You may choose to leave message tracking enabled. Monitor occasionally to make sure that no more than the desired hard disk space is consumed for storage of these logs.)
 - Disable SMTP logging. (You may choose to leave these logs enabled. Monitor occasionally to make sure that no more than the desired hard disk space is consumed for storage of these logs.)

To Decrease the Voice Connector Logging Settings (Exchange 2000 and Exchange 2003)

-
- Step 1** Log on to the Exchange server on which the Voice Connector is installed.
- Step 2** On the Windows Start menu, click **Programs > Microsoft Exchange > Exchange System Manager**.
- Step 3** In the left-hand pane, expand the **Connectors** container.
- Step 4** Right-click **Exchange 2000 Voice Connector (<Server Name>)**, and select **Properties**.
Note that the properties pages for administering the Voice Connector are always displayed in English.
- Step 5** Click the **Advanced** tab.
- Step 6** Click **Warning (Level 3)** to adjust the logging level.
- Step 7** Click **OK** and exit Exchange System Manager.
- Step 8** Open the Windows Services MMC.
- Step 9** Right-click **Exchange 2000 Voice Connector** and select **Restart**.
- Step 10** Exit the Windows Services MMC.
-

Messages Are Not Delivered from Octel to Cisco Unity

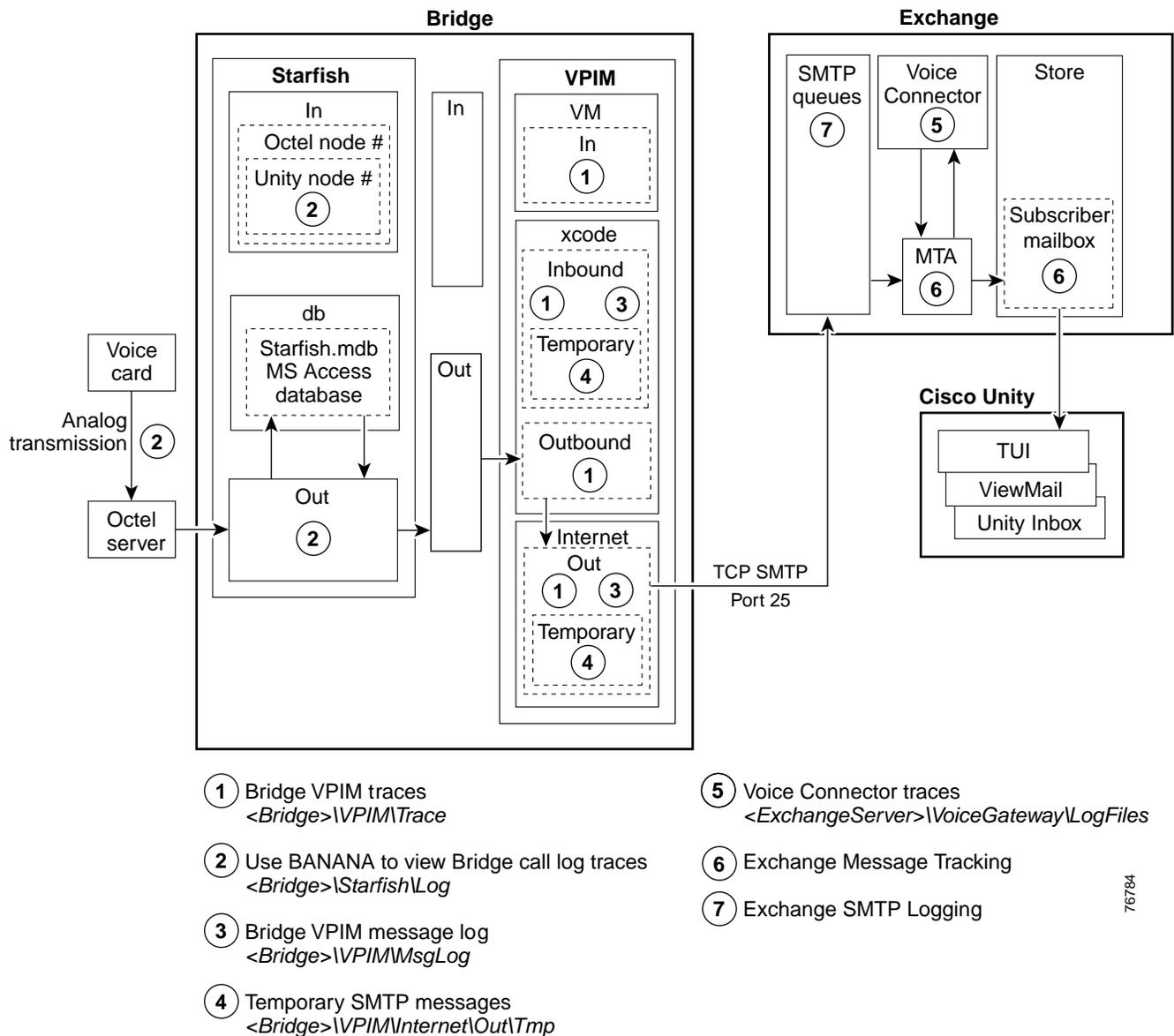
This section provides troubleshooting steps for identifying why a voice message is not delivered from an Octel node to a Cisco Unity subscriber.

When an Octel subscriber sends a voice message to a Cisco Unity subscriber, the Octel node passes the message to the Cisco Unity Bridge via analog lines. The Bridge converts the received Octel message to a VPIM message (with proprietary extensions) and sends it via SMTP to the Voice Connector for

Exchange 2000. The Voice Connector converts the message to a WAV file and hands it back to Exchange to be delivered to the Cisco Unity subscriber mailbox. Note that the Cisco Unity server does not play a role in delivering voice messages from an Octel node to a Cisco Unity subscriber mailbox.

Figure 6-3 illustrates at a high level the message flow from Octel to Cisco Unity, and the troubleshooting logs, traces, and tools that you can use to determine where the problem is along the path.

Figure 6-3 Troubleshooting Message Flow from Octel to Cisco Unity



76784

Bridge In and Out Directories

Note the Bridge\In and Bridge\Out directories in Figure 6-3.

Conceptually, these directories divide the Bridge into the SMTP side and the analog side. The Unity Bridge service controls messages on the analog side, and the Digital Networking service controls messages on the SMTP side. Bridge\In and Bridge\Out are transitional directories. Messages from Cisco Unity are delivered to the Bridge\In directory by the Digital Networking service, where they are picked up by the Unity Bridge service for delivery to the Octels. In the other direction, messages from the Octels are delivered to the Bridge\Out directory by the Unity Bridge service, where they are picked up by the Digital Networking service for delivery to Cisco Unity via Exchange. If either service is stopped for some reason, messages will queue up as shown in the following table.

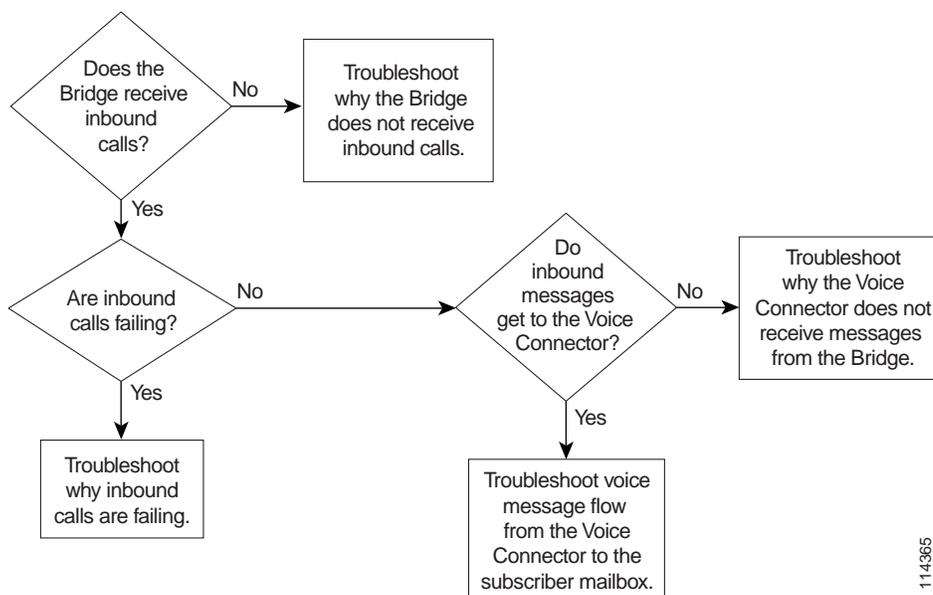
Table 6-3 Messages Queue Up When the Unity Bridge Service and/or the Digital Networking Service Stop

Digital Networking Service	Unity Bridge Service	Messages from Cisco Unity to the Octels...	Messages from the Octels to Cisco Unity...
Running	Not Running	Will queue up in the Bridge\In directory until the Unity Bridge service starts and picks them up.	Will queue up on the Octel servers.
Not Running	Running	Will be stuck in the Exchange SMTP outgoing queues.	Will queue up in the Bridge\Out directory until the Digital Networking service starts and picks them up.
Not Running	Not Running	Will be stuck in the Exchange SMTP outgoing queues.	Will queue up on the Octel servers.

Troubleshooting Why Messages Are Not Delivered from Octel to Cisco Unity

Figure 6-4 illustrates the troubleshooting process at a high level.

Figure 6-4 Troubleshooting Why Messages Are Not Delivered from Octel to Cisco Unity



114365

The following list provides an overview of the troubleshooting steps. Detailed procedures and troubleshooting steps follow the list.

1. Enable the various logs and traces as described in the [“Enabling Logs and Traces”](#) section on page 6-27.
2. If you are tracking down problems with messages that have already been sent, skip to the next step to begin troubleshooting. Otherwise, send a test message from an Octel subscriber to a Cisco Unity subscriber. Make a note of the serial number of the sending and receiving nodes.
3. [Does the Bridge Receive Inbound Calls?](#) If the Bridge does not receive inbound calls, see the [“Troubleshooting Why the Bridge Does Not Receive Inbound Calls”](#) section on page 6-31.
4. [Are Inbound Calls Failing?](#) If inbound calls are failing, see the [“Troubleshooting Why Inbound Calls Are Failing”](#) section on page 6-33.
5. [Do Inbound Messages Get to the Voice Connector?](#) If inbound messages do not reach the Voice Connector, see the [“Troubleshooting Why the Voice Connector Does Not Receive Messages from the Bridge”](#) section on page 6-38.
Otherwise, see the [“Troubleshooting Voice Message Flow from the Voice Connector to the Subscriber Mailbox”](#) section on page 6-42.
6. Reset the logs and traces as described in the [“After You Finish Troubleshooting”](#) section on page 6-43.

Enabling Logs and Traces

Before you begin sending test messages to track down the problem, do all of the following procedures to enable the applicable logs, traces, and other troubleshooting tools:

- [To Install BANANA](#), page 6-27
- [To Enable Troubleshooting Logs and Traces on the Bridge Server](#), page 6-28
- [To Increase the Voice Connector Logging Level](#), page 6-28
- [To Enable Message Tracking in Exchange 2000](#), page 6-28
- [To Enable SMTP Logging in Exchange 2000](#), page 6-29

To Install BANANA

If you have not already done so, install the Bridge Analog Network And Node Analyzer (BANANA).

-
- Step 1** Disable virus scanning services and the Cisco Security Agent service, if applicable.
 - Step 2** Insert the Cisco Unity Bridge compact disc in the CD-ROM drive, and browse to the **BANANA** directory.
 - Step 3** Double-click **setup.exe**.
 - Step 4** Click **OK** at the welcome screen.
 - Step 5** If applicable, change the directory where BANANA will be installed.
 - Step 6** Click the **Installation** button.
 - Step 7** If applicable, change the program group where BANANA will appear.
 - Step 8** Click **Continue**.
 - Step 9** If a Version Conflict message box is displayed warning that a file being copied is not newer than the file on your system, click **Yes** to keep the existing file.

- Step 10** When the installation is done, click **OK**.
- Step 11** Enable virus-scanning and the Cisco Security Agent services, if applicable



Note The most up-to-date version of BANANA is available at <http://www.CiscoUnityTools.com>. When you start BANANA, it checks the Cisco Unity Tools website to see if a newer version is available, and if so, prompts you about upgrading.

To Enable Troubleshooting Logs and Traces on the Bridge Server

- Step 1** In the Bridge Administrator, go to the **Digital Networking** page and set Retention Days For Temporary SMTP Messages to the number of days that you want to retain the messages.
- Step 2** Set the Tracing Level to **Flow**.
- Step 3** Click **Save**.
- Step 4** Go to the **System Settings** page, and set the Call Tracing Level to **Verbose**.
- Step 5** Click **Save**.

To Increase the Voice Connector Logging Level

- Step 1** Log on to the Exchange server on which the Voice Connector is installed.
- Step 2** On the Windows Start menu, click **Programs > Microsoft Exchange > Exchange System Manager**.
- Step 3** In the left-hand pane, expand the **Connectors** container.
- Step 4** Right-click **Exchange 2000 Voice Connector (<Server name>)**, and select **Properties**.
- Step 5** Click the **Advanced** tab.
- Step 6** In the Logging Level list, click **Information**.
- Step 7** Click **OK**.
- Step 8** In the Windows Services applet, right-click **Exchange 2000 Voice Connector (<Server name>)**, and select **Restart**.

To Enable Message Tracking in Exchange 2000

You need to enable message tracking on each Exchange server that participates in message delivery: the Exchange server (or servers) on which the Voice Connector is installed, and the Exchange server on which the Cisco Unity subscriber mailbox is located.

- Step 1** Open the Exchange System Manager. (On the Windows Start menu, click **Programs > Exchange > Exchange System Manager**.)
- Step 2** Right-click the Exchange server on which you want to enable message tracking, and select **Properties**.
- Step 3** Check the **Enable Message Tracking** check box.
- Step 4** Click **OK**.

- Step 5 Repeat [Step 1](#) through [Step 4](#) for each Exchange server that participates in message delivery.
-

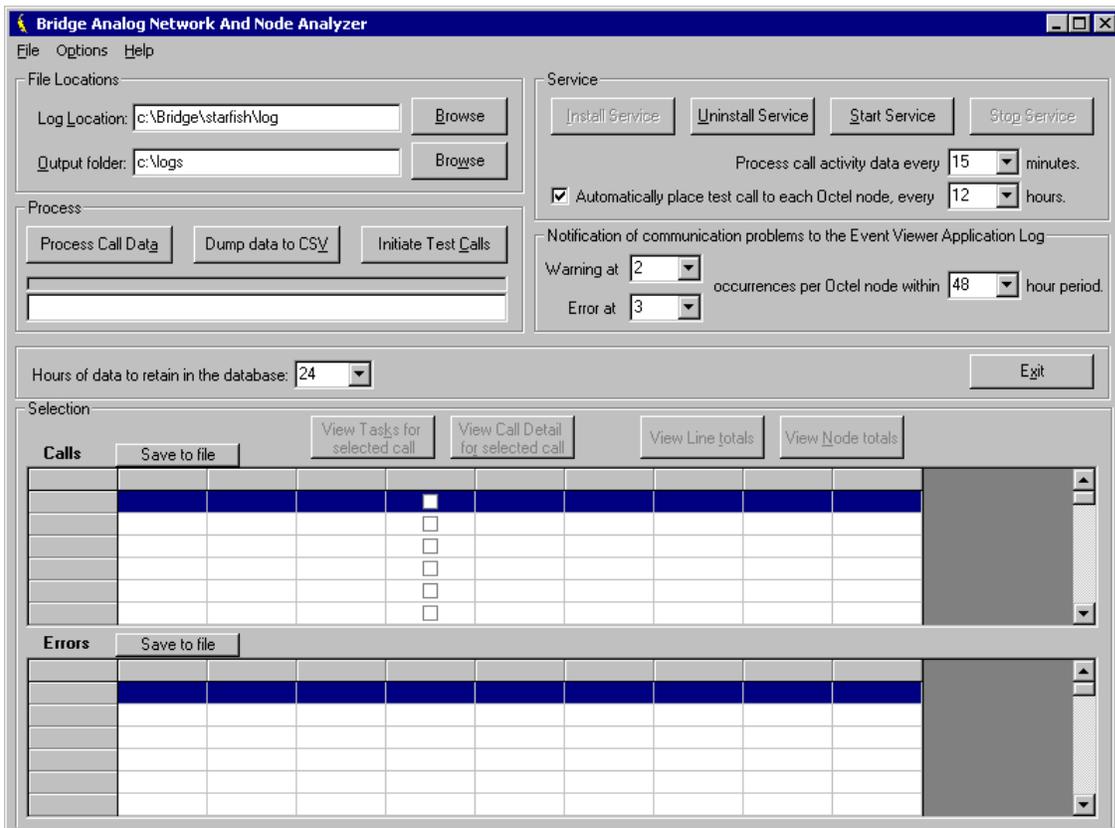
To Enable SMTP Logging in Exchange 2000

- Step 1 Open the Exchange System Manager.
- Step 2 In the left-hand pane, expand **Servers** > <**Server where Voice Connector is installed**> > **Protocols** > **SMTP**.
- Step 3 Right-click the Default SMTP Virtual Server (or any other SMTP Connector that is routing mail) and select **Properties**.
- Step 4 Check the **Enable Logging** check box.
- Step 5 In the Active Log Format list, click **NCSA Common Log File Format**.
- Step 6 Click **Properties** and enter the location for the log file.
- Step 7 Click **OK** twice and close the Exchange System Manager.
-

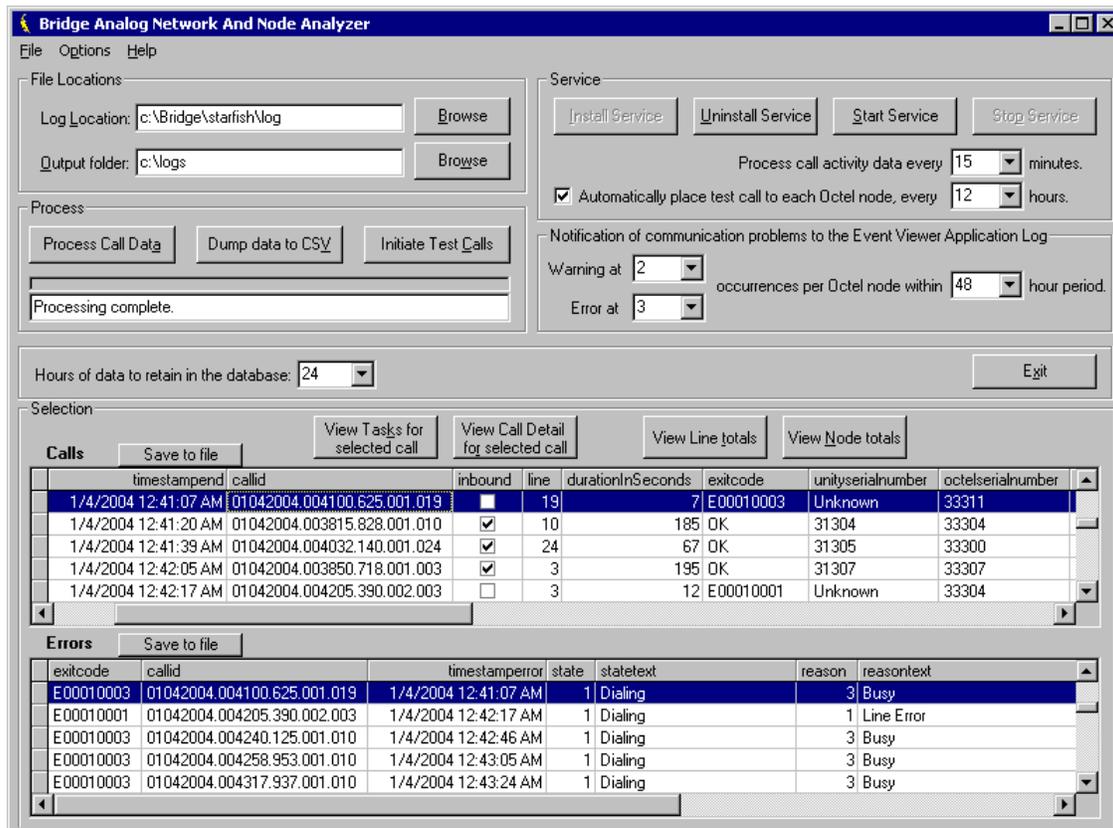
Does the Bridge Receive Inbound Calls?

To Determine Whether Messages from the Octels Get to Bridge

- Step 1 On the Windows Start menu on the Bridge server, click **Programs** > **BANANA** > **BANANA admin**.



- Step 2** If you have not already done so, set the Log Location and Output Folder location as described in the following sub-steps. If you have already set the locations, skip to [Step 3](#).
- In the Files Location section, if the path for the Log Location is set to d:\Bridge\Starfish\Log, skip to step **b**. Otherwise, enter or browse to the directory where the analog call traces are stored. This directory can be identified by the presence of files with names that begin with SFLOG.
 - If desired, change the location of the Output Folder. This is the directory in which BANANA stores the logs and CSV files that it generates.
- Step 3** Click **Process Call Data**. BANANA processes the log file, and then populates the Calls and Errors grids. Depending on the amount of data in the log file, this could take several minutes.



Step 4 In the Calls grid, click the **Inbound** column header to sort the calls by inbound and outbound. Inbound calls are indicated with a check mark.

If you want to see whether a specific call was received, and there are numerous calls in the grid, you may want to sort the calls by the TimeStampBegin column, the UnitySerialNumber column, or the OctelSerialNumber column.

Step 5 If you do not see any inbound calls, or if you were looking for a specific inbound call and do not see it, go to the [“Troubleshooting Why the Bridge Does Not Receive Inbound Calls”](#) section on page 6-31.

Otherwise, go to the [“Are Inbound Calls Failing?”](#) section on page 6-32.

Troubleshooting Why the Bridge Does Not Receive Inbound Calls

- Verify that the analog phone lines are plugged into the Bridge server and Octel servers.
- Verify the delivery phone number for the Bridge. Call the Bridge delivery phone number to see whether the Bridge answers. If the delivery phone number is correct and the Bridge answers, the inbound call will show up in BANANA admin. (In BANANA admin, click Process Call Data to see the record added to the Calls and Errors grids.)
- Check the node profiles on the Octel servers to verify that they are configured with the correct delivery phone number for the Bridge.

- If you have modified the default values for Queued Call Threshold and Max Ports Per Node on the System Settings page in the Bridge Administrator, and if message traffic is heavy enough, it is possible that all the ports will be used for outgoing messages, leaving no ports available for incoming messages. If this is a concern, you may want to designate one or more ports to be used only for incoming calls. The Line Status page in the Bridge Administrator allows you to specify whether each line is to be used for both incoming and outgoing calls or only for incoming calls. See the [“Controlling the Number of Ports Used for Outgoing Messages”](#) section on page 5-1 for more information.

Are Inbound Calls Failing?

In the Calls grid of the BANANA admin, click the ExitCode column header to sort the calls by exit code. Calls that completed successfully are indicated with “OK” in the ExitCode column. Calls that did not complete successfully have an error code (a number beginning with an “E”) listed in the ExitCode column.

For each call in the Calls grid that encountered an error, a record exists in the Errors grid. This record provides specific details regarding the condition under which the call was terminated, including the state of the protocol that was in process, and the reason the call could not be completed. When you click a call with an error code in the Calls grid, the corresponding record is highlighted in the Errors grid. The record in the Errors grid lists the exit code, call state, and reason for the call failure.

The screenshot shows the BANANA admin interface with two main sections: 'Calls' and 'Errors'.

Calls Grid:

timestamp	callid	inbound	line	durationInSeconds	exitcode	unityserialnumber	octelserialnumber
1/18/2004 11:00:17 PM	01042004.005927.312.001.023	<input type="checkbox"/>	23	1288850	E00090006	31300	33305
1/18/2004 11:02:01 PM	01042004.005321.937.001.021	<input checked="" type="checkbox"/>	21	1289320	E00120007	31305	33305
1/18/2004 11:05:25 PM	01042004.004444.515.001.017	<input type="checkbox"/>	17	1290041	E00280999	31305	33305
1/4/2004 12:05:00 AM	01042004.000350.125.001.001	<input type="checkbox"/>	1	70	OK	31300	33305
1/4/2004 12:09:43 AM	01042004.000843.406.001.021	<input type="checkbox"/>	21	60	OK	31300	33305

Errors Grid:

exitcode	callid	timestamperror	state	statetext	reason	reasontext
E00300999	01042004.005959.578.001.004	1/18/2004 11:00:03 PM	30	Call Out Process Initiated	999	Unknown
E00090006	01042004.005927.312.001.023	1/18/2004 11:00:17 PM	9	Message Header Response	6	Received DTMF String Longer T
E00200007	01042004.005854.640.001.010	1/18/2004 11:00:30 PM	20	Admin Request	7	Received DTMF String Shorter T
E00120007	01042004.004823.375.001.001	1/18/2004 11:00:32 PM	12	Text Name Confirmation	7	Received DTMF String Shorter T
E00120007	01042004.004822.343.001.024	1/18/2004 11:00:59 PM	12	Text Name Confirmation	7	Received DTMF String Shorter T

If the inbound calls have error codes, or if you were looking for a specific inbound call and it has an error code, go to the [“Troubleshooting Why Inbound Calls Are Failing”](#) section on page 6-33.

If the inbound call(s) completed successfully, a copy of the message should be saved to the Bridge\VPIM\Internet\Out and Bridge\VPIM\Internet\Out\Tmp directories.

The message will stay in the Bridge\VPIM\Internet\Out\Tmp directory only for the number of days that is set in the Retention Days for Temporary SMTP Messages setting on the Digital Networking page of the Bridge Administrator. The message will stay in the Bridge\VPIM\Internet\Out directory until it is successfully delivered via SMTP.

In Cisco Unity Bridge 3.0(5) and later, messages that the Bridge could not deliver are stored in Bridge\VPIM\Internet\Out\Failed. Note that when the Bridge saves a message to the Failed directory, it also logs a message in the Event Viewer Application log. So check both the Failed directory and the Event Viewer.

Verify that the message appears in the Bridge\VPIM\Internet\Out\Tmp directory. If the message is there, go to the “[Troubleshooting Why the Voice Connector Does Not Receive Messages from the Bridge](#)” section on page 6-38.

Troubleshooting Why Inbound Calls Are Failing

When the Bridge uses a Cisco gateway connected to Cisco CallManager for analog connectivity with the Octels, verify that:

- The Cisco gateway is supported. The only supported Cisco gateways are those listed in the “Supported Cisco Gateways” section of *Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm.
- The DTMF duration and interdigit timing settings for Cisco CallManager and gateways have been set to 100 milliseconds. (Any value within the range 80 and 100 milliseconds is fine.) In some versions of Cisco CallManager, the default value for the H225 DTMF Duration parameter is 300 milliseconds, which causes problems for the Bridge. Refer to the applicable Cisco documentation for details on locating and changing the applicable parameters in Cisco CallManager and the gateways.

If the above steps do not fix the problem, refer back to BANANA admin, as described below. The following table maps error codes to configuration problems and other problems that result in inbound call failures.

Table 6-4 Configuration and Other Problems That Result in Inbound Call Failures

Error Code	Description
E00020005	<p>On an inbound call, after the Bridge plays the opening prompt, it expects to receive the BD handshake tones from the calling node. When the Bridge answers an incoming call but no BD is received:</p> <ul style="list-style-type: none"> This may indicate that the calling Octel has not detected that the Bridge answered, due to poor line quality or problems with audio in the Bridge to Octel direction. Check to see whether the digits received were CD (a wake-up packet) and/or if the following warning appears in the Event Viewer Application log: <ul style="list-style-type: none"> Event Type: Warning Event Source: Bridge Event Category: None Event ID: 108 <p>Bridge received an incoming call that could not be processed. The calling server does not have a Serial Number defined in its Bridge node profile. Verify that all remote servers configured to communicate with Bridge have Serial Numbers for all Bridge nodes.</p> <p>Receipt of a wake-up packet of CD indicates that the calling Octel server does not have the serial number of the Unity recipient node defined in the applicable network node profile. The Octel is requesting the serial number from the Bridge. Because the Bridge can proxy for more than one serial number within the Octel network, the Bridge cannot respond with a serial number. The calling Octel must have the serial number(s) for the Unity nodes configured in the applicable network node profile(s) prior to calling the Bridge.</p> <p>Also verify that:</p> <ul style="list-style-type: none"> The Octel server(s) are supported. The only supported Octel servers are those listed in “Supported Voice Messaging Systems” section of the <i>Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software</i>, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm. The Octel server(s) are running a supported protocol. The Octel servers must be running Octel analog networking. Neither Octel digital networking nor the VOICENET protocol is supported by the Bridge.
E00030005	<p>Verify that:</p> <ul style="list-style-type: none"> The Octel server(s) are supported. The only supported Octel servers are those listed in “Supported Voice Messaging Systems” section of the <i>Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software</i>, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm. The Octel server(s) are running a supported protocol. The Octel servers must be running Octel analog networking. Neither Octel digital networking nor the VOICENET protocol is supported by the Bridge.

Table 6-4 Configuration and Other Problems That Result in Inbound Call Failures (continued)

Error Code	Description
E00020014	<p>If the calling Octel server does not have the Cisco Unity node serial number defined in its node configuration, the Bridge hangs up immediately when it receives a call from the Octel node. Additionally, the Bridge logs the following warning to the Windows Event Log:</p> <p>Event Type: Warning Event Source: Bridge Event Category: None Event ID: 108 Bridge received an incoming call that could not be processed. The calling server does not have a Serial Number defined in its Bridge node profile. Verify that all remote servers configured to communicate with Bridge have Serial Numbers for all Bridge nodes.</p> <p>Because the Bridge requires the Cisco Unity node serial number to be configured on the Octel server, you must define the serial number for the Cisco Unity node in the node profile on the Octel server.</p>

Table 6-4 Configuration and Other Problems That Result in Inbound Call Failures (continued)

Error Code	Description
E00040013	<p>On an inbound call from an Octel to the Bridge, after the Bridge receives the BD handshake tones and sends the CDD handshake response, the Bridge expects to receive an encrypted string of 18 DTMF digits that includes the serial number of the node that the Octel is attempting to communicate with. If the Bridge hangs up without sending a response, it is possible that the serial number sent from the Octel did not match any of the Unity Node profiles configured on the Bridge.</p> <p>On the Bridge server, verify that the serial number on each Unity Node is correct, and that a Unity Node with the correct serial number has been created for each node that the Bridge represents within the Octel network.</p> <p>If the serial numbers in the Unity Node profiles on the Bridge are correct, then the calling Octel may be sending an incorrect serial number. At this point in the call, the Bridge does not know the serial number of the calling Octel server. The easiest way to find out which Octel called is to look at CallManager or PBX log files. If you do not have access to the phone system log files, and if there are only a few Octel servers in the network, then all of the node profiles on each Octel server can be checked for an incorrect serial number. However, when there are many Octel servers in the network, checking every node profile on every Octel server to find an incorrect serial number when you do not know the number you are looking for can be very time consuming. If this error appears repeatedly, the following steps may help to determine the serial number that the calling Octel was attempting to contact.</p> <ol style="list-style-type: none"> 1. Browse to the \Bridge\Starfish\Log directory on the Bridge server. 2. In Notepad, open the sflog.*.log for the period during which the behavior has been observed. 3. Search for the string Initial Handshake Failed. You should see a sequence of events similar to the following: <pre>Line 4: Call Received. Line 4: Playing 1.sph Line 4: Received BD Line 4: Playing CDD Line 4: Received 12*D8#93697B08#CB* Line 4: Initial handshake failed. Received either bad data or a request to communicate with a node that is not yet configured on Bridge. Line 4: Received Line 4: Incoming Call Completed.</pre> <p>Because Octel analog networking packets are encrypted, you cannot determine the serial number of the node that the Octel is attempting to communicate with by looking at the DTMF packet. But there is a decryption utility on the Bridge server that can be used to determine the serial number. For the decryption utility to work, you will need to find two occurrences of this handshake failure in the log file.</p> <ol style="list-style-type: none"> 4. Copy the DTMF packet from the “Received” line that appears immediately after “Playing CDD” for both occurrences. (In the example above, you would copy the packet 12*D8#93697B08#CB*, and if the above example included another occurrence of the handshake failure, you would also copy that DTMF packet.) 5. On the Bridge server, open a command prompt window and change to the directory where starfish.exe is located. (The default location is \Bridge\Starfish\Bin.) 6. At the command line in the bin directory, enter the following command: <pre>starfish -p <packet1> <packet2></pre> <p>Where <packet1> is the DTMF packet copied from the “Received” line of the first occurrence and <packet2> is the DTMF packet copied from the “Received” line of the second occurrence.</p> <p>The utility returns the possible matches for the serial number of the node that is being called. It is possible that the utility will return 30 or more matches, but most of them can be eliminated as possibilities because they contain more than 5 digits. For example:</p>

Table 6-4 Configuration and Other Problems That Result in Inbound Call Failures (continued)

Error Code	Description
E00040013, continued	<pre>C:\Bridge\Starfish\Bin>Starfish -p 12#*2*C#110B#88D95 12*#**72110B#88D95</pre> <p>Please wait while running Packet Prediction...</p> <pre>DTMF packet(s) successfully decoded. Serial # 14801 DTMF packet(s) successfully decoded. Serial # 20953 DTMF packet(s) successfully decoded. Serial # 80337 DTMF packet(s) successfully decoded. Serial # 86489 DTMF packet(s) successfully decoded. Serial # 145873 DTMF packet(s) successfully decoded. Serial # 152025 DTMF packet(s) successfully decoded. Serial # 211409 DTMF packet(s) successfully decoded. Serial # 217561 DTMF packet(s) successfully decoded. Serial # 276945 DTMF packet(s) successfully decoded. Serial # 283097 DTMF packet(s) successfully decoded. Serial # 342481 DTMF packet(s) successfully decoded. Serial # 348633 DTMF packet(s) successfully decoded. Serial # 408017 DTMF packet(s) successfully decoded. Serial # 414169 DTMF packet(s) successfully decoded. Serial # 473553 DTMF packet(s) successfully decoded. Serial # 479705 DTMF packet(s) successfully decoded. Serial # 539089 DTMF packet(s) successfully decoded. Serial # 545241 DTMF packet(s) successfully decoded. Serial # 604625 DTMF packet(s) successfully decoded. Serial # 610777 DTMF packet(s) successfully decoded. Serial # 670161 DTMF packet(s) successfully decoded. Serial # 676313 DTMF packet(s) successfully decoded. Serial # 735697 DTMF packet(s) successfully decoded. Serial # 741849 DTMF packet(s) successfully decoded. Serial # 801233 DTMF packet(s) successfully decoded. Serial # 807385 DTMF packet(s) successfully decoded. Serial # 866769 DTMF packet(s) successfully decoded. Serial # 872921 DTMF packet(s) successfully decoded. Serial # 932305 DTMF packet(s) successfully decoded. Serial # 938457 DTMF packet(s) successfully decoded. Serial # 997841</pre> <p>It is unlikely that you will ever encounter an Octel node with a serial number longer than 5 digits, so you can consider any matches greater than 5 digits to be invalid. In the above example, that leaves only 14801, 20953, 80337 and 86489 as potential matches. At this point, the list is small enough that you should be able to determine which of these serial numbers should be configured as a Unity Node on the Bridge, or which serial number may have been configured in error on the network profile of an Octel node.</p>
E00160010	Confirm that the Octel node with which the Bridge communicates supports the fax feature.
E00160099	Confirm that all gateway and phone system devices between the Octel and the Bridge support fax transmission.
E00220011	<p>Most subscriber name information is propagated throughout the Octel analog network via “pulling.” That is, when a node requires name information for a particular subscriber, it calls the other node, requests the information, and the other node provides the information if it is available. A few voice mail systems also support the concept of “pushing” subscriber name information out to another node. For example, the Avaya Interchange may not have name information when requested by the Bridge, but it may retrieve the name information later from the other voice mail system, and then call the Bridge and attempt to “push” the name information to the Bridge.</p> <p>Bridge 3.0(5) and earlier versions do not support the “push” concept of name propagation, and will refuse this action. Bridge 3.0(6) and later can be configured to accept pushes of mailbox information. See the “Acceptance of Requests to Push Mailbox Information to the Bridge (Bridge 3.0(6) and Later)” section on page 1-2 for more information.</p>

Do Inbound Messages Get to the Voice Connector?

When a message has reached the Bridge\VPIM\Internet\Out directory, it will wait there until it is delivered to the Voice Connector via SMTP. Usually, a message will arrive in the Bridge\VPIM\Internet\Out directory and leave the directory again within one minute, so you may not even see it. (Note however that a copy of the message should be saved to the Bridge\VPIM\Internet\Out\Tmp directory if you have set the Retention Days for Temporary SMTP Messages setting on the Digital Networking page to a value greater than 0.)

To Verify That a Message Gets to the Voice Connector

-
- Step 1** Log on to the Exchange server on which the Voice Connector is installed.
- Step 2** Open the GwIvc_<Date>.log. The default location for the Voice Connector log files is <Exchange Server Path>\VoiceGateway\LogFiles.
- Step 3** Check the log during the time the message was sent for any inbound messages similar to “Processing incoming OMNI address message.” If there are no inbound messages, the message did not reach the Voice Connector.
- Step 4** If the message did not reach the Voice Connector, go to the [“Troubleshooting Why the Voice Connector Does Not Receive Messages from the Bridge”](#) section on page 6-38.
- If the message did reach the Voice Connector, go to the [“Troubleshooting Voice Message Flow from the Voice Connector to the Subscriber Mailbox”](#) section on page 6-42.
-

Troubleshooting Why the Voice Connector Does Not Receive Messages from the Bridge

- Verify that the domain name is entered correctly. Do the following procedure.

To Verify That the Domain Name Is Entered Correctly

-
- Step 1** In a command prompt window on the Bridge server, enter the command **nslookup <Exchange/SMTP Server>**, where <Exchange/SMTP Server> is the fully qualified domain name of the Exchange/SMTP server that handles incoming SMTP messages.
- Step 2** If the returned response is **Non-Existent Domain**, check the configuration of the DNS zones where the servers are located. Make any necessary changes so that the fully-qualified domain name of the Exchange/SMTP server is recognizable from the zone in which the Bridge server is located.
-

- Verify that the Unity SMTP Mail Suffix is configured correctly on the Bridge server, and determine whether you need to identify an ESMTP server name. Do the following procedure.

To Verify That the Unity SMTP Mail Suffix Is Configured Correctly

-
- Step 1** Open the Exchange 2000 System Manager.
- Step 2** Double-click **Recipient Policies**.
- Step 3** Double-click the **Default Policy**.

- Step 4** Click the **Email Addresses** tab. The Unity SMTP Mail Suffix that is configured on the Bridge Unity Node should be identical to the SMTP address listed here.
- Step 5** Open a command window on the Bridge server.
- Step 6** At the command prompt, enter **telnet <Unity SMTP Mail Suffix> 25**.
- Step 7** If you see the message **220 <ESMTP Server + domain> Microsoft ESMTP Mail Service, Version: <Version number> Ready at <Date and time>**, you do not need to identify a separate ESMTP server name in the Bridge configuration.

If you see the error message **Connection to <Unity SMTP Mail Suffix>...Could Not Open a Connection to Host on Port 25: Connect Failed**, you need to enter an ESMTP server in the Digital Networking configuration on the Bridge server. You should be able to telnet to the ESMTP server on port 25.

- Verify that the relay of messages is not restricted from the Bridge server to the Exchange SMTP server(s). Depending on your network configuration, you may need to manually enter a DNS MX record for the Exchange server in order to allow SMTP message delivery to it, but usually this is not necessary.
- Look in the SMTP logs to see if any errors are reported.
- Use Exchange Message Tracking in the Exchange System Manager to see whether the message is reaching Exchange at all. The message will be addressed to the Voice Connector in the format (IMCEAOMNI-AvVoiceMessage@<Unity SMTP Mail Suffix>).
- Are messages stuck in the MTS-IN and MTS-OUT queues? Do one of the following procedures, as applicable:

To View the MTS-IN and MTS-OUT Queues in Exchange 2000

- Step 1** Log on to the Exchange server on which the Voice Connector is installed.
- Step 2** Start Exchange System Manager. (On the Start menu, click **Programs > Microsoft Exchange > System Manager**.)
- Step 3** Look for **AvExchangeIVC_<Machine name>** or **Exchange 2000 Voice Connector (<Servername>)** under the Connectors subtree for your site.
- Step 4** Look in the MTS-IN and MTS-OUT queues to see if any messages appear to be stuck.
- Step 5** Restart the Exchange 2000 Voice Connector service by using the Services Control Panel.
- Step 6** Confirm that the SMTP service is running in the Services Control Panel.

To View the Voice Connector Queue in Exchange 2003

- Step 1** Log on to the Exchange server on which the Voice Connector is installed.
- Step 2** Start Exchange Systems Manager. (On the Start menu, click **Programs > Microsoft Exchange > System Manager**.)
- Step 3** Expand the **Servers** container, and then expand the server on which the Voice Connector is installed.
- Step 4** Within the server container, click **Queues**. You should see AvExchangeIVC<Server name> listed in the pane on the right.

- Step 5** Double-click **AvExchangeIVC<Server name>**.
A queue window opens.
- Step 6** Click **Find Now** to see all of the messages that are in the queue.

-
- Check the Windows Event Viewer System and Application logs for errors or warnings on the Bridge server and on the Exchange server on which the Voice Connector is installed.
 - Check to see whether, after entering the Windows 2000 SMTP server, e-mail entering your Exchange organization is re-routed to a smart host, non-Exchange corporate SMTP relay server, secure e-mail server, or any other traffic filtering server that may not route incoming SMTP messages to the Voice Connector in Exchange. In particular, this may be an issue when Exchange is using a shared Domain Name Space where Exchange is not configured as authoritative for this address. If this is true in your circumstance, a special Recipient Policy for the Voice Connector and an Exchange SMTP connector can be configured to send only those message addressed to the Voice Connector from the Bridge directly to the Voice Connector without being re-routed. See the following procedures:
 - [To Create a Special Recipient Policy for the Voice Connector, page 6-40](#)
 - [To Apply the Special Recipient Policy to the Voice Connector, page 6-41](#)
 - [To Configure the Bridge to Use the Special Recipient Policy, page 6-41](#)
 - [To Configure an Exchange SMTP Connector to Route Messages from the Bridge Server Directly to the Voice Connector, page 6-42](#)

**Caution**

Consult the Exchange administrator for your organization before doing the following procedures. Miscommunication of the Recipient Policies and/or the SMTP connector could result in problems routing other SMTP mail for the organization.

To Create a Special Recipient Policy for the Voice Connector

- Step 1** On the Exchange server on which the Voice Connector is installed, open the Exchange System Manager. (The Recipient Policy must be created on the Exchange server on which the Voice Connector is installed.)
- Step 2** Right-click **Recipient Policies** and click **New > Recipient Policy**.
- Step 3** In the New Policy window, confirm that **E-Mail Addresses** is the only selection, and click **OK**.
- Step 4** On the General tab, enter a meaningful name. Do not configure any Filter rules.
- Step 5** On the E-Mail Addresses (Policy) tab, select the SMTP address and click **Edit**.
- Step 6** Copy the address (for example, “@domain.com”) from the Address field and click **Cancel**.
- Step 7** On the E-Mail Addresses (Policy) tab, click **New**.
- Step 8** Select **SMTP Address** and click **OK**.
- Step 9** Paste the SMTP address that you copied in [Step 6](#) into the Address field.
- Step 10** Insert a name (for example, vconnector) followed by a period between the @ sign and the rest of the address (for example, “vconnector.domain.com”). You can use any name, though it must match what you configure in the [“To Configure the Bridge to Use the Special Recipient Policy” procedure on page 6-41](#).
- Step 11** Verify that the check box **This Exchange Organization Is Responsible for All Mail Delivery to This Address** is checked.

- Step 12** Click **OK**.
- Step 13** Check the check box next to the address that you added in [Step 10](#), and verify that the row is highlighted.
- Step 14** Click **Set as Primary**, and click **OK**.
When you click Set as Primary, the new address should change to bold text.
- Step 15** Click **Yes** to the warning about updating the corresponding recipient e-mail addresses.
- Step 16** Right-click the new policy and click **All Tasks > Move Down** until Move Down is grayed out.
The new policy must be the lowest policy on the list, except the Default Policy.
-

To Apply the Special Recipient Policy to the Voice Connector

- Step 1** On the Exchange server on which the Voice Connector is installed, open the Exchange System Manager.
- Step 2** Expand the **Connectors** container in the left-hand pane.
- Step 3** Right-click **Exchange 2000 Voice Connector (<Server name>)**, and select **Properties**.
- Step 4** At the bottom of the Options tab, click the drop down list for **Recipient Policy to Calculate Enterprise GDI for MTS-IDs**.
- Step 5** Select the new recipient policy you created in the [“To Create a Special Recipient Policy for the Voice Connector” procedure on page 6-40](#).
- Step 6** Click **Apply**, then click **OK** to exit.
- Step 7** Restart the Exchange 2000 Voice Connector service.
-

To Configure the Bridge to Use the Special Recipient Policy

- Step 1** On the Bridge server in the Bridge Administrator, go to the **Digital Networking** page.
- Step 2** In the ESMTP Server field, enter either the fully qualified domain name or the IP address of the Exchange server on which the Voice Connector is installed, and click **Save**.
- Step 3** Go to the Unity Node page and click **Edit**. Enter the address you used for the new recipient policy in the [“To Create a Special Recipient Policy for the Voice Connector” procedure on page 6-40](#), but without the @ sign (for example, “mybridge.domain.com”), and click **Save**.
- Step 4** Repeat [Step 3](#) for each Unity Node.



Note If you need to make the change to a lot of Unity Nodes, you can use the Cisco Unity Bridge Bulk Node utility. The utility is available for download from the Cisco Unity Tools website at <http://www.ciscounitytools.com>. For details on the Bulk Node utility, refer to the Readme.htm file that is included with the utility.

- Step 5** Open the Services applet on the Bridge Server, and restart the Digital Networking service.
-

To Configure an Exchange SMTP Connector to Route Messages from the Bridge Server Directly to the Voice Connector

-
- Step 1** On the Exchange server on which the Voice Connector is installed, open the Exchange System Manager.
- Step 2** Expand the tree in the left pane to view the Connectors directory. On some servers the Connectors directory will be in the Organization root. On others, most notably where multiple Routing Groups are being used, you will need to be sure to select the Connectors directory under the Routing Group in which the Voice Connector is installed.
- Step 3** Right-click **Connectors** and click **New > SMTP Connector**.
- Step 4** On the General tab, enter a meaningful name.
- Step 5** On the General tab, select **Forward All Mail Through This Connector to the Following Smart Hosts**. In the field below, enter the IP address of the Exchange server on which the Voice Connector is installed, enclosed in square brackets (for example, “[10.10.255.1]”).
- Step 6** On the General tab, click **Add**.
- Step 7** Select the server on which the Voice Connector is installed and click **OK** to set this as the bridgehead server for the SMTP connector.
- Step 8** Click the **Address Space** tab.
- Step 9** On the Address Space tab, click **Add**.
- Step 10** Select **SMTP** and click **OK**.
- Step 11** In the E-Mail Domain field, enter the address you used for the new recipient policy in the [“To Create a Special Recipient Policy for the Voice Connector” procedure on page 6-40](#), but without the @ sign (for example, “vconnector.domain.com”).
- Step 12** Leave the value in the Cost field set to 1, then click **OK**.
- Step 13** Click **OK** to complete configuration of the SMTP connector.
- Step 14** Send a test voice message from Octel to a Cisco Unity subscriber to see whether the message is delivered.
- Step 15** Send a test e-mail to an outside address to verify that e-mail still works.
-

Troubleshooting Voice Message Flow from the Voice Connector to the Subscriber Mailbox

Follow the steps in this section when voice messages make it to the Voice Connector, but are not delivered to the subscriber mailbox.

- Open the GwIvc.log and look for any errors about the incoming message. Troubleshoot any errors that are displayed.
- On the Exchange server on which the Voice Connector is installed, look in the Windows Event Viewer System and Application logs. Look for warnings or errors. In particular, look for warnings or errors that indicate that messages have been returned because of invalid attachments.
- Verify whether the Voice Connector settings are correct. Do the following procedure.

To Verify Voice Connector Settings

-
- Step 1** On the Exchange server on which the Voice Connector is installed, in the Exchange System Manager under the Connectors subtree, right-click **AvExchangeIVC_<Machine name>**, and select **Properties**.



Note When the Exchange System Manager Cleanup Agent has been run, the name of the Voice Connector changes to Exchange 2000 Voice Connector (<Machine name>).

- Step 2** Click the **Address Space** tab and confirm that a type **OMNI** is listed with an Address of * and a Cost of 1.
- Step 3** Confirm that the Connector Scope is set to **Entire Organization**.
-

- If the Voice Connector is not installed in the same routing group as the mailbox of the subscriber who sent the message, verify that Exchange routing group connectors are properly set up to route messages between the groups.
- Use Exchange message tracking to follow the message through Exchange and determine why it was not delivered.

After You Finish Troubleshooting

When finished troubleshooting, you should reset most of the logs and traces back to their defaults. However, leave the call tracing level on the System Settings page in the Bridge Administrator set to Verbose, as this call tracing level is required by BANANA.



Caution

Logs and traces that you enable on the Bridge server, on the Exchange server on which the Voice Connector is installed, and on the Cisco Unity server can take up a great deal of hard disk space. Disable the logs and traces when you finish troubleshooting, with the exception of the call traces (also referred to as the starfish logs) on the Bridge server.

Reset the following logs and traces:

- In the Bridge Administrator, on the Digital Networking page:
 - Reset the Retention Days For Temporary SMTP Messages back to 0 (zero). (These messages consume significant hard disk space, so you should always configure this setting to zero unless you are troubleshooting and also monitoring hard disk consumption.)
 - Reset the Tracing Level back to None. (Typically, these logs do not consume significant hard disk space, so you may choose to leave the Tracing Level set to Flow.)
- In the Exchange System Manager:
 - Reset the Voice Connector Logging Level back to Warning. (You may choose to leave these logs set to the Information level, which provides more detail than the Warning level. With logging at the Information level, you should monitor the hard disk space consumed by the log files. You may need to adjust the Log Recycle Days setting or set a limit for the hard disk space allowed for the logs.)
 - Disable Exchange message tracking. (You may choose to leave message tracking enabled. Monitor occasionally to make sure that no more than the desired hard disk space is consumed for storage of these logs.)
 - Disable SMTP logging. (You may choose to leave these logs enabled. Monitor occasionally to make sure that no more than the desired hard disk space is consumed for storage of these logs.)

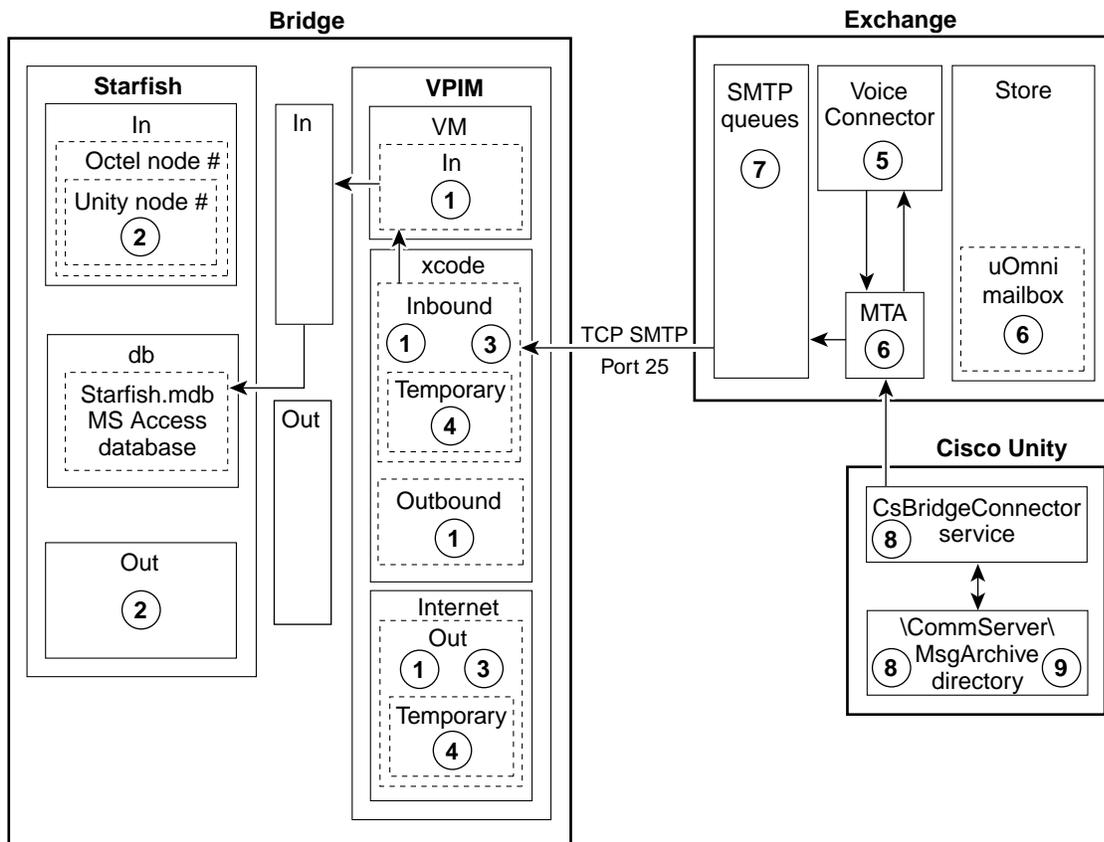
Directory Messages Are Not Processed

If voice messages between Cisco Unity and the Octels are delivered successfully in both directions, chances are that directory messages will be also be delivered successfully. As [Figure 6-5](#) and [Figure 6-6](#) illustrate, the trouble spots are similar. However, if you do encounter a problem with directory messages, see the “[CsBridgeConnector Traces](#)” section on [page 6-45](#) for information on enabling the traces on the Cisco Unity bridgehead server.

If directories get out of synch, see the following sections for information on how to force full synchronizations:

- [Full Synchronization of Bridge Subscribers with Octel Node Directories](#), [page 6-46](#)
- [Full Synchronization of Cisco Unity Subscribers with the Unity Node Directories](#), [page 6-47](#)

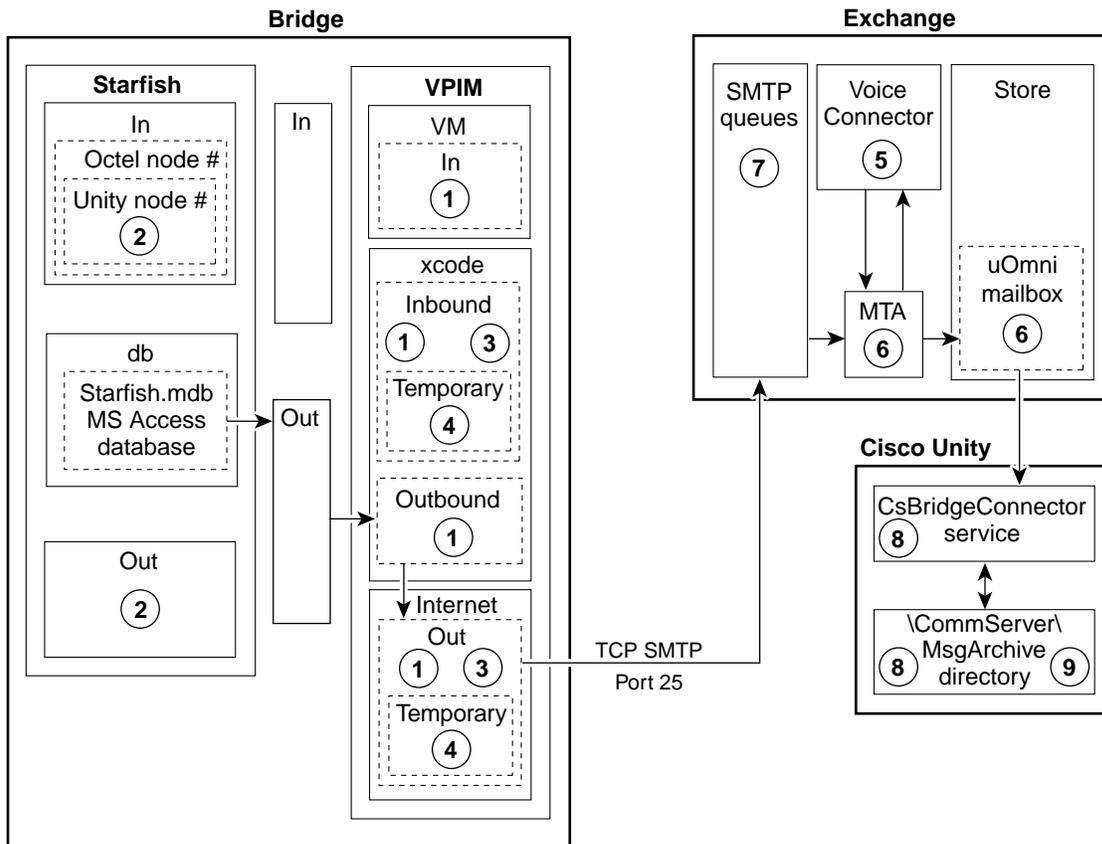
Figure 6-5 Troubleshooting Problems with Directory Messages from Cisco Unity to the Bridge



- | | |
|--|--|
| ① Bridge VPIM traces
<Bridge>\VPIM\Trace | ⑤ Voice Connector traces
<ExchangeServer>\VoiceGateway\LogFiles |
| ② Use BANANA to view Bridge call log traces
<Bridge>\Starfish\Log | ⑥ Exchange message tracking—Exchange System Manager |
| ③ Bridge VPIM message log
<Bridge>\VPIMMsgLog | ⑦ Exchange SMTP logging—Exchange System Manager |
| ④ Temporary SMTP messages
<Bridge>\VPIM\Xcode\Inbound\Tmp | ⑧ CsBridgeConnector traces—Unity Diagnostic Tool |
| | ⑨ Sent/received vCard data |

76785

Figure 6-6 Troubleshooting Problems with Directory Messages from the Bridge to Cisco Unity



- | | |
|--|--|
| ① Bridge VPIM traces
<Bridge>\VPIM\Trace | ⑤ Voice Connector traces
<ExchangeServer>\VoiceGateway\LogFiles |
| ② Use BANANA to view Bridge call log traces
<Bridge>\Starfish\Log | ⑥ Exchange Message Tracking–Exchange System Manager |
| ③ Bridge VPIM message log
<Bridge>\VPIMMsgLog | ⑦ Exchange SMTP Logging–Exchange System Manager |
| ④ Temporary SMTP messages
<Bridge>\VPIM\Xcode\Inbound\Tmp | ⑧ CsBridgeConnector traces–Unity Diagnostic Tool |
| | ⑨ Sent/received vCard data |

76783

CsBridgeConnector Traces

The CsBridgeConnector macro traces can be used to troubleshoot directory synchronization problems.

To Enable CsBridgeConnector Traces

-
- Step 1** On the Windows Start menu, click **Programs > Cisco Unity > Unity Diagnostic Tool**.
- Step 2** On the Cisco Unity Diagnostic Tasks screen, click **Configure Macro Traces**. The Welcome to the Configure Macro Traces wizard displays.
- Step 3** Click **Next**. The Configure Macro Traces page is displayed.

- Step 4** Expand **Bridge Directory Synchronization Traces**. Check the box next to the applicable macro trace(s):
- Basic Bridge delivery synchronization trace—Set this trace to verify that directory synchronization is working correctly within Cisco Unity.
 - General Bridge delivery synchronization trace—Set this trace to narrow down directory synchronization problems to a specific Cisco Unity component.
 - Extensive Bridge delivery synchronization trace—Set this trace to include additional Cisco Unity components and enable extensive logging.
- Step 5** Click **Next** and then click **Finish**.
- Step 6** On the Cisco Unity Diagnostic Tasks screen, click **Start New Log Files**.
- Step 7** After the problem reoccurs, or sufficient time has passed to gather message data, in the tree in the left pane of the Unity Diagnostic tool, click **Processes > AvCsMgr**, and click the **Current** log file to view it. The selected log file is formatted and displayed in the right pane.
- Step 8** To export or save a copy of the log file, click **Action > Export List**.
- Step 9** Name the file and save it to a location of your choice in .txt or .csv format.
- Step 10** Disable all diagnostic traces that were activated in [Step 4](#).
-

Full Synchronization of Bridge Subscribers with Octel Node Directories

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

To Synchronize Bridge Subscribers with Octel Node Directories

- Step 1** On the Cisco Unity bridgehead server desktop, double-click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.
- Step 3** In the Unity Settings pane, click **Administration - Full synchronization of Bridge Subscribers with Octel Node Directories**.
- Step 4** In the **New Value** list, click **1**, then click **Set**.
- Step 5** When prompted, click **OK**.
- Step 6** Click **Exit**.
-

Full Synchronization of Cisco Unity Subscribers with the Unity Node Directories

For directory data about newly-created subscribers to be automatically sent to the Bridge, you first create the subscribers in Cisco Unity, and then create corresponding Unity Node(s) on the Bridge. If you do the reverse and create a Unity Node on the Bridge before creating any subscribers with the same serial number, you will have to force a synchronization.

During normal operation, Cisco Unity automatically synchronizes subscriber information with the Bridge on a regular basis. When a subscriber account is added, deleted, or modified, Cisco Unity sends the account information to the Bridge. The Bridge makes this information available to other Octel nodes when they make an administrative call to retrieve the voice and text names of Cisco Unity subscribers.

You may want to force synchronization if the Cisco Unity server, the Bridge, or the network connection to the Bridge has been down for a period of time, and if there have been numerous changes to subscriber information in Cisco Unity.

Directory synchronization does not affect messaging. Subscribers can still send and receive messages when the directories are not synchronized.

Use one of the following procedures, as applicable to your situation:

- [To Trigger a Directory Synchronization of Cisco Unity Subscriber Information with the Unity Node Directories on the Bridge Server\(s\), page 6-47](#)—This updates all Unity nodes on selected Bridge server(s).
- [To Trigger a Directory Synchronization of Cisco Unity Subscriber Information with a Specific Unity Node Directory on the Bridge Server, page 6-47](#)—This updates a specific Unity node on one Bridge server.

To Trigger a Directory Synchronization of Cisco Unity Subscriber Information with the Unity Node Directories on the Bridge Server(s)

-
- Step 1** On the Cisco Unity bridgehead server, in the Cisco Unity Administrator, go to the **Network > Bridge Options > Synchronization** page.
 - Step 2** Verify that each Bridge server to which directory information will be sent is configured with a Unity Node for each serial number listed in the Node ID table.
 - Step 3** In the Cisco Unity Bridge Servers table, check the check box next to each Bridge address to which Cisco Unity subscriber information should be sent.
 - Step 4** Click **Synchronize** to force a full synchronization of Cisco Unity subscribers with the subscriber directory on the Bridge. All Unity nodes on the selected Bridge server will be updated.

For large directories the synchronization may take several hours. Subscribers can still send and receive messages while the directories are synchronizing.

To Trigger a Directory Synchronization of Cisco Unity Subscriber Information with a Specific Unity Node Directory on the Bridge Server

-
- Step 1** On the Bridge server, open the Bridge Administrator.
 - Step 2** Click **Unity Nodes**.
 - Step 3** On the list of nodes, click the Unity node whose directory needs to be updated.

- Step 4** Click **Edit**.
 - Step 5** Either print a copy of the page or write down the information that is on it.
 - Step 6** Click **Delete**, and then **OK** on the warning dialog box.
 - Step 7** Click **Add** to add back the node that you just deleted.
 - Step 8** Reenter the information from the deleted node (which you captured in [Step 5](#)), and click **Save**.
Directory information about all Cisco Unity subscribers associated with the same serial number as the Unity node will be sent to the Bridge.
-