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

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 4-7 or the "Messages Are Not Delivered from Octel to Cisco Unity" section on page 4-24 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 that sends outbound SMTP messages to the Bridge server. See the "Configuring the Bridge and Testing the Configuration" section on page 2-15 for more information.

6. Use the Domino Administrator to confirm that the Interop Gateway Foreign domain document exists. Also verify that the Interop Gateway mail file itself exists on the Domino server and directory specified in the Foreign domain document. See the "To Confirm That the Interop Gateway Foreign Domain Document and Mail File Exist" procedure on page 4-3. Note that if Cisco Unity cannot find the Interop Gateway mail file, you should see errors in Event Viewer. In this case:

   – If the Interop Gateway Foreign domain document and/or mail file has been inadvertently deleted, reconfigure the Interop Gateway, as described in the "Configuring the Interop Gateway" section on page 2-7. Be sure to use the same Foreign domain name that you used previously.

   – If you suspect that the Interop Gateway mail file may have been inadvertently moved to another Domino server, see the "Moving the Interop Gateway Mail File" section on page 3-11 for information on how to move the mail file such that Cisco Unity is aware of the change.

7. Use the Domino Administrator to confirm that Interop Gateway Foreign domain name is correct. See the "To Confirm That the Foreign Domain Name Settings Are Correct" procedure on page 4-3.

   If you determine that the Foreign domain name has been changed in some but not all of the places where the name is stored, refer to the "Changing the Interop Gateway Foreign Domain Name" section on page 3-9 for information on how to change the foreign domain such that Cisco Unity is aware of the change.

8. 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 2-9.

9. 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.

10. Each Bridge delivery location is correctly configured.

11. 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.

12. The correct serial number and legacy mailbox ID is assigned to each Cisco Unity subscriber.

Procedures for Troubleshooting Configuration Problems

To Confirm That the Interop Gateway Foreign Domain Document and Mail File Exist

Step 1   In the Domino Administrator, click the **Configuration** tab.

Step 2   In the left pane, expand **Messaging > Domains**. You should see the Foreign domain document used by the Interop Gateway in the list in the right pane. (You may need to expand the list in the right pane.)

Step 3   Open the Foreign domain document.

Step 4   Confirm that the Foreign domain name is correct.

Step 5   Click the **Mail Information** tab, and write down the server name and mail file name.

Step 6   Close the Foreign domain document.

Step 7   Browse to the directory on the Domino server specified in the Foreign domain document, and confirm that the Interop Gateway mail file itself exists.

To Confirm That the Foreign Domain Name Settings Are Correct

The Foreign domain name used by the Interop Gateway is stored in several places, and the name must be exactly the same in each place. The following procedure describes how to check the Foreign domain name in each of the places in which it is stored.

Step 1   In the Domino Administrator, click the **Configuration** tab.

Step 2   In the left pane, expand **Messaging > Domains**. You should see the Foreign domain document used by the Interop Gateway in the list in the right pane (you may need to expand the list).

Step 3   Write down the name displayed in the list and then close the Foreign domain document.

Step 4   If the recipient of the message(s) that you are tracing is a Bridge subscriber, do the following sub-steps. Otherwise, skip to Step 5.

    a.   In the Domino Administrator, click the **People and Groups** tab.

    b.   In the left pane, expand **People** such that you see the Person document for the Bridge subscriber when you scroll through the list in the right pane.

    c.   Double-click the Person document for the Bridge subscriber.

    d.   On the Basics tab in the Forwarding Address field, write down the Foreign domain name. This is the name to the right of the @ symbol.

    e.   Close the Person document.

Step 5   On a Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 6   In the left pane of the Tools Depot window, expand Administration Tools and double-click **Advanced Settings Tool**.

Step 7   In the Unity Settings list, click **Networking—Change Interop Gateway Foreign Domain Name (Domino Only)**.

Step 8   Write down the name in the Current Value field.

Step 9   Close the Advanced Settings tool.

Step 10   In the left pane of the Tools Depot window, expand **Diagnostic Tools**.

Step 11   Double-click **Data Link Explorer**.

Step 12   In the Table Name list, scroll down and click **Configuration**.

Step 13   In the Column Name list, click **NodeName**.

Step 14   In the list in the bottom pane, scroll down towards the end of the list, and click the row where the name in the NodeName column is **ForeignDomain**.

Step 15   Write down the name in the NodeValue column.

Step 16   Close the Data Link Explorer window and exit Tools Depot.

Step 17   Compare the names you wrote down in Step 3, Step 4, Step 8, and Step 15. If the names are not exactly the same, change the Foreign domain name according to the instructions in the "Changing the Interop Gateway Foreign Domain Name" section on page 3-9.

If the names are exactly the same, and your installation consists of multiple Cisco Unity servers, repeat Step 5 through Step 17 on another Cisco Unity server until you have checked the settings on all of the Cisco Unity servers. If you discover a mismatch at any point and change the Foreign domain name according to the instructions in the "Changing the Interop Gateway Foreign Domain Name" section, the name will be changed on every Bridge subscriber Person document and every Cisco Unity server.

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 4-4
- Tools for Troubleshooting Communication Problems Between the Bridge and Cisco Unity, page 4-5
- Tools for Troubleshooting Problems with the Interop Gateway, page 4-6
- Tools for Troubleshooting Directory Synchronization Problems on the Cisco Unity Server, page 4-6

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 4-7
- Messages Are Not Delivered from Octel to Cisco Unity, page 4-24
- Directory Messages Are Not Processed, page 4-42

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 3-5 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.mmddtttt.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 Interop Gateway

- Cisco Unity Diagnostic Tool—Because the Interop Gateway runs as a service on a Cisco Unity server, you can set traces for it by using the Cisco Unity Diagnostic tool. The provides details.

- Event Viewer—The Interop Gateway logs errors to the application log in Event Viewer.

- Domino Administrator—You can use the Domino Administrator for:

  – Opening the Interop Gateway mail file.

  – Viewing the Interop Gateway Foreign domain document.

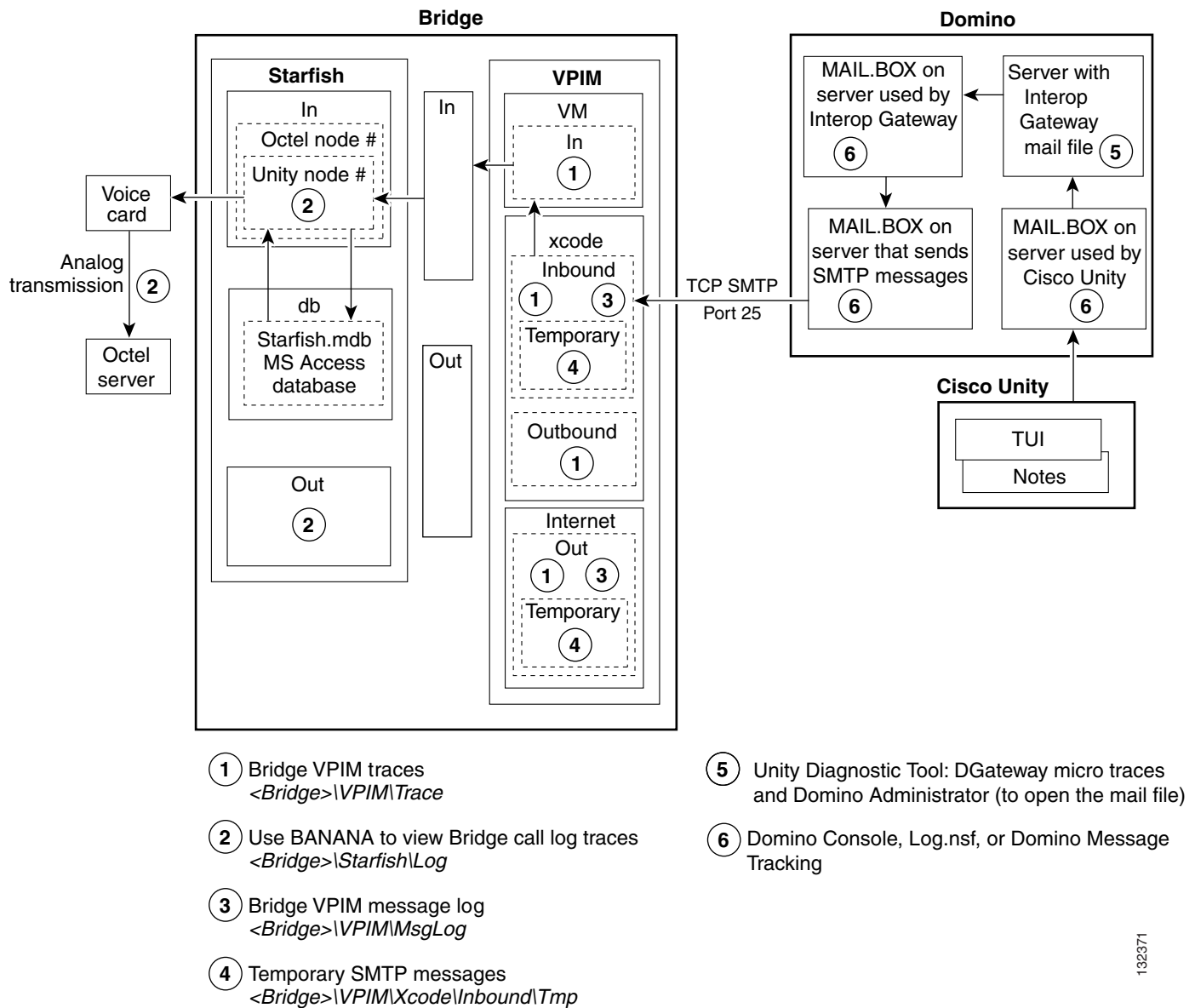 – Opening Log.nsf or using Domino Messaging Tracking

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 Domino, which routes the message to the Interop Gateway mail file. The Interop Gateway converts the message to VPIM format (with proprietary extensions) and hands it back to Domino to be sent to the Bridge via SMTP. The Bridge converts the received VPIM message to an Octel message and sends it to the Octel node via analog lines.

Figure 4-1 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 MAIL.BOX on the Domino server used by Cisco Unity for mail delivery. (This is the Domino server on which the mail file of the Person document for the Cisco Unity server is located.) This is true when subscribers use the TUI to send messages, but when subscribers use the DUC-enabled Notes client, messages originate from the Domino server on which the mail file of the subscriber sending the message is located.

Figure 4-1   *Troubleshooting Message Flow from Cisco Unity to Octel*

① Bridge VPIM traces
    <Bridge>\VPIM\Trace

② Use BANANA to view Bridge call log traces
    <Bridge>\Starfish\Log

③ Bridge VPIM message log
    <Bridge>\VPIM\MsgLog

④ Temporary SMTP messages
    <Bridge>\VPIM\Xcode\Inbound\Tmp

⑤ Unity Diagnostic Tool: DGateway micro traces
    and Domino Administrator (to open the mail file)

⑥ Domino Console, Log.nsf, or Domino Message
    Tracking

132371

Bridge In and Out Directories

Note the Bridge\In and Bridge\Out directories in Figure 4-1.

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 Domino. If either service is stopped for some reason, messages will queue up as shown in the following table.

Table 4-1   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 MAIL.BOX on the Domino server that sends outgoing SMTP messages.	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 MAIL.BOX on the Domino server that sends outgoing SMTP messages.	Will queue up on the Octel servers.

Troubleshooting Why Messages Are Not Delivered from Cisco Unity to Octel

Figure 4-2 illustrates the troubleshooting process at a high level.

Figure 4-2   Troubleshooting Why Messages Are Not Delivered from Cisco Unity to Octel
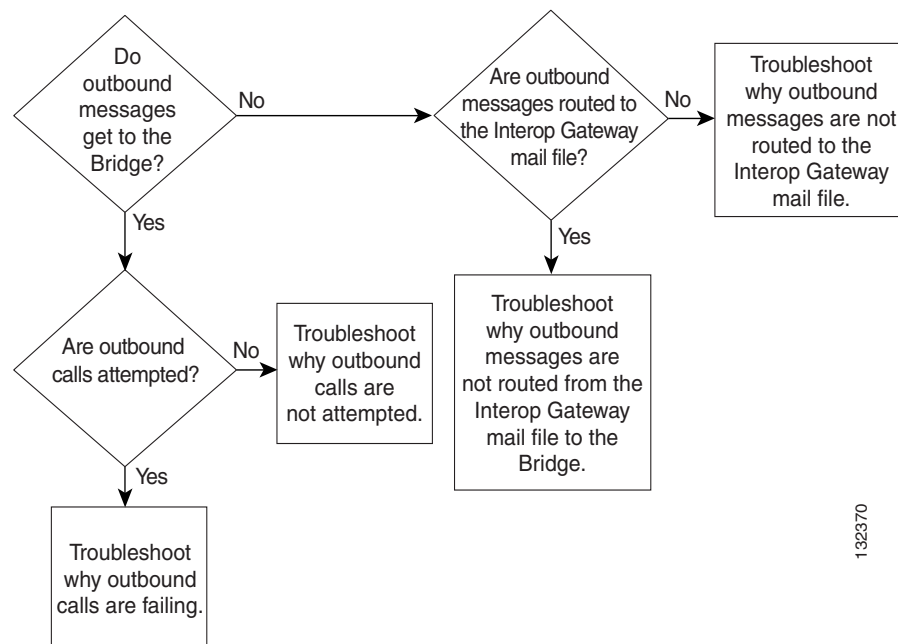
The following list provides an overview of the troubleshooting steps. Detailed procedures and troubleshooting steps follow the list.

1. Enable the various logs and traces as described in the "Enabling Logs and Traces" section on page 4-10.

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 4-14.

5. Determine why calls from the Bridge to the Octels are failing. Go to the "Troubleshooting Why Outbound Calls Are Failing" section on page 4-14.

6. Are Outbound Messages Routed to the Interop Gateway Mail File?

   If messages are not routed to the Interop Gateway mail file, go to the "Troubleshooting Why Outbound Messages Are Not Routed to the Interop Gateway Mail File" section on page 4-20.

   If messages are routed to the Interop Gateway mail file, go to the "Troubleshooting Why Outbound Messages Are Not Routed from the Interop Gateway Mail File to the Bridge" section on page 4-21.

7. Reset the logs and traces as described in the "After You Finish Troubleshooting" section on page 4-23.

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 4-10
- To Enable Troubleshooting Logs and Traces on the Bridge Server, page 4-11
- To Set Diagnostic Traces, page 4-11

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 Set Diagnostic Traces

Step 1   On the Windows Start menu on the Cisco Unity server on which the Interop Gateway service is running
(this may or may not be the bridgehead server), click **Programs > Cisco Unity > Unity Diagnostic
Tool**.

Step 2   On the Cisco Unity Diagnostic Tasks screen, click **Configure Micros Traces**. The Welcome to the
Configure Micro Traces wizard is displayed.

Step 3   Click **Next**. The Configure Micro Traces page is displayed.

Step 4   Scroll down and enable the following micro traces:

- DGateway
- MALLn
- NoteCommon

Step 5   Click **Next** and then click **Finish**.

Step 6   On the Cisco Unity Diagnostic Tasks screen, click **Start New Log Files**.

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 Domino to the
Bridge server. Go to the "Are Outbound Calls Attempted?" section on page 4-12.

Step 3   If messages do not get to the Bridge, go to the "Are Outbound Messages Routed to the Interop Gateway Mail File?" section on page 4-19.
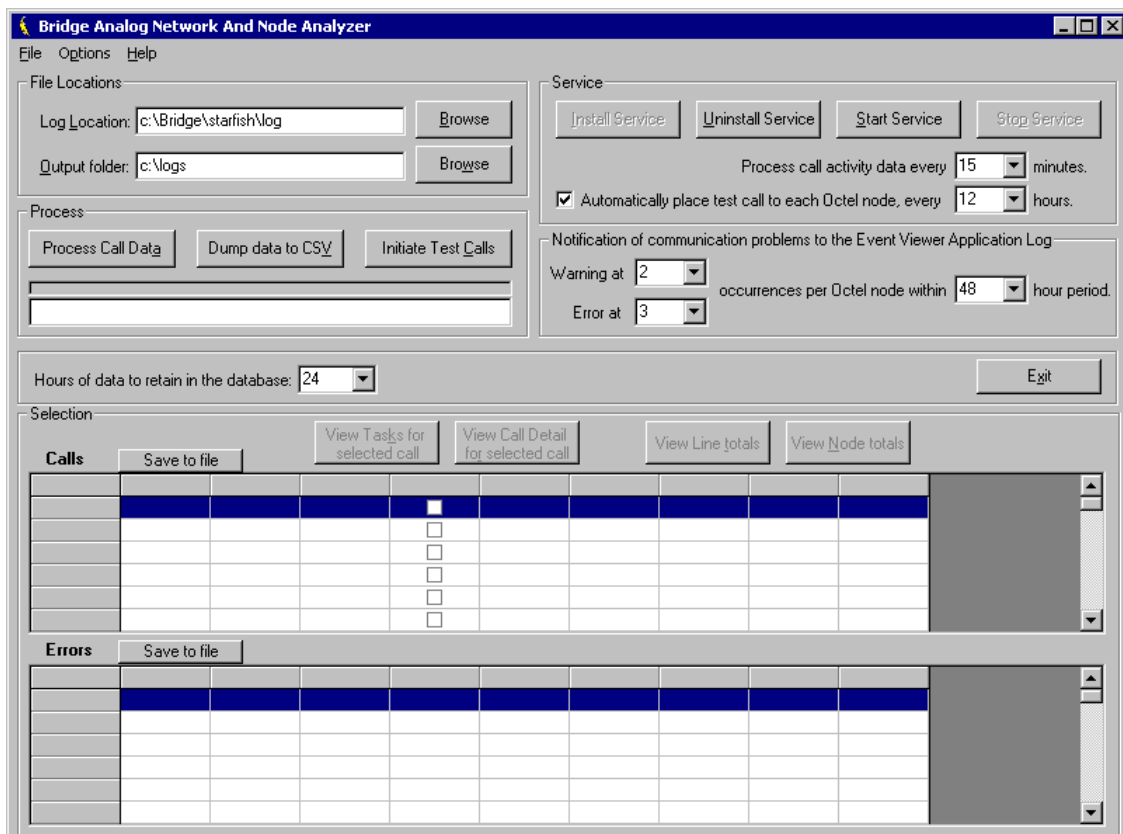
Are Outbound Calls Attempted?

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 4-14.

Otherwise, go to the "Troubleshooting Why Outbound Calls Are Failing" section on page 4-14.

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/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 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.

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

Table 4-2   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.

Table 4-2 **Configuration and Other Problems That Result in Outbound Call Failures (continued)**

Error Code	Description
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.
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: • The Octel server(s) are supported. The only supported Octel servers are those listed in "Supported Voice Messaging Systems" section of the *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 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: • 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: • The Octel server(s) are supported. The only supported Octel servers are those listed in "Supported Voice Messaging Systems" section of the *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 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 4-2   Configuration and Other Problems That Result in Outbound Call Failures (continued)

Error Code	Description
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.
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	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. Confirm that the phone number specified for the node being called is correct by dialing the phone number from a phone.

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 8-1 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.

Are Outbound Messages Routed to the Interop Gateway Mail File?

If outbound messages do not reach the Bridge, the first step is to determine whether the messages were routed to the Interop Gateway mail file, as described in the following procedure:

To Confirm That Messages Are Routed at the Interop Gateway Mail File

Step 1 On the Cisco Unity server on which the Interop Gateway service is running, open the Services MMC. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 2 Right-click **CsDomInteropGty**, and click **Stop**.

Step 3 Send a test message to an Octel recipient. Because the Interop Gateway service has been stopped, if the message arrives at the Interop Gateway mail file, the message will remain there until the service is started.

Step 4 Use the Domino Administrator or Notes to open the Interop Gateway mail file to see if the message is there.

In order to use the Domino Administrator or Notes to access the Interop Gateway mail file, you will need to verify that you have permission to do so. How you do this depends on the Domino version and security policies for your organization. Use the following as a guide, and consult your Domino documentation for more information:

If the Domino server on which the Interop Gateway mail file is located is running Domino 6.0 or later:

- If you have Full Access Administration rights, you will be able to open the mail file.

- If someone who has Full Access Administration rights is available, have the administrator add you to the Interop Gateway mail file Access Control List (ACL) with at least Editor permissions.

If the Domino server on which the Interop Gateway mail file is located is running Domino 5.x, or if someone with Full Access Administration rights is unavailable:

- Log on to the Domino Administrator by using the name and password of the Person document that was created for the Cisco Unity server on which the Interop Gateway service was configured to run. This account should have Editor plus Delete Documents permissions in the ACL of the Interop Gateway mail file.

  You can either use this account whenever you open the Interop Gateway mail file, or you can add yourself to the Interop Gateway mail file ACL with at least Editor permissions.

Step 5 After seeing whether the message is in the mail file, close it.

Step 6 On the Cisco Unity server, restart the Interop Gateway service, **CsDomInteropGty**, and close the Services MMC.

If the test message was in the Interop Gateway mail file, go to the "Troubleshooting Why Outbound Messages Are Not Routed from the Interop Gateway Mail File to the Bridge" section on page 4-21.

If the test message was not in the Interop Gateway mail file, go to the "Troubleshooting Why Outbound Messages Are Not Routed to the Interop Gateway Mail File" section on page 4-20.

Troubleshooting Why Outbound Messages Are Not Routed to the Interop Gateway Mail File

Each Cisco Unity server has a corresponding Person document and mail file in Domino. When subscribers send messages via the TUI, Cisco Unity hands off the messages to the Domino server on which the mail file of the Person document for the sending Cisco Unity server is located. For messages addressed to remote recipients (either Bridge subscribers or blind addresses), Domino routes the messages to the Interop Gateway mail file according to your Connection documents. The route the messages takes depends on your Domino configuration. Similarly, when subscribers use the DUC-enabled Notes client to send a message to a remote recipient, the message is routed from the Domino server on which the subscriber mail file is located to the Domino server on which the Interop Gateway mail file is located, according to your Connection documents.

For outbound messages to the Bridge, you should see an entry in the Domino console or in log.nsf from the Domino router about routing a message addressed to
OMNI:<Dial ID>_<Remote Mailbox Number>@<Foreign Domain Name>

For example:

04/22/2005 11:54:09 AM Router: Message 0067D3E9 transferred to DOMSERVER1/DOMORG for OMNI:001_5234@voicemail.europe.cisco.com via Notes

The portion of the address before the "@" symbol is either the extension address of a Bridge subscriber or a blind address. The portion of the address after the "@" symbol must be the Foreign domain name used by the Interop Gateway. In the above example, "voicemail.europe.cisco.com" is the Foreign domain name.

If you have determined that messages are not being delivered to the Interop Gateway mail file, use the following list to troubleshoot the problem.

1. Confirm that the following Domino servers are running:

    – The Domino server used by Cisco Unity for message delivery (or the Domino server on which the sending subscriber mail file is located).

    – The Domino server on which the Interop Gateway mail file is located.

    – All Domino servers used in message routing to the Domino server on which the Interop Gateway mail file is located.

    Also confirm that the Domino router is running on all of those servers.

2. Scroll back through the Domino console or look in log.nsf for a message similar to "No route point found to <Foreign Domain Name>." If you see this message, review your Connection documents to see whether you can determine what is preventing Domino from routing the message to the Domino server on which the Interop Gateway mail file is located. Refer to your Domino Administrator documentation for more information.

    The "No route point found" message may also indicate that the Interop Gateway Foreign domain name may have been changed in some but not all of the places where the name is stored. If you suspect that the Interop Gateway Foreign domain name may have been inadvertently changed, refer to the "Changing the Interop Gateway Foreign Domain Name" section on page 3-9 for information on how to change the Foreign domain name such that Cisco Unity is aware of the change.

3. Check to see if the message is stuck in MAIL.BOX on the Domino server used by the sending Cisco Unity for message delivery, or if the message is stuck in MAIL.BOX on any of the Domino servers that are involved in routing messages to the Domino server on which the Interop Gateway mail file is located. Refer to your Domino documentation for more information.

4. Check to see if there is a quota on the Interop Gateway mail file and if Domino is configured to not deliver messages if the mail file is over quota.

5. Check the Interop Gateway Foreign domain document to make sure that it contains the correct server name and mail file name.

6. Go to the "After You Finish Troubleshooting" section on page 4-23 for details on how to reset the logs and traces to default values, and if you were unable to solve the problem, instructions are provided on how to gather the necessary logs to provide to Cisco TAC.

Troubleshooting Why Outbound Messages Are Not Routed from the Interop Gateway Mail File to the Bridge

Outbound messages received by the Interop Gateway are addressed in the following format:

OMNI:<Dial ID>_<Remote Mailbox Number>@<Foreign Domain Name>

The Interop Gateway uses the Dial ID in the address to look up the corresponding delivery location settings in SQL to obtain the Bridge server full computer name. After converting the message to the proprietary VPIM format, the Interop Gateway gives the message back to Domino for routing via SMTP to the Bridge. The message is placed in MAIL.BOX of the Domino server used for message delivery by the Cisco Unity server on which the Interop Gateway service is running. From there, the message is routed to the Domino server that handles outbound SMTP messages, according to your Connection documents. The route that the message takes depends on your configuration.

The Interop Gateway addresses messages to the Bridge in the following format:

<Remote Mailbox Number>@<Bridge Server Full Computer Name>

For example:

5234@ParisBridge2.europe.cisco.com

Use the following list to troubleshoot why outbound messages are not routed from the Interop Gateway mail file to the Bridge.

1. Scroll back through the Domino console, use Domino Message Tracking, or check log.nsf for router errors or messages addressed to the Bridge. For example, perhaps the Bridge server full computer name on the delivery location was entered incorrectly or that it could not be resolved to an IP address. Or if your organization has more than one Bridge, perhaps the wrong Bridge server full computer name was entered on the delivery location, in which case, the message was successfully sent to another Bridge.

    The following procedure briefly describes how to open log.nsf. Consult your Domino documentation for more information about log.nsf and about using Domino Message Tracking.

To Open Log.nsf to Look for Messages Addressed to the Bridge or for Router Errors

Step 1   Open the Domino Administrator on the applicable Domino server (or go to the applicable server within the Domino Administrator).

Step 2   Click the **Files** tab.

Step 3   In the list of files in the right pane, double-click **log.nsf**.

Step 4   In the left pane, click **Mail Routing Events**.

Step 5   In the pane in the right, scroll to the date and to the time the covers when the message was sent, and double-click the row. The Mail Routing Events window opens.

Step 6   The router will log a line similar to the following for messages that are successfully delivered to the Bridge:

04/22/2005 11:54:30 AM Router: Message 0067DBBC transferred to PARISBRIDGE2.EUROPE.CISCO.COM for 5234@parisbridge2.europe.cisco.com via SMTP

If the router could not resolve the Bridge server full computer name to an IP address, you should see an error like the following:

DNS: Non-existent domain

2.   Verify that the Bridge server full computer name is configured correctly, as follows:

    a.   In the Cisco Unity Administrator, go to the Bridge Delivery Location page for the applicable remote Octel server on the Cisco Unity bridgehead server.

    b.   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.

    c.   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.

3.   Verify that the Bridge server full computer name resolves to the IP address of the Bridge.

As a best practice, we recommend that you use Domain Name Service (DNS) for name resolution. If you are using DNS, confirm that there is a host address resource (A) record and a mail exchange (MX) record in DNS using the Bridge server full computer name and the IP address of the Bridge.

If using DNS is not an option, then confirm that there is an entry in the HOSTS file on the Domino server that handles outbound SMTP messages for your Domino network. (On servers running Microsoft Windows, the HOSTS file is located in the %windir%\System32\Drivers\Etc directory.)

    a.   In a command prompt window on the Bridge server, enter the command ping <Bridge Server Full Computer Name>.

    b.   If an IP address is returned, confirm that it is the IP address of the Bridge server.

If the returned response is Unknown host <Bridge Server Full Computer Name>, then correct the IP address in DNS or the HOSTS file, as applicable.

4.   Check to see if the message is stuck in MAIL.BOX on the Domino server used by the Interop Gateway for message delivery, or if the message is stuck in MAIL.BOX on any of the Domino servers that are involved in routing messages to the Domino server which sends outbound SMTP messages. Refer to your Domino documentation for more information.

5.   Confirm that Domino server(s) used for relaying messages outside of the organization is 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.

6.   If there is a firewall between the Bridge and the SMTP relay server, confirm that SMTP traffic is allowed on port 25.

7. Check to see whether e-mail leaving your Domino organization is re-routed to a smart host, non-Domino corporate SMTP relay server, secure e-mail server, or any other traffic filtering server that may not route SMTP messages to the Bridge server.

8. Go to the "After You Finish Troubleshooting" section on page 4-23 for details on how to reset the logs and traces to default values, and if you were unable to solve the problem, instructions are provided on how to gather the necessary logs to provide to Cisco TAC.

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 and on the Cisco Unity server on which the Interop Gateway service is running 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.)

- If you need to provide the Interop Gateway log file to Cisco TAC, do the "To Retrieve the Unity Diagnostic Tool Log File for the Interop Gateway" procedure on page 4-23 (which includes instructions for setting the traces back to the default).

  Otherwise, reset the traces for the Interop Gateway back to the default, as described in the "To Reset the Unity Diagnostic Tool to Default Traces" procedure on page 4-24.

To Retrieve the Unity Diagnostic Tool Log File for the Interop Gateway

Step 1   On the Windows Start menu on the Cisco Unity server on which the Interop Gateway service is running, click **Programs > Cisco Unity > Unity Diagnostic Tool**.

Step 2   On the Cisco Unity Diagnostic Tasks screen, click **Gather Log Files**. The Welcome to the Gather Log Files wizard is displayed.

Step 3   Click **Select Logs.**

Step 4   If desired, click **Browse** to change the directory for the log files.

Step 5   Click **Next**. The Select Logs to Gather page is displayed.

Step 6   Expand **CsDomInteropGty**, and click to select the check box for the last diagnostic file.

Step 7   Click **Next**. When the processing of the files is finished, the Completing the Gather Logs wizard page is displayed.

Step 8   Click **View Directory** to open a window of the directory.

Step 9   On the Completing the Gather Logs wizard page, click **Finish**.

Step 10   On the Cisco Unity Diagnostic Task page, click **Reset to Default Traces**.

Step 11   Click **Start New Log Files**.

Step 12   Exit the Cisco Unity Diagnostic tool.

**To Reset the Unity Diagnostic Tool to Default Traces**

Step 1   On the Windows Start menu on the Cisco Unity server on which the Interop Gateway service is running, click **Programs > Cisco Unity > Unity Diagnostic Tool**.

Step 2   On the Cisco Unity Diagnostic Task page, click **Reset to Default Traces**.

Step 3   Click **Start New Log Files**.

Step 4   Exit the Cisco Unity Diagnostic tool.

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 Interop Gateway mail file. The Interop Gateway converts the message to a WAV file and hands it back to Domino to be delivered to the Cisco Unity subscriber mail file. 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 4-3 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 4-3   *Troubleshooting Message Flow from Octel to Cisco Unity*
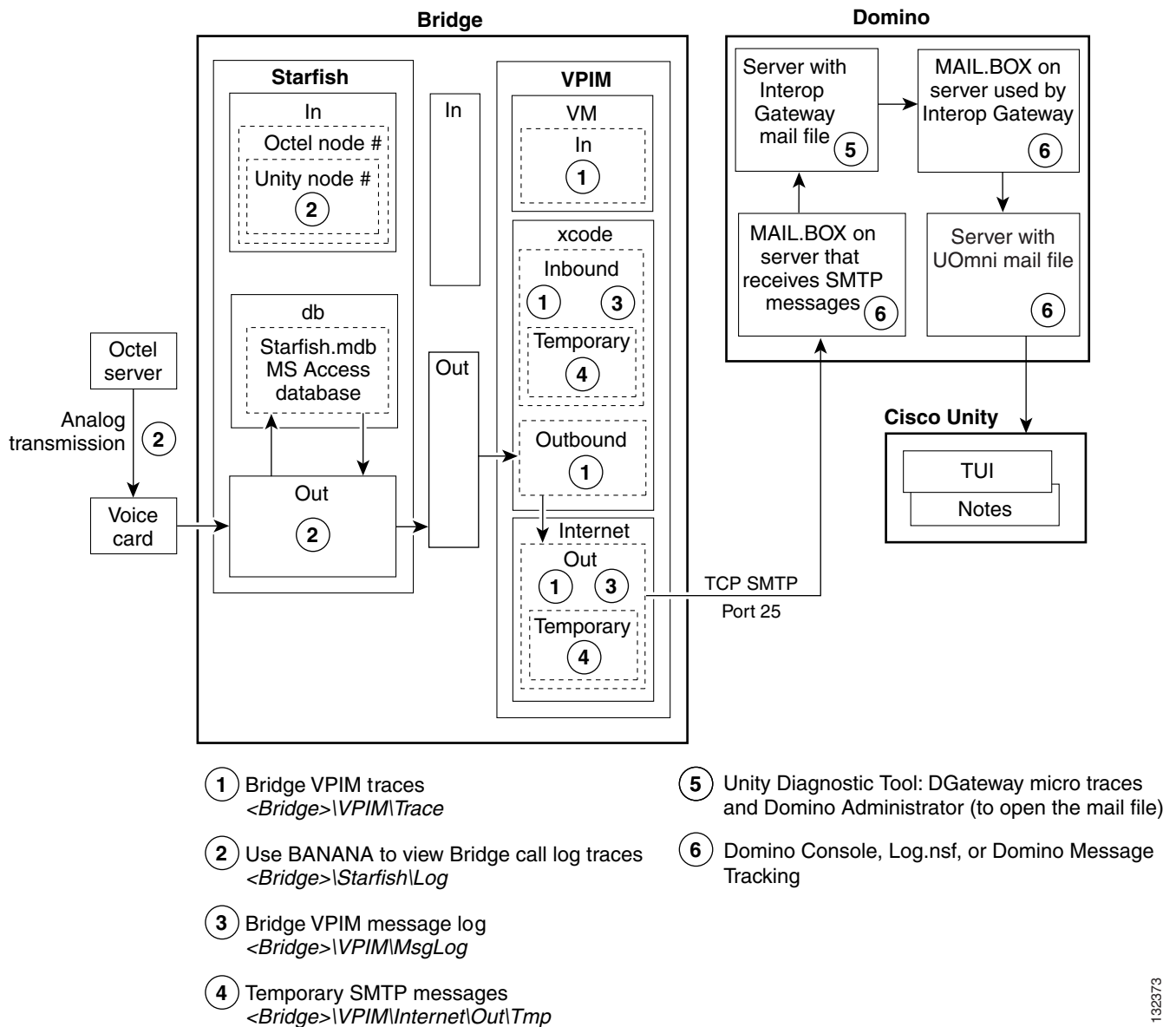
Bridge In and Out Directories

Note the Bridge\In and Bridge\Out directories in Figure 4-3.

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 Domino. If either service is stopped for some reason, messages will queue up as shown in the following table.

Table 4-3   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 MAIL.BOX on the Domino server that sends outgoing SMTP messages.	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 MAIL.BOX on the Domino server that sends outgoing SMTP messages.	Will queue up on the Octel servers.

Troubleshooting Why Messages Are Not Delivered from Octel to Cisco Unity

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

Figure 4-4   Troubleshooting Why Messages Are Not Delivered from Octel to Cisco Unity
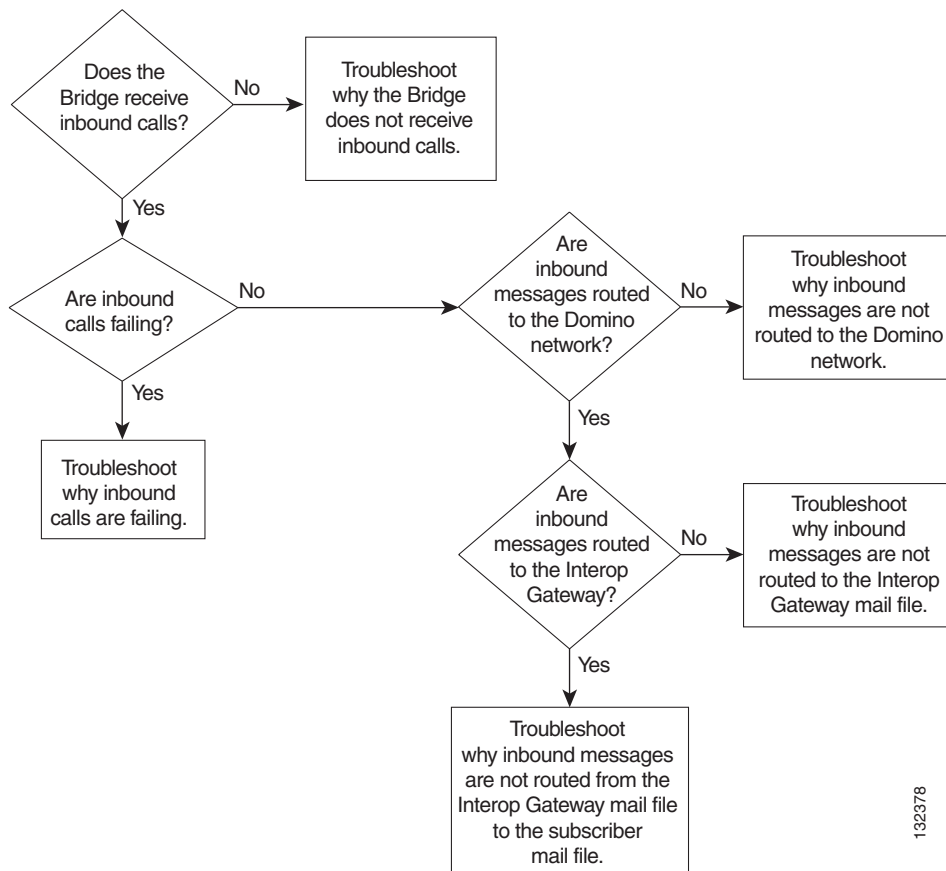
The following list provides an overview of the troubleshooting steps. Detailed procedures and troubleshooting steps follow the list.

1. Enable the various logs and traces as described in the "Enabling Logs and Traces" section on page 4-27.

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 4-30.

4. Are Inbound Calls Failing? If inbound calls are failing, see the "Troubleshooting Why Inbound Calls Are Failing" section on page 4-32.

5. Are Inbound Messages Routed to the Domino Network? If inbound messages are not routed to the Domino Network, see the "Troubleshooting Why Inbound Messages Are Not Routed to the Domino Network" section on page 4-37.

6. Are Inbound Messages Routed to the Interop Gateway Mail File? If inbound messages are not routed to the Interop Gateway mail file see the "Troubleshooting Why Inbound Messages Are Not Routed to the Interop Gateway Mail File" section on page 4-40.

   Otherwise, see the "Troubleshooting Why Inbound Messages Are Not Routed from the Interop Gateway Mail File to the Subscriber Mail File" section on page 4-40.

7. Reset the logs and traces as described in the "After You Finish Troubleshooting" section on page 4-41.

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 4-27
- To Enable Troubleshooting Logs and Traces on the Bridge Server, page 4-28
- To Set Diagnostic Traces, page 4-28

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**.
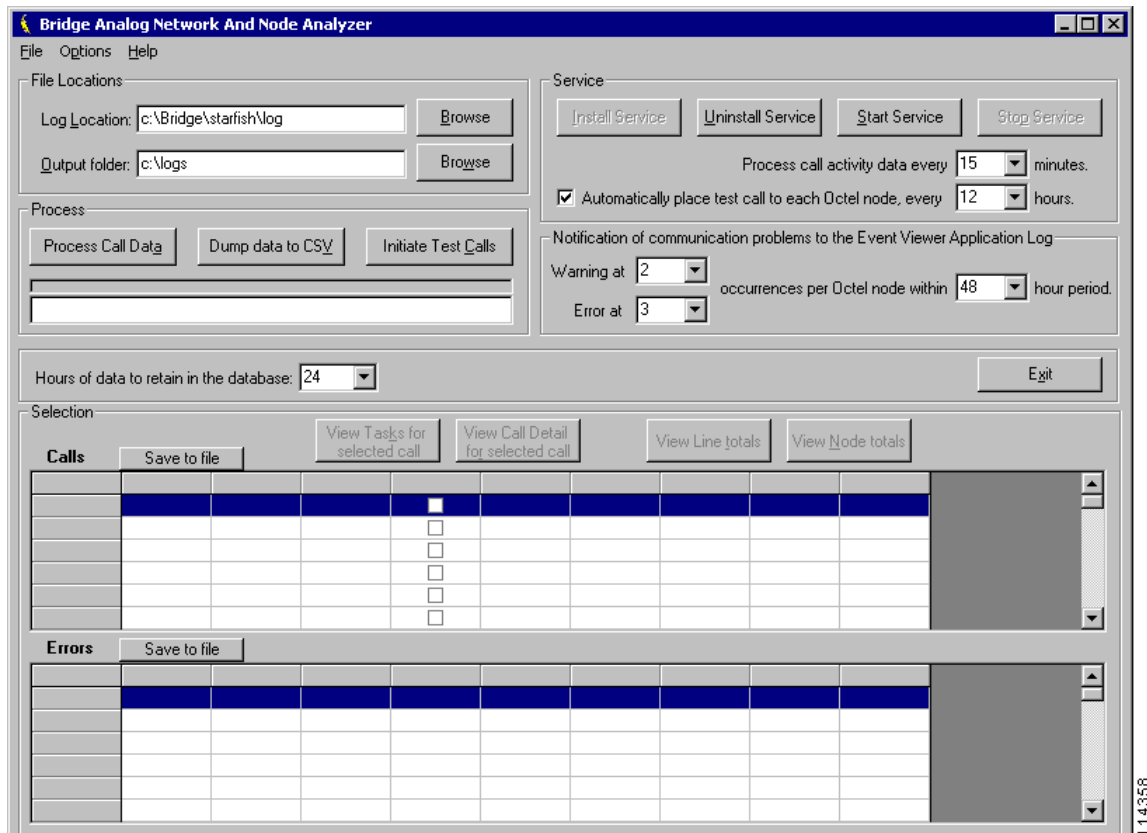
Step 5   Click **Save**.

To Set Diagnostic Traces

Step 1   On the Windows Start menu on the Cisco Unity server on which the Interop Gateway service is running (this may or may not be the bridgehead server), click **Programs > Cisco Unity > Unity Diagnostic Tool**.

Step 2   On the Cisco Unity Diagnostic Tasks screen, click **Configure Micros Traces**. The Welcome to the Configure Micro Traces wizard is displayed.

Step 3   Click **Next**. The Configure Micro Traces page is displayed.

Step 4   Scroll down and enable the following micro traces:

- DGateway
- MALLn
- NoteCommon

Step 5   Click **Next** and then click **Finish**.

Step 6   On the Cisco Unity Diagnostic Tasks screen, click **Start New Log Files**.
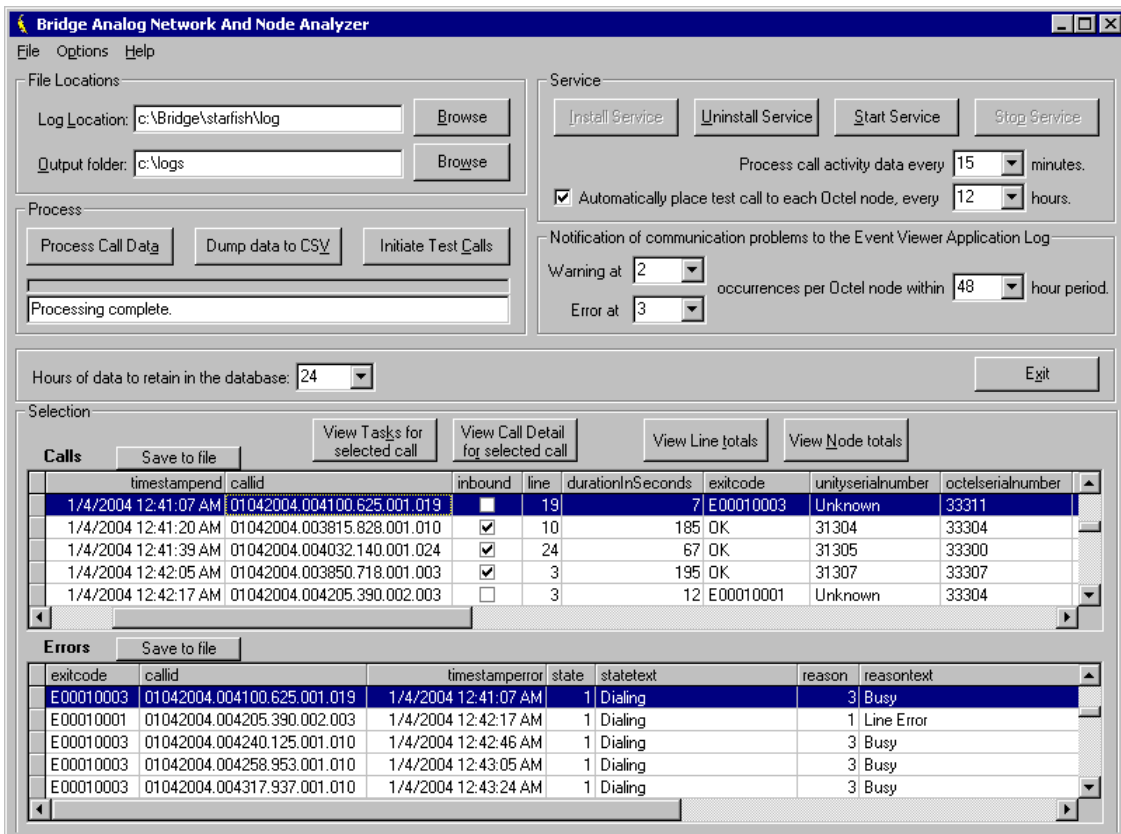
Does the Bridge Receive Inbound Calls?

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.

    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 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 4-30.

Otherwise, go to the "Are Inbound Calls Failing?" section on page 4-31.

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 3-1 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.

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 4-32.

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

Error Code	Description

E00020005	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:
	
	• 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:
	
	    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.
	
	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.
	
	Also verify that:
	
	• The Octel server(s) are supported. The only supported Octel servers are those listed in "Supported Voice Messaging Systems" section of the *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 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	Verify that: • The Octel server(s) are supported. The only supported Octel servers are those listed in "Supported Voice Messaging Systems" section of the *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 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 4-4   ***Configuration and Other Problems That Result in Inbound Call Failures (continued)***

Error Code	Description
E00020014	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: 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. 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.

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

Error Code	Description
E00040013	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.
	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.
	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.
	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>

	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.
	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:
	starfish -p <packet1> <packet2>
	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.
	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:

Cisco Unity Bridge 3.0 Networking Guide (With IBM Lotus Domino)

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

Error Code	Description
| E00040013, continued | C:\Bridge\Starfish\Bin>Starfish -p 12#*2*C#110B#88D95 12*#**72110B#88D95<br><br>Please wait while running Packet Prediction...<br><br>```
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
```<br><br>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. |
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	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. 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.

Are Inbound Messages Routed to the Domino Network?

If the server that receives incoming SMTP messages is a Domino server, you can open log.nsf in the Domino Administrator, or use Domino Message Tracking to see if the incoming SMTP message was received.

If your organization uses a non-Domino server as an ESMTP e-mail host that acts as a relay server, ask the network administrator if there is a message tracking function or log on the server. Also find out which Domino server (or servers) the ESMTP e-mail host routes inbound messages to, so that you can check log.nsf (or Domino Message Tracking) to see if the Domino server (or servers) received the message.

The following procedure briefly describes how to open log.nsf to look for a message addressed to the Foreign domain used by the Interop Gateway. Consult your Domino documentation for more information about log.nsf or about using Domino Message Tracking.

To Open Log.nsf to Look for a Message Addressed to the Interop Gateway Foreign Domain

Step 1   Open the Domino Administrator on the applicable Domino server (or go to the applicable server within the Domino Administrator).

Step 2   Click the **Files** tab.

Step 3   In the list of files in the right pane, double-click **log.nsf**.

Step 4   In the left pane, click **Mail Routing Events**.

Step 5   In the pane in the right, scroll to the date and to the time the covers when the message was sent, and double-click the row. The Mail Routing Events window opens.

Step 6   Search for a line similar to the following:

4/21/2005 03:18:22 AM Router: Message 00389ADF transferred to <DominoServer>/<DominoOrg> for IMCEAOMNI-AvVoiceAddress@<ForeignDomainName> via Notes

All messages sent from the Bridge will be addressed to the Interop Gateway as follows: IMCEAOMNI-AvVoiceAddress@<ForeignDomainName>

where <ForeignDomainName> is the Foreign domain name that is used by the Interop Gateway.

Step 7   If you do not see a message addressed to the Interop Gateway Foreign domain, go to the "Troubleshooting Why Inbound Messages Are Not Routed to the Domino Network" section on page 4-37.

If you have determined that the message was received, then go to the "Are Inbound Messages Routed to the Interop Gateway Mail File?" section on page 4-39.

Troubleshooting Why Inbound Messages Are Not Routed to the Domino Network

1.   On the Bridge server, check the <BridgePath>\VPIM\Internet\Out\Tmp directory to confirm that the Bridge sent the message.

After the Bridge successfully receives a message from an Octel, the message is converted to the proprietary VPIM format, and it is routed to the <BridgePath>\VPIM\Internet\Out directory on the Bridge server. The message will wait there for a minute or less, and then it is sent out from the Bridge via SMTP. If you have set the Retention Days for Temporary SMTP Messages setting on the Digital Networking page to a value greater than 0, a copy of the message is saved to the <BridgePath>\VPIM\Internet\Out\Tmp directory when the Bridge sends it out via SMTP.

In Cisco Unity Bridge 3.0(5) and later, messages that the Bridge could not deliver are stored in <BridgePath>\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.

2. Using Notepad, open the message in the <BridgePath>\VPIM\Internet\Out\Tmp (or the Failed directory if the message could not be delivered) to see the domain name that is used in the "To" address.

The proprietary VPIM messages are text files, and they can be opened with Notepad so that you can view the information in the message header. The message header contains the "To" address, which may help you determine why the message was not delivered to your Domino network. For example:

> Date: Mon, 26 Jul 2004 16:07:56 -0700
> From: 705@ParisBridge10.europe.cisco.com
> FromSN: 16882
> To: IMCEAOMNI-AvVoiceMessage@voicemail.europe.cisco.com
> X-AVT-TO: 1001@UnityBridgeheadServer3
> X-Bridge-Ports: 4
> ToSN: 12345
> MIME-Version: 1.0 (Voice 2.0)
> Content-Type: multipart/Voice-Message;

The "To" address in the above example is:
IMCEAOMNI-AvVoiceMessage@voicemail.europe.cisco.com

The portion of the "To" address after the "@" symbol must exactly match the Foreign domain name used by the Interop Gateway. So in the above example, "voicemail.europe.com" is the Interop Gateway Foreign domain name. The Bridge uses the name that was entered on the Unity SMTP Mail Suffix field of the applicable Unity Node when it constructs the "To" address of the SMTP messages destined for Cisco Unity.

Compare the domain name in the "To" address to the name in the Foreign domain document on the Domino server on which the Interop Gateway mail file is located. If the domain name in the "To" address does not exactly match the Interop Gateway Foreign domain name, correct the problem on the Bridge. In the Bridge Administrator, go to the Unity Node whose serial number matches the number in the "ToSN" portion of the message header, and enter the Interop Gateway Foreign domain name in the Unity SMTP Mail Suffix field.

3. Check if there is a value in the ESMTP Server field on the Digital Networking page in the Bridge Administrator. (Note that as a best practice, we recommend that you do not enter a value in the ESMTP Server field.)

If there is an address in ESMTP Server field on the Digital Networking page, that address is used by the Bridge when it establishes a network connection to the SMTP server that it sends the messages to. If the ESMTP Server field is empty, the domain name in the "To" address of the message is used by the Bridge when it establishes a network connection, which means that the domain name must resolve to the IP address of a server that accepts incoming SMTP messages to your Domino network.

As a best practice, we recommend that you leave the ESMTP Server field blank and use Domain Name Service (DNS) for name resolution. If you are using DNS, confirm that there is a host address resource (A) record and a mail exchange (MX) record in DNS using the Interop Gateway Foreign domain name and the IP address of the server that handles incoming SMTP messages.

If using DNS is not an option, then confirm that there is an entry in the HOSTS file on the Bridge server to resolve the Interop Gateway Foreign domain name to the IP address of a server that handles incoming SMTP messages for your Domino network. (The HOSTS file is located in the %windir%\System32\Drivers\Etc directory.)

4. Verify that the address that the Bridge uses to establish a network connection is to a server that accepts incoming SMTP messages for your Domino organization. Depending on your network configuration, this could be a Domino server with the SMTP Listener task enabled, or an ESMTP e-mail host that acts as a relay server, which then routes the messages to a Domino server(s).

   a. In a command prompt window on the Bridge server, enter the command **ping <Foreign Domain Name>**, where <Foreign Domain Name> is the Interop Gateway Foreign domain name.

   b. If an IP address is returned, confirm that it is the IP address of a server that accepts incoming SMTP messages to your Domino network.

   If the returned response is **Unknown host <Foreign Domain Name>**, then correct the IP address in DNS or the HOSTS file, as applicable.

5. Verify SMTP Connectivity as follows:

   a. Open a command prompt window on the Bridge server.

   b. Enter **telnet <Address> <Port>**. In this command:

   <Address> is the address that you entered in the ESMTP Server field on the Digital Networking page, or if you did not enter an address in the ESMTP Server field, <Address> is the address that you entered in the Unity SMTP Mail Suffix field on the Unity Nodes page.

   <Port> is the number from the SMTP Port field on the Digital Networking page. The default value is 25.

   You should see a response similar to the following:

   220 server1.mail.companya.com ESMTP Service (Lotus Domino Release 6.5)
   ready at Thu, 27 Jan 2005 17:59:44 -0800

   The response should be from the fully qualified domain name of the responding SMTP server (in the above example, "server1.mail.companya.com").

   c. If the test is successful, enter **quit** to end the telnet session.

   If the test fails, this may indicate a problem with the port. There could be a firewall blocking the port, or the SMTP server is not using the port. Check the settings on the destination SMTP server, and if needed, change the SMTP Port number that is specified on the Digital Networking page in the Bridge Administrator.

Are Inbound Messages Routed to the Interop Gateway Mail File?

If you have determined that messages from the Bridge were received by the server that handles incoming SMTP messages, do the following procedure to determine if messages from the Bridge get routed to the Interop Gateway Mail File.

To Determine Whether Messages Are Routed to the Interop Gateway Mail File

Step 1 On the Cisco Unity server on which the Interop Gateway service is running, open the Services MMC. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 2 Right-click **CsDomInteropGty**, and click **Stop**.

Step 3 Send a test message to a Cisco Unity subscriber from an Octel subscriber. Because the Interop Gateway service has been stopped, if the message arrives at the Interop Gateway mail file, the message will remain there until the service is started.

Step 4 Use the Domino Administrator or Notes to open the Interop Gateway mail file to see if the message is there.

In order to use the Domino Administrator or Notes to access the Interop Gateway mail file, you will need to verify that you have permission to do so. How you do this depends on the Domino version and security policies for your organization. Use the following as a guide, and consult your Domino documentation for more information:

If the Domino server on which the Interop Gateway mail file is located is running Domino 6.0 or later:

- If you have Full Access Administration rights, you will be able to open the mail file.
- If someone who has Full Access Administration rights is available, have the administrator add you to the Interop Gateway mail file Access Control List (ACL) with at least Editor permissions.

If the Domino server on which the Interop Gateway mail file is located is running Domino 5.x, or if someone with Full Access Administration rights is unavailable:

- Log on to the Domino Administrator by using the name and password of the Person document that was created for the Cisco Unity server on which the Interop Gateway service was configured to run. This account should have Editor plus Delete Documents permissions in the ACL of the Interop Gateway mail file.

  You can either use this account whenever you open the Interop Gateway mail file, or you can add yourself to the Interop Gateway mail file ACL with at least Editor permissions.

Step 5 After seeing whether the message is in the mail file, close it.

Step 6 On the Cisco Unity server, restart the Interop Gateway service, **CsDomInteropGty**, and close the Services MMC.

If the message was in the Interop Gateway mail file, go to the "Troubleshooting Why Inbound Messages Are Not Routed from the Interop Gateway Mail File to the Subscriber Mail File" section on page 4-40

If the message was not in the Interop Gateway mail file, go to the "Troubleshooting Why Inbound Messages Are Not Routed to the Interop Gateway Mail File" section on page 4-40.

Troubleshooting Why Inbound Messages Are Not Routed from the Interop Gateway Mail File to the Subscriber Mail File

1. Open log.nsf or use Domino Message Tracking to see if any routing errors are reported.

2. Verify that the applicable Connection documents are in place so that the Domino server on which the Interop Gateway mail file is located can route messages to the Domino server on which the subscriber mail file is located.

3. Check to see if the message is stuck in MAIL.BOX on the Domino server used by the Interop Gateway for message delivery, or if the message is stuck in MAIL.BOX on any of the Domino servers that are involved in routing messages to the Domino server on which the subscriber mail file is located. Refer to your Domino documentation for more information.

4. Check to see if there is a quota on the subscriber mail file and if Domino is configured to not deliver messages to mail files that are over quota.

Troubleshooting Why Inbound Messages Are Not Routed to the Interop Gateway Mail File

1. Open log.nsf or use Domino Message Tracking to see if any routing errors are reported.

2. Check to see whether, after entering the SMTP server, e-mail entering your organization is re-routed to a smart host, non-Domino corporate SMTP relay server, secure e-mail server, or any other traffic filtering server that may not route incoming SMTP messages to Domino.

3. Verify that the applicable Connection documents are in place so that the Domino server that receives incoming SMTP messages can route messages to the Domino server on which the Interop Gateway mail file is located.

4. Check to see if the message is stuck in MAIL.BOX on any of the Domino servers that are involved in routing messages to the Domino server on which the Interop Gateway mail file is located. Refer to your Domino documentation for more information.

5. If a Domino server is used for routing incoming SMTP messages from the Bridge, verify that the SMTP Listener is enabled.

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 and on the Cisco Unity server on which the Interop Gateway service is running 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.)

- If you need to provide the Interop Gateway log file to Cisco TAC, do the "To Retrieve the Unity Diagnostic Tool Log File for the Interop Gateway" procedure on page 4-41 (which includes instructions for setting the traces back to the default).

  Otherwise, reset the traces for the Interop Gateway back to the default, as described in the "To Reset the Unity Diagnostic Tool to Default Traces" procedure on page 4-42.

To Retrieve the Unity Diagnostic Tool Log File for the Interop Gateway

Step 1   On the Windows Start menu on the Cisco Unity server on which the Interop Gateway service is running, click **Programs > Cisco Unity > Unity Diagnostic Tool**.

Step 2   On the Cisco Unity Diagnostic Tasks screen, click **Gather Log Files**. The Welcome to the Gather Log Files wizard is displayed.

Step 3   Click **Select Logs.**

Step 4   If desired, click **Browse** to change the directory for the log files.

Step 5   Click **Next**. The Select Logs to Gather page is displayed.

Step 6   Expand **CsDomInteropGty**, and click to select the check box for the last diagnostic file.

Step 7   Click **Next**. When the processing of the files is finished, the Completing the Gather Logs wizard page is displayed.

Step 8   Click **View Directory** to open a window of the directory.

Step 9   On the Completing the Gather Logs wizard page, click **Finish**.

Step 10   On the Cisco Unity Diagnostic Task page, click **Reset to Default Traces**.

Step 11   Click **Start New Log Files**.

Step 12   Exit the Cisco Unity Diagnostic tool.

To Reset the Unity Diagnostic Tool to Default Traces

Step 1   On the Windows Start menu on the Cisco Unity server on which the Interop Gateway service is running, click **Programs > Cisco Unity > Unity Diagnostic Tool**.

Step 2   On the Cisco Unity Diagnostic Task page, click **Reset to Default Traces**.

Step 3   Click **Start New Log Files**.

Step 4   Exit the Cisco Unity Diagnostic tool.

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 4-5 and Figure 4-6 illustrate, the trouble spots are similar. However, if you do encounter a problem with directory messages, see the "CsBridgeConnector Traces" section on page 4-44 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 4-45
- Full Synchronization of Cisco Unity Subscribers with the Unity Node Directories, page 4-46

Figure 4-5   *Troubleshooting Problems with Directory Messages from Cisco Unity to the Bridge*

#		#	
1	Bridge VPIM traces *<Bridge>\VPIM\Trace*	**5**	Unity Diagnostic Tool: DGateway micro traces and Domino Administrator (to open mail file)
2	Use BANANA to view Bridge call log traces *<Bridge>\Starfish\Log*	**6**	Domino Console, Log.nsf, or Domino Message Tracking
3	Bridge VPIM message log *<Bridge>\VPIM\MsgLog*	**7**	Unity Diagnostic Tool: CsBridgeConnector traces
4	Temporary SMTP messages *<Bridge>\VPIM\Xcode\Inbound\Tmp*	**8**	Sent/received vCard data

132374

Figure 4-6   ***Troubleshooting Problems with Directory Messages from the Bridge to Cisco Unity***

① Bridge VPIM traces
    <Bridge>\VPIM\Trace

② Use BANANA to view Bridge call log traces
    <Bridge>\Starfish\Log

③ Bridge VPIM message log
    <Bridge>\VPIM\MsgLog

④ Temporary SMTP messages
    <Bridge>\VPIM\Xcode\Inbound\Tmp

⑤ Unity Diagnostic Tool: DGateway micro traces
    and Domino Administrator (to open mail file)

⑥ Domino Console, Log.nsf, or Domino Message
    Tracking

⑦ Unity Diagnostic Tool: CsBridgeConnector traces

⑧ Sent/received vCard data

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 4-46—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 4-46—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.