Setting Up Cisco Unity and the Bridge for Networking

In this chapter, you will find a task list and procedures for setting up Bridge Networking for the first time.

If you are unfamiliar with Bridge Networking, you should first read the "About Bridge Networking" chapter and then review this chapter before beginning the setup. Planning is essential to a successful setup.

Prerequisites

Before starting the setup, verify that the following prerequisites have been met. (Detailed information about the prerequisites can be found in the "Overview of Mandatory Tasks for Installing the Cisco Unity Bridge" chapter of the *Cisco Unity Bridge Installation Guide*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/big/dom/index.htm.)

- System and networking requirements for the Bridge have been met. In particular, the Cisco Unity server(s) must be at Cisco Unity 4.0(5) or later.
- The required hardware and software have been installed on the Bridge server.
- A license file has been obtained and installed on the Bridge server.
- The Bridge server has been connected to the phone system, and a hunt group has been created on the phone system for the analog extensions used for the Bridge.

The starting point for the task lists assumes that Cisco Unity has been installed on the bridgehead server as described in the applicable *Cisco Unity Installation Guide*, available at: http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

For Installations with Multiple Cisco Unity Servers Networked Together

For installations with multiple Cisco Unity servers networked together, you should first set up the servers for Digital Networking as described in the "Digital Networking" chapter of the applicable *Networking in Cisco Unity Guide*. Note that in order to use Bridge Networking, all of the networked Cisco Unity servers must be at version 4.0(5) or later.

After the Cisco Unity servers have been set up for Digital Networking, verify the following settings before starting the Bridge Networking setup:

- Verify that the addressing search scope is set to either the dialing domain or the global scope on all the networked servers, so that Cisco Unity subscribers, no matter which server they are associated with, can address messages to Bridge delivery locations and/or Bridge subscribers. Refer to the "Setting the Addressing Search Scope" section in the "Digital Networking" chapter.

- If you want outside callers to be able to reach Bridge subscribers from the automated attendant (for example, from the opening greeting) or directory assistance:
  - Verify that the Cisco Unity server(s) on which the Bridge subscribers will be created are in the same dialing domain as the Cisco Unity server that outside callers call into. Refer to the "Dialing Domains" and "Customizing the Primary Location" sections in the "Digital Networking" chapter.
  - Verify that the automated attendant and directory handler(s) search scopes are set to the dialing domain scope. Refer to the "Setting the Directory Handler Search Scope" and the "Setting the Automated Attendant Search Scope" sections in the "Digital Networking" chapter.

Note The *Networking in Cisco Unity Guide* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Task List: Setting Up Cisco Unity and the Bridge for Networking

Use this task list to set up networking between Cisco Unity and the Bridge for the first time. The cross-references take you to detailed procedures related to each item in the list.

Make Design Decisions

1. Make decisions about your Cisco Unity numbering plan, and gather information needed to configure Cisco Unity and the Bridge for networking. See the "Making Design Decisions and Gathering Needed Information" section on page 2-4.

Prepare the Network

2. Make changes as needed to provide basic network connectivity between the Bridge server and the server(s) that route incoming and outgoing SMTP messages to and from your Domino network. See the "Resolving Names and IP Addresses" section on page 2-6.
3. Configure the Interop Gateway. See the "Configuring the Interop Gateway" section on page 2-7.

Configure the Cisco Unity Server Designated as the Bridgehead

4. Run ConfigMgr.exe to enable and create components necessary for the server to function as the bridgehead server. See the "Designating the Bridgehead Server" section on page 2-9.
5. Set Bridge options. See the "Setting Bridge Options" section on page 2-10.
6. Configure the subscriber template that will be used for the auto-creation of Bridge Subscribers. See the "Configuring the Subscriber Template That Will Be Used for Auto-Created Bridge Subscribers" section on page 2-10.
7. Create Bridge delivery location(s). See the "Creating and Configuring Bridge Delivery Locations" section on page 2-11.

Create New or Modify Existing Subscriber Accounts for Testing Purposes

8. Create a few new subscriber accounts (or modify a few existing Cisco Unity subscriber accounts) for testing purposes. See the "Creating New or Modifying Existing Subscriber Accounts for Testing Purposes" section on page 2-14.

Configure the Bridge Server

9. Configure settings on the Bridge server, and test the configuration. See the "Configuring the Bridge and Testing the Configuration" section on page 2-15.

Configure the Octel Servers

10. Configure the Octel servers. See the "Configuring the Octel Servers" section on page 2-22 for some high-level information (refer to the Octel product documentation for details).

Test the Setup

11. Test the Octel analog network to verify that the Bridge can communicate with each of the configured Octel nodes. See the "Testing the Octel Analog Network" section on page 2-22.
12. Test the complete setup to verify that Cisco Unity can exchange voice and directory messages with the Octels. See the "Testing the Setup" section on page 2-24.

    If you are unable to send and receive messages, see the "Troubleshooting Bridge Networking" chapter for information that can help you find and fix the problem.

Finish the Setup

13. If you have not already done so, create a delivery location for each Octel node with which Cisco Unity will communicate. See the "Finishing the Creation and Configuration of Bridge Delivery Locations" section on page 2-25.
14. As applicable, add the legacy serial number and mailbox ID to each existing Cisco Unity subscriber account, or create new Cisco Unity subscribers with the serial and mailbox numbers. See the "Adding the Serial Number and Mailbox ID to Cisco Unity Subscriber Accounts" section on page 2-25.
15. Configure the serial number and mailbox number to be used for messages from unidentified callers. See the "Setting the Serial Number and Mailbox ID for Unidentified Callers" section on page 2-27.
16. Optionally, create Bridge subscribers on the Cisco Unity server designated as the bridgehead. See the "Creating Bridge Subscriber Accounts" section on page 2-27.

Enable Optional Features

17. Optionally, extend identified subscriber messaging to include Bridge subscribers. See the "Extending Identified Subscriber Messaging to Include Bridge Subscribers" section on page 2-36.
18. Optionally, enable the Bridge server to send delivery receipts to Cisco Unity subscribers when the extended-absence greeting for an Octel subscriber is enabled and the mailbox is accepting messages. See the "Enabling the Bridge Server to Send Extended-Absence Delivery Receipts" section on page 2-39.
19. Optionally, if the Bridge server is at version 3.0(6) or later, enable the Bridge server to accept requests to push remote mailbox information. See the "Enabling the Bridge to Accept Requests to Push Mailbox Information (Bridge 3.0(6) and Later)" section on page 2-40.

Monitor Message Traffic Flow and Adjust Settings

20. After Cisco Unity and the Bridge are configured, and messaging between Cisco Unity and Octel subscribers is working correctly, see the "Monitoring and Maintaining Bridge Networking" chapter for information on monitoring message traffic flow, and for tips on adjusting settings that control the number of ports on the Bridge server that will be used for calls to the Octel nodes.

Making Design Decisions and Gathering Needed Information

Before you begin setting up Cisco Unity and the Bridge for networking, be sure to gather the appropriate information. Following is a check list of the information that you will need. For detailed information on planning a migration, refer to the *Cisco Unity Bridge Design Guide*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/design/bdg/index.htm.

- Develop a migration strategy to determine whether the Octel servers will require reprogramming.
- Determine the placement and number of Bridge servers.
- Review your numbering plan strategy to determine:
  - Dial IDs on primary location(s)
  - Dial IDs on Bridge delivery location(s)
  - Prefixes on Bridge delivery location(s)
  - Remote mailbox lengths on Bridge delivery location(s)
  - Serial numbers and mailbox numbers for Cisco Unity subscribers migrating from Octel, or for existing Cisco Unity subscribers
  - Primary and alternate extensions for Cisco Unity subscribers
  - Primary and alternate extensions for Bridge subscribers
- Decide whether you want Bridge subscribers to be created automatically on a usage basis, or whether you want to create Bridge subscribers manually before subscribers begin using the system.
- Write down the fully qualified domain name (FQDN) and IP address of the Bridge server(s).
- Determine the Interop Gateway foreign domain name, and write it down.
- Determine the server(s) that will handle outgoing SMTP messages to the Bridge. Depending on your network, this could be a Domino server or another server configured to relay SMTP messages to addresses outside of your Domino network.
- Determine the Domino server on which the Interop Gateway mail file will be located. Verify that the server can route messages to the server that sends outgoing SMTP messages. Also verify that the server on which the Interop Gateway mail file is located can route messages to all Domino servers that contain Cisco Unity subscriber mail files, and that all those servers can route messages to the server on which the Interop Gateway mail file will be located.
- Write down the IP address of the server(s) that will accept incoming SMTP messages from the Bridge. Depending on your network, this could be a Domino server or another server configured to relay SMTP messages to your Domino network. Note that the IP address is paired with the Interop Gateway foreign domain name for name resolution. Verify that the SMTP Listener task is enabled on the server, and that the server can route messages to the Domino server on which the Interop Gateway mail file will be located.
- Decide which Cisco Unity server will be designated the bridgehead server.
- Write down the name, serial number, and phone number for each Octel node.
- Review the following pages on the Cisco Unity Administrator. You may want to make note of the information that you will need to enter on the pages.
  - Primary Locations > Profile
  - Primary Location > Addressing Options
  - Call Management > Directory Handler > Search Options
  - Bridge Delivery Location > Profile

  - Bridge Delivery Location > Prefixes
  - Bridge Delivery Location > Subscriber Creation Options
  - Bridge Options > Subscriber Creation Options
  - Bridge Options > Unknown Caller
  - Subscriber Template settings, Subscriber COS settings, and Subscriber settings (for Cisco Unity subscribers, Bridge subscribers, and auto-created Bridge subscribers)
- Review the following pages on the Bridge Administrator. You may want to make note of the information you will need to enter on the pages.
  - System Settings
  - Digital Networking
  - Unity Nodes
  - Octel Nodes

Determining the Domain Name

In order for messages to be exchanged between the Bridge and Cisco Unity, the same domain name (for example "voice@domain.com") will need to be configured, as follows:

- On the Unity node profile on the Bridge server.
- On the SMTP Domain Name field on the Network > Primary Location page in the Cisco Unity Administrator.
- As the foreign domain name in the Interop Gateway Configuration wizard. See the "Choosing the Interop Gateway Foreign Domain Name" section on page 1-15.

Consult with the Domino administrator for your organization to determine an appropriate domain name to use.

Optional: Gathering or Confirming Octel Node Serial Numbers (Bridge 3.0(6) or Later)

After the Bridge server is connected to the phone system, you can use the GetSN command-line utility to retrieve or confirm the serial number of a remote Octel node. The utility makes a call to the phone number that you provide and attempts to retrieve the serial number of the remote node. To collect multiple serial numbers, you can run the utility as part of a batch file.

Retrieving an Octel Node Serial Number by Using GetSN

Step 1 On the Bridge server, stop the Unity Bridge service if it is running.

Step 2 Open a command prompt window.

Step 3 Set the working drive to that on which the Bridge software is installed.

Step 4 Enter **cd \bridge\starfish\bin** to change to the directory where GetSN.exe is located.

Step 5 Run GetSN with the following command line:

GetSN <Phone Number>

Commas can be used in the dial string to specify a pause. For example, to dial a 9 and then pause before dialing the number 5552900, enter:

GetSN 9,5552900

The resulting output includes the call trace as well as the serial number, if it can be determined from the call.

Step 6 Restart the Unity Bridge service.

Preparing the Network

Resolving Names and IP Addresses

The Bridge server and the Domino (or relay) servers that handle incoming and outgoing SMTP messages require some mechanism for name resolution. While any method or combination of methods may be used, two common ways to accomplish name resolution are through Domain Name System (DNS), and by using HOSTS files.

Whether you use DNS or HOSTS files, you will need to know the fully qualified domain name (FQDN) and IP address of the Bridge server. The FQDN is displayed in the Windows System Control Panel on the Network Identification tab in the Full Computer Name field. You will also need to know the Interop Gateway foreign domain name and the IP address of the Domino (or relay) server that handles incoming SMTP messages.

If your organization uses DNS:

- Add a host address resource (A) record and a mail exchange (MX) record in DNS for the Bridge server.
- Add an MX record in DNS using the Interop Gateway foreign domain name and the IP address of the Domino (or relay) server that handles incoming SMTP messages.

Refer to the Microsoft Windows or applicable operating system documentation for more information about adding A and MX records in DNS.

If your organization does not use DNS, you can use HOSTS files for name resolution. A HOSTS file is a text file that contains the mappings of IP addresses to host and domain names. On Microsoft Windows systems, the HOSTS file is located in the C:\WINNT\System32\Drivers\Etc directory. Edit the HOSTS files as follows:

- On the Domino (or relay) server that handles outgoing SMTP messages, add an entry to the HOSTS file with the FQDN and IP address of the Bridge server.
- On the Bridge server, add an entry to the HOSTS file with the Interop Gateway foreign domain name and the IP address of the Domino (or relay) server that handles incoming SMTP mail.

Additionally, verify that the server that handles incoming SMTP messages is able to route messages to the Domino server on which the Interop Gateway mail file will be located. Refer to your Domino documentation for more information.

Configuring the Interop Gateway

You can configure the Interop Gateway service—CsDomInteropGty—to run on the Cisco Unity bridgehead server, or on any other Cisco Unity server networked to the bridgehead via Digital Networking. Note the following:

- Although the Interop Gateway mail file can be located on a Domino server that belongs to a cluster, or you can specifically cluster the Interop Gateway mail file, the Interop Gateway monitors only the Domino server on which the mail file was created. If the Domino server on which the Interop Gateway mail file was created fails-over or is marked busy by the Domino Cluster Manager, the Interop Gateway does not monitor the replica of the mail file (which is on another Domino server in the cluster). Domino will route messages to the mail file replica, but the messages will not be processed by the Interop Gateway until the Domino server on which the mail file was created becomes active again.
- Configure the Interop Gateway only on one Cisco Unity server. Configuring multiple Interop Gateways is not supported.

Caution The mail file used by the Interop Gateway can become quite large. We recommend that you monitor the mail file size and compact it as needed to prevent the mail file from consuming too much disk space. Refer to your Domino documentation for more information about compacting databases.

To Configure the Interop Gateway

Step 1 On the Cisco Unity server, browse to the directory in which Cisco Unity is installed (the default location is C:\CommServer).

Step 2 Double-click **UnityDominoInterOpSetup.exe** to run the Interop Gateway Configuration wizard.

Step 3 On the Welcome screen, click **Next**.

Step 4 On the Configure the Interop Gateway screen, click either **Use a New Foreign Domain** or **Use an Existing Foreign Domain**.

- If you choose to use a new Foreign domain, in the text box, enter the domain name that will be used to route Bridge messages to the Interop Gateway mail file. For example, if “domain.com” is the domain name for your organization, you can enter **voice.domain.com**. The Interop Gateway Configuration wizard creates a new Foreign domain document with the specified name.

Caution If you choose to use an existing Foreign domain, verify that the mail file for the Foreign domain was created using the Mail Router Mailbox (R6 or R5) template. Do not use a mail file for the Foreign domain that was created with the Mail (R6 or R5) template. Refer to your Domino documentation for information on creating Foreign domain documents and creating databases.

See the “Interop Gateway and Bridge Networking” section on page 1-15 for more information on choosing a Foreign domain name.

Caution Changing the foreign domain name after the Interop Gateway Configuration wizard has been run is an involved process. Be very careful when entering the foreign domain name or choosing one from the list. See the “Changing the Interop Gateway Foreign Domain Name” section on page 3-9 for more information.

- If you chose to use an existing Foreign domain, click the Foreign domain name on the list.

Note The Foreign domain name must be a unique domain name in your Domino network, and it must be used exclusively by the Interop Gateway.

Step 5 Click **Next** to go to the Foreign Domain Mail Information screen. If you chose to use an existing Foreign domain, the mail file name and the Domino server on which the mail file resides are displayed. Verify the information, and skip to Step 6.

If you chose to create a new Foreign domain:

a. Click the down button for the Domino Server list and wait for the list to be populated with all of the Domino server names in your network. Choose the server on which the Interop Gateway mail file will be created. Although you can type in the server name, you must enter the server name by using the hierarchical naming format (for example "ServerName/Org").

b. In the Mail File Name field, enter the name of the mail file to be monitored by the Interop Gateway (for example, interop.nsf). The Interop Gateway Configuration wizard will create the mail file, so enter a file name that does not already exist.

Step 6 Click **Next**. Choose the Windows account that the Interop Gateway service will log on with. We recommend that you choose Local System. However, if you choose an existing Windows account, you will need to ensure that it has the same level of permissions as were set by the Permissions wizard during Cisco Unity setup for the directory and messaging services account.

Step 7 Click **Next** and review the summary information to verify that it is correct.

Step 8 Click **Finish.** The wizard configures and starts the Interop Gateway service on the Cisco Unity server. When the wizard finishes, a message box displays to let you know whether the configuration was successful.

Note If the system is using the Cisco Unity failover feature, you must run the Interop Gateway Configuration wizard first on the primary server and then on the secondary server. When you have finished configuring Bridge Networking on the primary Cisco Unity server, run the Interop Gateway Configuration wizard on the secondary server, and be sure to use the same Foreign domain that you specified above. (You will choose to use an existing Foreign domain.)

To Verify the Interop Gateway Configuration

Do the following procedure to verify that the Interop Gateway is configured properly, that the Interop Gateway service is running, and that the foreign domain document and mail file have been created.

Step 1 Open the Services MMC on the Cisco Unity server on which you ran the Interop Gateway Configuration wizard. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 2 Verify that the Status for the CsDomInteropGty service is **Started**, and that the Startup Type is set to **Automatic**.

Step 3 Exit the Services MMC.

Step 4 Open the Domino Administrator.

Step 5 Click the **Configuration** tab.

Step 6 In the left pane, expand **Messaging**, and click **Domains**.

Step 7 Verify that there is a foreign domain document with the name that you specified in the Interop Gateway Configuration wizard.

Step 8 Open the foreign domain document.

Caution Do not change any information in the Foreign Domain document. Instead, rerun the Interop Gateway Configuration wizard if you need to change information in the document.

Step 9 Click the **Mail Information** tab, and verify that the Gateway server name and Gateway mail file name fields contain the correct information.

Step 10 Close the foreign domain document, and exit Domino Administrator.

Step 11 On the applicable Domino server, open **My Computer** and browse to the Domino directory to verify that the Interop Gateway mail file was created.

Configuring the Cisco Unity Server Designated as the Bridgehead

Designating the Bridgehead Server

In installations with multiple Cisco Unity servers networked together, one Cisco Unity server is designated the bridgehead server and is set up for networking with the Bridge. To designate a Cisco Unity server as a bridgehead server, you run the ConfigMgr.exe utility with the Create Bridge Account option. ConfigMgr.exe installs and configures components required by the bridgehead server, as follows:

- Configures the server to automatically start and stop the CsBridgeConnector service.
- Configures the UnityDb SQL database to track changes to Cisco Unity subscribers in the network so that the CsBridgeConnector service can process the changes and send them to the Bridge server(s).
- Creates the default Bridge Subscriber Template, which is used for auto-created Bridge Subscribers.
- Configures the Cisco Unity Administrator to allow the creation of Bridge delivery locations and Bridge subscribers.
- Configures the Cisco Unity Administrator to enable the link to the Network > Bridge Options pages.
- Creates the UOmni mail file where the Interop Gateway will deliver directory messages from the Bridge server for the CsBridgeConnector service to process. Note that the UOmni mail file is located on the Domino server that was selected in the Cisco Unity Server Message Store Configuration wizard during setup of the Cisco Unity bridgehead server.

To Designate the Bridgehead Server

Step 1 On the Cisco Unity server, browse to the directory in which Cisco Unity is installed (the default location is CommServer).

Step 2 Double-click **ConfigMgr.exe**. The ConfigMgr dialog box appears.

Step 3 Click **Create Bridge Account**.

Step 4 Click **OK** in the dialog box that displays after the configuration has completed.

Step 5 Close the ConfigMgr dialog box.

Setting Bridge Options

Set the Bridge options only on the Cisco Unity bridgehead server. For detailed information about the Bridge Option settings, see the "Bridge Options Subscriber Creation Settings" section on page 7-6.

To Set Bridge Options

Step 1 In the Cisco Unity Administrator, go to the **Network > Bridge Options > Subscriber Creation Options** page.

Step 2 Select the subscriber template that will be used for auto-created Bridge subscribers.

We recommend that you use the default {Bridge Subscriber} Template.

Step 3 As applicable, check or uncheck the check boxes that allow the automatic creation, deletion, and modification of Bridge subscriber objects based on directory information that is received from the Bridge.

If you are unsure about enabling this functionality, leave the check boxes checked; they can be changed later if necessary.

Do not synchronize the directories at this time because the Bridge server has not yet been configured.

Configuring the Subscriber Template That Will Be Used for Auto-Created Bridge Subscribers

To Configure the Subscriber Template That Will Be Used for Auto-Created Bridge Subscribers

Step 1 In the Cisco Unity Administrator, go to any **Subscribers > Subscriber Templates** page.

Step 2 Click the **Find** icon, and double-click the template selected in Step 2 of the "To Set Bridge Options" procedure on page 2-10.

Step 3 Review the settings on the template, and make changes as applicable.

Step 4 Click the **Save** icon.

Creating and Configuring Bridge Delivery Locations

Create a Bridge delivery location on the Cisco Unity bridgehead server for each Octel node with which Cisco Unity will communicate. If the Octel network has a large number of nodes, you may prefer to configure only a few delivery locations at this time and proceed with the rest of the setup. After verifying that messaging works correctly between Cisco Unity and the Octel nodes for which delivery locations have been configured, you can create the rest of the delivery locations.

Typically, there is a one-to-one correspondence of Bridge delivery locations and Octel nodes. However, it is possible (though rare) that an Octel server may be configured to have mailboxes with different lengths. In this case, you must create separate Bridge delivery locations that have the same Octel Node Serial Number but with a different number in the Remote Mailbox Length field.

If there are multiple Bridge servers, divide the delivery locations and corresponding Octel nodes among the Bridge servers. For example, on Bridge server 1 you create Octel nodes called New York and Boston, and on Bridge server 2 you create Octel nodes called London and Paris. On the Cisco Unity bridgehead server, you then create four delivery locations that correspond to the four Octel nodes. For the New York and Boston delivery locations, you enter the fully qualified domain name of Bridge server 1, and for the London and Paris delivery locations, you enter the fully qualified domain name of Bridge server 2.

For additional detailed information about the delivery location settings, see the following sections:

- Bridge Delivery Locations Profile Settings, page 7-1
- Bridge Delivery Locations Prefixes, page 7-4
- Bridge Delivery Locations Subscriber Creation Settings, page 7-5

You can create Bridge delivery locations by using the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard. See the following sections:

- Using the Cisco Unity Administrator to Create Bridge Delivery Locations, page 2-11
- Using the Cisco Unity Bulk Import Wizard to Create Bridge Delivery Locations, page 2-12

Using the Cisco Unity Administrator to Create Bridge Delivery Locations

You can create Bridge delivery locations one at a time by using the Cisco Unity Administrator.

To Create Bridge Delivery Locations by Using the Cisco Unity Administrator

Step 1 In the Cisco Unity Administrator, go to the **Network > Delivery Locations > Profile** page.

Step 2 Click the **Add** icon.

Step 3 Enter a meaningful name for the location.

Step 4 Enter the Dial ID. See the "Guidelines for Assigning Dial IDs and Extensions" section on page 9-2 for detailed information about choosing a Dial ID.

Step 5 Select **Bridge** as the Destination Type for the location.

Step 6 Enter the Octel Node Serial Number of the Octel server that corresponds to this Bridge delivery location. This number must match the Serial Number of one of the Octel Nodes configured on the Bridge server.

Step 7 Enter the Bridge Server Full Computer Name of the Bridge server that will be configured to send messages to and receive messages from the Octel server that corresponds to this Bridge delivery location.

To determine the fully qualified domain name of the Bridge server, do the following sub-steps:

a. On the Windows Start menu on the Bridge server, click **Settings > Control Panel**.

b. Double-click **System**.

c. Click the **Network Identification** tab. The fully qualified domain name of the Bridge server is listed on this tab as the Full Computer Name.

Step 8 Enter a value for the Remote Mailbox Length. This should be the length of the subscriber mailboxes on the remote Octel server that corresponds to this Bridge delivery location.

Step 9 Click **Add**.

Step 10 Record a voice name for the location.

Step 11 Optionally, go the **Delivery Location > Prefixes** page and enter prefixes as needed.

Step 12 Go to the **Delivery Location > Subscriber Creation** page, and configure settings for auto-created Bridge subscribers that are associated with the delivery location.

Using the Cisco Unity Bulk Import Wizard to Create Bridge Delivery Locations

The Cisco Unity Bulk Import wizard allows you to create or modify multiple delivery locations at once by importing data in a CSV file. If you have already created delivery locations, you can run Cisco Unity Bulk Import to export the data about the delivery locations to a CSV file.

Use the following procedure to prepare your CSV file. To learn more about preparing a CSV file for use with the Cisco Unity Bulk Import wizard—including information on the required and optional column headers for your CSV file—refer to the Cisco Unity Bulk Import wizard Help.

To Prepare a CSV File for Creating Bridge Delivery Locations

Step 1 Create a CSV file in a spreadsheet application (or another applicable application) on the Cisco Unity server, or in a directory that you can browse to from the server.

Step 2 Enter the required column headers in the first row. Column headers must be in uppercase, separated by commas, and spelled as indicated below:

DTMF_ACCESS_ID, DISPLAY_NAME, BRIDGE_SERVER_ADDRESS, REMOTE_NODE_ID, MAILBOX_LENGTH

Step 3 If desired, add optional column headers to the first row. Be sure to separate the column headers with commas.

Step 4 Add the data for the delivery locations in the subsequent rows. When finished:

- Confirm that each row contains the applicable data corresponding to each column header.
- Confirm that the data is separated by commas, and that no tabs, spaces, or semicolons separate the data in the file.
- If any data includes a space, quotes, or commas, contain it within quotes.
- Note that each row does not have to contain data in the optional columns.

Step 5 Save the file as a CSV file.

Step 6 Continue with the following "To Create Bridge Delivery Locations by Using the Cisco Unity Bulk Import Wizard" procedure.

To Create Bridge Delivery Locations by Using the Cisco Unity Bulk Import Wizard

Step 1 Before you run the Cisco Unity Bulk Import wizard, disable virus-scanning services and intrusion-detection software on the Cisco Unity server, if applicable. Otherwise, the Cisco Unity Bulk Import wizard may run slowly.

Step 2 On the Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Bulk Import**.

Step 3 On the Welcome page, click **Next**.

Step 4 On the Select Import Operation, in the Locations section, click **CSV File**, and then click **Next**.

Step 5 On the Select Location Operation page, click **Create New Locations**, and then click **Next**.

Step 6 On the Type of Locations page, click **Bridge**, and then click **Next**.

Step 7 On the Files page, specify the name and location of the input file.

Step 8 Specify the name and location of the output file, or use the default location and file name, which is based on the input file. For example, if the input file is C:\Temp\Bridge_Locations.csv, the default output file will be C:\Temp\Bridge_Locations.out.csv.

Step 9 Click **Next** to proceed to the Valid Location Data page, which displays a table with validated rows of data from the input CSV file. If you do not want to import a row of data, uncheck the check box in the first column of the row.

If errors were found in any of the rows, you can click the Errors link at the bottom of the page to open the output CSV file to correct the errors, or you can ignore the errors for now and proceed with the import.

Step 10 Click **Next** to start the import process and display the Creating Locations page, which provides status information about the import.

Step 11 When the delivery locations are created, click **Next** to display the Cisco Unity Bulk Import Wizard Finished page, which displays summary information.

Step 12 If you had import errors, continue with the following "To Correct Errors That Occurred When Importing Delivery Location Data from a CSV File" procedure.

To Correct Errors That Occurred When Importing Delivery Location Data from a CSV File

Step 1 Browse to the directory location of the output file that you specified during the import. (The default location and file name is based on the input file. For example, if the input file is C:\Temp\Bridge_Locations.csv, the default output file will be C:\Temp\Bridge_Locations.out.csv.)

This file contains all of the records that were not imported.

Step 2 Use a text editor to open the output file.

Step 3 Correct any records in the output file by using the error information listed in the Results column of the file.

Step 4 When you have finished editing the output file, save it as a CSV file with a new name.

Step 5 Run the Cisco Unity Bulk Import wizard again with the new CSV file.

Step 6 Repeat this procedure until all delivery locations are created without error.

Modifying Existing Delivery Locations by Using the Cisco Unity Bulk Import Wizard

If you want to use the Cisco Unity Bulk Import wizard to make modifications to existing delivery locations, you will need to create a CSV file for the modifications. We recommend that you run the Cisco Unity Bulk Import wizard to export your existing delivery location data to a CSV file, and then edit the CSV file to use for the modification.

Note that the DTMF_ACCESS_ID column is used as the primary key to find the existing delivery location, and therefore it cannot be modified by the Cisco Unity Bulk Import wizard.

Creating New or Modifying Existing Subscriber Accounts for Testing Purposes

If you have a large number of Cisco Unity subscribers to add or modify for Bridge Networking, you may choose at this point to add or modify only a few subscriber accounts, to test the configuration. Do the following "To Create Subscribers for Testing Bridge Networking" procedure, which calls attention to the settings that are of interest for networking with the Bridge.

Note that for synchronization between Cisco Unity and the Bridge to occur automatically, there must be at least one Cisco Unity subscriber configured with the Unity Node Serial Number for each Unity node that will be configured on the Bridge.

For detailed information about the creation and modification of subscriber accounts, see the following sections:

- Adding the Serial Number and Mailbox ID to New Cisco Unity Subscriber Accounts, page 2-25
- Adding the Serial Number and Mailbox ID to Existing Cisco Unity Subscriber Accounts, page 2-25

For information about subscriber templates, classes of service, and all other details that you need to consider before creating Cisco Unity subscribers, refer to the "Creating Subscriber Accounts" chapter of the *Cisco Unity System Administration Guide*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

To Create Subscribers for Testing Bridge Networking

Step 1 In the Cisco Unity Administrator, go to the **Configuration > Settings** page.

Step 2 Check the **Display Fields Required for Cisco Unity Bridge Networking on Subscribers Profile Page** check box.

Step 3 Click the **Save** icon.

Step 4 Go to the **Subscribers > Subscribers > Profile** page.

Step 5 If creating new subscriber accounts, do the following sub-steps. If modifying existing subscriber accounts, skip to Step 6.

a. Click the **Add** icon.

b. Click **Select** to import an existing Domino user.

c. Click **Find** to find a Notes mail user.

d. Click the user name on the list.

e. Enter the applicable information on the Add Subscriber page. For testing Bridge Networking, be sure to enter correct values for the Unity Node Serial Number and the Legacy Mailbox ID.

f. Click **Add**.

g. Record a voice for the subscriber.

h. Change any of the other subscriber settings as applicable, and click the **Save** icon.

i. Repeat Step a through Step h to create additional subscriber accounts.

Step 6 If modifying existing subscriber accounts, do the following sub-steps:

a. Click the **Find** icon, select an option from the Find By list, click **Find**, and select the applicable subscriber from the list to view the subscriber Profile settings.

b. Confirm that the subscriber has a recorded voice name.

c. For testing Bridge Networking, be sure to enter correct values for the Unity Node Serial Number and the Legacy Mailbox ID.

d. Change any of the other subscriber settings as applicable, and click the **Save** icon.

e. Repeat Step a through Step d as needed to modify other subscriber accounts.

Configuring the Bridge Server

Configuring the Bridge and Testing the Configuration

See the following sub-sections:

Accessing the Tools Used for Configuring the Bridge

The primary tool that you will use to configure the Bridge is the web-based Bridge Administrator. You use the Bridge Administrator to configure all settings on the Bridge server, as well as to create, modify, and delete Unity and Octel nodes.

A command line utility, the Cisco Unity Bridge Bulk Node utility, is available for download from the Cisco Unity Tools website at http://www.ciscounitytools.com. With the Bulk Node utility, you can create, modify, and delete Unity or Octel nodes on the Bridge server by using information from a comma-separated value (CSV) file. For details on the Bulk Node utility, refer to the Readme.htm file that is included with the utility.

The procedures in the following "Configuring the Bridge" section provide instructions for using the Bridge Administrator to configure required settings and to create Unity and Octel nodes. You can access the Bridge Administrator locally or remotely by using Internet Explorer:

- To access the Bridge Administrator from a local server, in Internet Explorer, enter http://Localhost, or use the shortcut on the desktop or on the Programs menu.
- To access the Bridge Administrator from a remote server, in Internet Explorer, enter http://machinename, where machinename is the name of the Cisco Unity Bridge server.

Configuring the Bridge

When setting up Cisco Unity and the Bridge, be sure to complete the following tasks before configuring the Bridge:

1. Configure the Cisco Unity bridgehead server for Bridge Networking.
2. Configure the serial number and mailbox ID for existing Cisco Unity subscribers.

If you set things up in this order, directory synchronization between Cisco Unity and the Bridge happens automatically. However, if the above steps are not complete prior to configuring the Bridge, you must manually synchronize the directories when the setup is complete.

Most of the pages in the Bridge Administrator have default settings. In most cases, the default settings are appropriate when configuring the Bridge for the first time. The following procedures include steps for all settings that are required for configuring the Bridge. Do the following procedures in the order listed:

- To Configure the System Settings Page, page 2-16
- To Configure the Digital Networking Page, page 2-16
- To Configure the Unity Nodes Page(s), page 2-17
- To Configure the Octel Node Page(s), page 2-17
- To Add Password Protection to the Bridge Administrator, page 2-18

To Configure the System Settings Page

Step 1 On the Configuration menu in the Bridge Administrator, click **System Settings**.

Step 2 In the Attempts On Bad Connection box, enter the number of times that the server will call a line with a bad connection before it returns the message as non-deliverable.

Step 3 In the Name Aging box, enter the number of days that the server will retain a usage-based directory entry that has not been referenced before deleting the entry.

If you want to disable name aging, enter **0**.

Step 4 Accept the default settings for Queued Call Threshold and Max Ports Per Node.

Step 5 Set the Call Tracing Level to **Verbose**.

Step 6 Click **Save**.

To Configure the Digital Networking Page

Step 1 On the Configuration menu in the Bridge Administrator, click **Digital Networking**.

Step 2 If the Bridge server will be sending SMTP messages to an ESMTP e-mail host that acts as a relay server, enter the IP address or fully qualified domain name of the e-mail host.

If you are unsure, do not enter anything in the ESMTP Server field at this point. After configuring the rest of the mandatory fields, there are instructions for testing network connectivity that will help you determine if you need to enter an address here.

Step 3 In the Bridge Server Full Computer Name box, enter the fully qualified domain name of the Bridge server. To determine the fully qualified domain name of the Bridge server, do the following sub-steps:

a. On the Windows Start menu on the Bridge server, click **Settings > Control Panel**.

b. Double-click **System**.

c. Click the **Network Identification** tab. The fully qualified domain name of the Bridge server is listed on this tab as the Full Computer Name.

The name that you enter here must match the name entered in the Cisco Unity Administrator on the delivery locations page(s) configured for this Bridge server in the Bridge Server Full Computer Name field.

Step 4 In the SMTP Port field, do not change the default (which is 25) unless you are certain that the server to which the Bridge will be sending SMTP messages uses a different port.

Step 5 Click **Save**.

Step 6 Restart the Digital Networking service on the Bridge server.

To Configure the Unity Nodes Page(s)

Step 1 On the Configuration menu in the Bridge Administrator, click **Unity Nodes**.

Step 2 Click **Add**.

Step 3 In the Serial Number box, enter the serial number of the Unity node. In some cases, this is the serial number of an Octel server that has migrated to Cisco Unity. In other cases, this is the serial number that has been agreed upon to represent Cisco Unity on the Octel analog network. In either case, this serial number must be configured in the node profile on each Octel server in the network. The serial number must match the serial number that has been assigned to at least one Cisco Unity subscriber in the network.

Step 4 In the Name box, enter the name of the node.

Step 5 In the Unity Bridgehead Server Name box, enter the server name of the Cisco Unity bridgehead server with which the Bridge communicates.

Step 6 In the Unity SMTP Mail Suffix box, enter the Interop Gateway foreign domain name.

Step 7 Select the codec used to encode all voice messages sent from the Bridge to Cisco Unity subscribers with this Unity Node.

All recorded voice names from the Bridge to the Cisco Unity bridgehead server will be sent by using the codec specified on the first Unity Node listed on the Unity Nodes page. We recommend that the same codec setting be used for all Unity Node profiles.

Step 8 Click **Save**.

Step 9 Repeat Step 2 through Step 8 for each serial number that the Bridge and Cisco Unity bridgehead server represent.

To Configure the Octel Node Page(s)

Step 1 On the Configuration menu in the Bridge Administrator, click **Octel Nodes**.

Step 2 Click **Add**.

Step 3 In the Serial Number box, enter the Octel analog networking serial number of the Octel server that this node corresponds to. The Serial Number should also match the number that was entered in the Cisco Unity Administrator in the Octel Node Serial Number field on the Delivery Locations page that corresponds to this Octel Node.

Step 4 In the Name box, enter the name of the node.

Step 5 In the Phone Number box, enter the phone number that the server dials to send messages to the remote node.

Step 6 Optionally, in the Extension box, enter an extension number if it must be dialed to reach the remote node.

Step 7 Optionally, in the Dial Sequence box, enter a dial sequence if one is required to call the remote node. At a minimum, this box must contain at least the default value **N**.

Step 8 Click **Save**.

Step 9 Repeat Step 2 through Step 8 for each Octel node in the network.

Adding Password Protection to the Bridge Administrator

Although the Bridge server itself is password protected, you may also want to add password protection to the Bridge Administrator.

To Add Password Protection to the Bridge Administrator

Step 1 Log on to the Bridge server platform by using the Administrator account.

Step 2 On the Windows Start menu, click **Programs > Administrative Tools > Internet Service Manager**.

Step 3 In the tree, click the server name.

Step 4 Right-click **Default Web Site** and select **Properties**.

Step 5 Click the **Directory Security** tab. In the Anonymous Access and Authentication section, click **Edit**.

Step 6 Select **Integrated Windows Authentication**, and uncheck the **Anonymous Access** check box.

Step 7 Click **OK** twice and close the Internet Service Manager.

Step 8 In Windows Explorer, browse to the **\Starfish\Asp** directory.

Step 9 Right-click the **\Starfish\Asp** directory and select **Properties**.

Step 10 Click the **Security** tab.

Step 11 Select **Everyone**. Uncheck the **Allow Inheritable Permissions From Parent** check box and click **Remove**.

Step 12 Click **Add** to add users or groups to the Access Control List (ACL). Click **OK** when finished.

Step 13 In the Permissions list, select **Full Control** for the person(s) you want to have access.

Caution Be sure to give Full Control in the Permissions list to the account that you will use to do upgrades; if the account used to do upgrades does not have Full Control, the Bridge setup program will fail.

Step 14 Click **OK** and close Windows Explorer.

Testing Networking and SMTP Connectivity

Do the following procedures in the order listed to test the configuration:

To Verify Network Connectivity

Use the following procedure to verify network connectivity from the Bridge server to the server that will receive SMTP messages that are destined for Cisco Unity.

Step 1 On the Bridge server, open a command prompt window.

Step 2 Enter **ping <Domain Name>** where <Domain Name> is the name that you entered on the Unity SMTP Mail Suffix field on the Unity Nodes page.

Step 3 You should receive a reply from the server.

Step 4 If the test is successful, continue with the "To Verify SMTP Connectivity" procedure on page 2-19.

If the test failed, this indicates a name resolution problem. As a first choice for fixing the name resolution problem, we recommend that you use DNS. Add a mail exchange (MX) record in DNS by using the Interop Gateway foreign domain name (which must exactly match the name in the Unity SMTP Mail Suffix field) and the IP address of the Domino (or relay) server that handles incoming SMTP messages. If using DNS is not an option, add an entry to the HOSTS file on the Bridge server using the Interop Gateway foreign domain name (which must exactly match the name in the Unity SMTP Mail Suffix field) and the IP address of the Domino (or relay) server that handles incoming SMTP messages.

Step 5 When the name resolution problem is fixed, continue with the "To Verify SMTP Connectivity" procedure on page 2-19.

To Verify SMTP Connectivity

Step 1 Open a command window on the Bridge server.

Step 2 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").

Step 3 If the test is successful, enter **quit** to end the telnet session. Continue with the "To Set Permissions to Access the Interop Gateway Mail File" procedure on page 2-20.

If the test fails, this indicates there is 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. Do not proceed to the next test until this issue has been resolved.

To Set Permissions to Access the Interop Gateway Mail File

Before sending the test message, you will need to verify that you have permission to open the Interop Gateway mail file to read and then delete the message. How you do this depends on the Domino version and the security policies for your organization. Use the following as a guide:

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 Editor plus Delete Documents 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 using the name and password of the Person document that was created for the Cisco Unity server on which the Interop Gateway Configuration wizard was run. This account should have Editor plus Delete Documents permissions to the Interop Gateway mail file.

  You can either use this account when verifying that the test message was received, or you can add yourself to the Interop Gateway mail file Access Control List (ACL) with Editor plus Delete Documents permissions.

Continue with the following "To Send a Test Message to the Interop Gateway Mail File" procedure.

To Send a Test Message to the Interop Gateway Mail File

Use telnet to send a test message from the Bridge to Domino and verify that the message appears in the Interop Gateway mail file. Repeat this test for each Unity SMTP Mail Suffix that is configured on the Bridge server.

Step 1 On the Cisco Unity server on which the Interop Gateway service is running, open the Services MMC.

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

Step 3 On the Bridge server, on the Windows Start menu, click **Run**.

Step 4 Enter **telnet** and click **OK**. This opens a telnet command prompt window.

Tip Because the backspace character is not supported in the telnet window, you may want to enter each command in Notepad, copy it, and then right click in the telnet window to paste the command. The commands require that you enter text that you have already entered in fields in the Bridge Administrator. You may want to copy the text that you entered in the Bridge Administrator fields and paste the text to ensure that you do not make a typing error.

Step 5 Enter **set local_echo**.

Step 6 Enter **open <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.

If a connection is successfully established, you will 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
```

Step 7 Enter **ehlo <FQDN>**, where <FQDN> is the Bridge Server Full Computer Name entered on the Digital Networking page. The server responds with a list of options that it supports.

Step 8 Enter **mail from: <Extension>@<FQDN>**, where <Extension> can be any number, and <FQDN> is the Bridge Server Full Computer Name entered on the Digital Networking page. This simulates the format of the "from" field of messages that the Bridge sends to Domino.

Step 9 Enter **rcpt to: IMCEAOMNI-AvVoiceMessage@<Mail suffix>**, where <Mail suffix> is the Unity SMTP Mail Suffix that you entered on the Unity Nodes page. The <Mail suffix> should exactly match the Interop Gateway foreign domain name. This is the "to" address that the Bridge uses when sending messages to Domino.

Step 10 Enter **data**. You should see a response similar to the following:

```
354 Start mail input; end with <CRLF> <CRLF>
```

Step 11 Enter **test**, or any text that you prefer as the content of the test message. Press Enter.

Step 12 Enter **.** (a period). Press Enter, and you should see a response similar to the following:

```
250 2.6.0 <FQDN> Queued mail for delivery
```

Step 13 Enter **quit**, and close the command prompt window.

Step 14 On the Domino server on which the Interop Gateway mail file is located, log on to the Domino Administrator using an account that has permission to open the Interop Gateway mail file to read and then delete the test message.

Step 15 Click the **Files** tab.

Step 16 Double-click the Interop Gateway mail file in the list to open it.

Step 17 If the message is there, then the Unity SMTP Mail Suffix is correct. If the message is not there, then see the "Troubleshooting Tips" section below for information on resolving the problem.

Step 18 Delete the message and close the mail file.

Caution You must delete the test message before starting the Interop Gateway service because the header of the message is not in the expected format.

Step 19 Close the Domino Administrator.

Step 20 On the Cisco Unity server on which the Interop Gateway service is running, open the Services applet.

Step 21 Right-click **CsDomInteropGty** and click **Start**.

Step 22 Close the Services MMC.

Troubleshooting Tips

If the message does not appear in the Interop Gateway mail file, check the following:

- Verify that the Unity SMTP Mail Suffix on the Unity Nodes page is correct. This name must exactly match the Interop Gateway foreign domain name. Use the Domino Administrator to open the foreign domain document to see the name.
- Verify that the applicable Connection documents are in place so that the Domino (or relay) server that receives incoming SMTP messages can route messages to the Domino server on which the Interop Gateway mail file is located.

Configuring the Octel Servers

If the Bridge is joining the Octel network as a new Octel node, information about the new node must be programmed on each existing Octel server. If the Bridge replaces an existing Octel server and serial number, some programming of the existing Octel servers is usually still required. For example, you may need to change the phone number for the existing node profile to that of the Bridge server, or change the primary transmission node from digital to analog. Additionally, in order for NameNet to function properly, schedules for administration calls need to be configured on the Octel servers. Refer to the applicable Octel documentation for detailed information.

Testing the Octel Analog Network

Before sending test messages between Cisco Unity and the remote voice messaging system(s), as a best practice, first verify that the Bridge can communicate with each of the configured Octel nodes. Testing the Octel analog network separately allows you to more quickly identify and fix any problems that you may encounter. To do the tests, you will use the 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 the Octel nodes in the analog network. It also provides detail and summary information of call activity.

BANANA contains an administration application called the BANANA admin that allows you to control how BANANA:

- Generates test calls to the Octel systems that are networked with the Bridge server.
- Extracts information from the call traces on the Bridge server and presents different views of the data.
- Monitors the call traces for error conditions, and logs warnings or errors to the Windows Event Viewer.

With the BANANA admin, you can also install and configure the BANANA service to do the tasks listed above at configurable intervals.

Caution The drive on which you plan to install BANANA requires at least 1 GB of free disk space.

Do the following procedures to install BANANA and initiate test calls. Refer to the BANANA Help file for information about other functionality provided by BANANA.

To Install 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

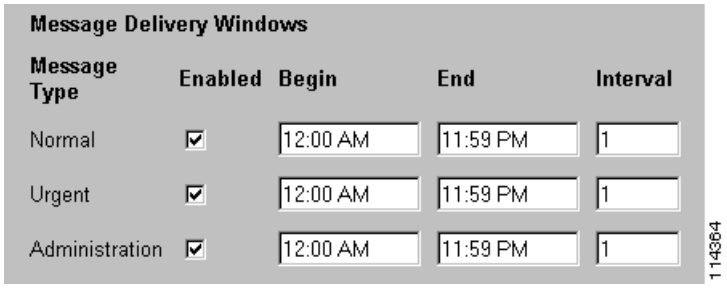
Note The most up-to-date version of BANANA is available at http://www.CiscoUnityTools.com. When you start BANANA, it checks the CiscoUnityTools website to see if a newer version is available, and if so, prompts you about upgrading.

To Adjust the Message Delivery Window Settings

Step 1 In the Bridge Administrator, click **Octel Nodes**.

Step 2 In the Node list, click an Octel node that you want to be tested, and click **Edit**.

Step 3 On the Octel Node page in the Message Delivery Windows section, adjust the schedule according to following illustration, so that the Bridge will not wait to initiate calls to the Octels to deliver normal, urgent, and administrative messages.



Note that BANANA makes only administrative calls when testing the Octel analog network. However, if you adjust the normal and urgent schedules as shown, you do not have to remember to adjust the schedule if you also send test messages from Cisco Unity subscribers to Octel subscribers.

Step 4 Click **Save**.

Step 5 Repeat Step 2 through Step 4 for each Octel node that you want to test.

To Initiate Test Calls to the Octel Nodes

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

Step 2 Configure the log and output folder locations.

Step 3 Specify the Octel nodes to be included when placing test calls.

Step 4 Place the test calls.

Step 5 Process the call data, and view the results.

Refer to the BANANA Help for details.

Testing the Setup

Before beginning this procedure, create test subscriber accounts on Cisco Unity and on each Octel node for which a delivery location has been configured. Be sure to record voice names for the subscribers. See the "Creating New or Modifying Existing Subscriber Accounts for Testing Purposes" section on page 2-14 for instructions.

To Test the Setup

Step 1 If you have not already done so, set the Message Delivery Window settings so that the Bridge does not wait to initiate calls to the Octels to deliver normal, urgent, and administrative messages, as described in the "To Adjust the Message Delivery Window Settings" section on page 2-23.

Step 2 Verify message flow from Cisco Unity to Octel. Log on to Cisco Unity and send a test message to an Octel subscriber on each Octel node. Verify that the recipient receives the message.

Step 3 Verify message flow from Octel to Cisco Unity. On each Octel node, log on and send a test message to a Cisco Unity subscriber. Verify that the recipient receives the message.

Step 4 Verify directory message flow from Cisco Unity to the Bridge, as follows:

a. Add a test Cisco Unity subscriber account with a serial number and legacy mailbox ID on a Cisco Unity server in the network.

b. Verify that shortly after creation, the subscriber is listed in the applicable Unity Node Directory listing of each Bridge server, with a Legacy Mailbox as defined on Cisco Unity.

Step 5 Verify directory message flow from the Bridge to Cisco Unity, as follows:

a. Enter the mailbox of a subscriber on a remote Octel server in the applicable Octel Node Directory on the Bridge (use a mailbox for which a Bridge Subscriber has not yet been created on the Cisco Unity bridgehead server).

b. Verify that the name information for the subscriber is retrieved by the Bridge via an administrative call to the Octel server.

c. Verify that the name of the remote Octel subscriber is added to the applicable Octel Node Directory on the Bridge server that is associated with the mailbox you entered.

d. Verify that, shortly thereafter, a Bridge Subscriber is automatically created on the Cisco Unity bridgehead server with the settings that you have configured for the associated delivery location.

Step 6 Change the Message Delivery Window settings back to their configuration prior to the test.

Finishing the Setup

Finishing the Creation and Configuration of Bridge Delivery Locations

If you have already created all Bridge delivery locations, skip to the "Adding the Serial Number and Mailbox ID to Cisco Unity Subscriber Accounts" section on page 2-25.

Otherwise, create a delivery location on the Cisco Unity bridgehead server for each Octel node with which Cisco Unity will communicate. See the "Creating and Configuring Bridge Delivery Locations" section on page 2-11 for detailed information. When finished, continue with the next section, "Adding the Serial Number and Mailbox ID to Cisco Unity Subscriber Accounts."

Adding the Serial Number and Mailbox ID to Cisco Unity Subscriber Accounts

In order for Cisco Unity subscribers to be able to send messages to and receive messages from subscribers on the remote voice messaging systems with which Cisco Unity communicates, each Cisco Unity subscriber account must be configured with a serial number and legacy mailbox ID. These numbers are used to identify a Cisco Unity subscriber when communicating with the Octel analog network via the Bridge.

Adding the Serial Number and Mailbox ID to New Cisco Unity Subscriber Accounts

You use either the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator to create new Cisco Unity subscriber accounts with the serial number and mailbox ID.

For detailed information about creating subscriber accounts, refer to the "Creating Subscriber Accounts" chapter of the *Cisco Unity System Administration Guide*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Adding the Serial Number and Mailbox ID to Existing Cisco Unity Subscriber Accounts

You can manually add the serial number and mailbox ID to existing subscriber accounts one at a time by using the Cisco Unity Administrator, or you can do so in bulk by using the Subscriber Information Dump and the Cisco Unity Bulk Import wizard, as described in the following procedure.

To Add the Octel Serial Number and Mailbox ID to Existing Cisco Unity Subscriber Accounts

Step 1 In the Cisco Unity Administrator, go to the **Configuration > Settings** page.

Step 2 Check the **Display Fields Required for Cisco Unity Bridge Networking on Subscribers Profile Page** check box.

Step 3 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 4 In the left pane of Tools Depot, expand the **Administration Tools** tree and double-click **Subscriber Information Dump**. The Subscriber Information Dump dialog box opens.

Step 5 Select **Full Subscribers Only** from the Subscribers to Dump list.

Step 6 Indicate the output file name and location.

Step 7 Use the default settings for the Separate Data With and Use Quotes Around fields. (By default, these fields are set respectively to "Commas" and "When the Data Includes a Comma.")

Step 8 Check the **Alias** and **Primary Extension** check boxes in the Data to Include in Output File list.

Step 9 Click **Start**.

When the output is complete, a message box opens with the number of errors encountered in the process. Click **OK** to view the error log, or **Cancel** if no errors were encountered.

Step 10 Exit the Subscriber Information Dump and Tools Depot.

Step 11 Make a copy the output CSV file.

Step 12 Open the output CSV file in a text editor or spreadsheet application.

Step 13 In the first row of the file, delete the column header **ALIAS**, and in its place, enter **SHORT_NAME**.

Step 14 In the first row of the file, delete the column header **PRIMARY_EXTENSION**, and in its place, enter **LEGACY_MAILBOX**.

Step 15 At the end of the first row of the file, enter a comma and a new column header: **REMOTE_NODE_ID**. Be sure to separate the column headers with a comma.

Step 16 In each row of subscriber data in the REMOTE_NODE_ID column, enter a comma and the serial number. For example:

```
SHORT_NAME,LEGACY_MAILBOX,REMOTE_NODE_ID
aabade,2001,55115
kbader,2002,55115
tcampbell,2003,55115
lcho,2004,55115
```

Step 17 Save and close the file.

Step 18 Disable any virus-scanning services on the Cisco Unity server.

Step 19 On the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Bulk Import**, and click **Next** on the Cisco Unity Bulk Import wizard welcome page.

Step 20 Accept the default, CSV file, and click **Next**.

Step 21 Specify where the log files should be saved, and click **Next**.

Step 22 On the Choose Subscriber Type dialog box, click either **Unified Messaging** or **Voice-Mail Only**, as applicable to your installation.

Step 23 On the Select Subscriber Import Option dialog box, click **Modify Existing Cisco Unity Subscribers**.

Step 24 On the Select the CSV File dialog box, browse to the CSV file containing the subscriber data.

Step 25 Follow the on-screen prompts to finish the import.

Step 26 Enable any virus-scanning services.

Setting the Serial Number and Mailbox ID for Unidentified Callers

The following procedure describes how to set the serial number and mailbox ID for unidentified callers (also referred to as unknown callers). The numbers that you enter here will be used for messages from unidentified callers to Bridge subscribers. For more information about these settings, see the "Bridge Options Unknown Caller Settings" section on page 7-9.

To Set the Serial Number and Mailbox ID for Unidentified Callers

Step 1 In the Cisco Unity Administrator on the bridgehead server, go to the **Network > Bridge Options > Unknown Caller** page.

Step 2 Enter a number in the Legacy Mailbox ID field.

Step 3 Enter a serial number in the Node ID field.

Step 4 Click the **Save** icon.

Creating Bridge Subscriber Accounts

There are several approaches and tools available for creating Bridge subscribers on the Cisco Unity server, or creating permanent directory entries on the Bridge server, which results in auto-created Bridge subscribers.

See the following sections for more information:

Before Creating Bridge Subscriber Accounts

This section lists—in order—the issues that you must consider before creating Bridge subscriber accounts. Bridge subscribers can be created only on a Cisco Unity bridgehead server. Do the following tasks on the Cisco Unity bridgehead server where you will be adding the Bridge subscribers.

1. Cisco Unity Configuration and Permissions

If you are unsure whether the account that you are using has sufficient rights and permissions to create subscribers, or whether Cisco Unity is properly configured to work with your message store, use the following "To Check Cisco Unity Setup and Permissions by Using the Cisco Unity SysCheck Tool" procedure.

To Check Cisco Unity Setup and Permissions by Using the Cisco Unity SysCheck Tool

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane of the Tools Depot window, in the Diagnostic Tools directory, double-click **SysCheck**.

Step 3 On the Welcome to the Cisco Unity Configuration Wizard page, click **Select Configuration Tests**, and click **Next**.

Step 4 Uncheck the boxes for the message stores that are not connected to Cisco Unity.

Step 5 Click **Test**.

Step 6 In the Test Results box, click the link provided to view the test results.

Step 7 If no errors are reported, proceed to Step 8. Otherwise, do the following sub-steps:

a. Follow the advice offered in the Resolution column to correct each configuration or permissions error.

b. Return to the Completing the Check Unity Configuration Wizard page, and click **Finish**.

c. Repeat Step 2 through Step 7 until no errors are reported.

Step 8 Click **Finish**.

2. Classes of Service

A class of service (COS) defines limits and permissions for subscribers who use Cisco Unity. For example, a COS dictates the maximum length of subscriber messages and greetings. Although most COS settings are not applicable to Bridge subscribers, they still must be members of a COS. In the Cisco Unity Administrator, a COS is specified in each subscriber template; thus, a subscriber is assigned to the COS that is specified in the template upon which the subscriber account is based. Cisco Unity includes predefined classes of service, which you can modify. You can also create new classes of service. For details, refer to the "Class of Service Settings" chapter in the *Cisco Unity System Administration Guide*.

3. Restriction Tables

Each COS specifies a restriction table for call transfers, one for message notification, and one for fax deliveries. Cisco Unity applies the restriction table associated with the COS of a subscriber, and displays an error message if the phone number is not allowed. Cisco Unity comes with predefined restriction tables, which you can modify.

Although most restriction table settings do not apply to Bridge subscribers because they cannot log on to Cisco Unity or use the Cisco Personal Communications Assistant (PCA), administrators can enter call transfer numbers for Bridge subscribers. For security purposes, you should modify the restriction table used for transfers in the COS to which Bridge subscribers belong, as necessary. For details, refer to the "Restriction Tables" chapter in the *Cisco Unity System Administration Guide*.

4. **Public Distribution Lists**

Public distribution lists are used to send voice messages to multiple subscribers at the same time. Cisco Unity assigns new subscribers to the public distribution lists that are specified in the template on which the subscriber account is based. For details, refer to the "Public Distribution List Settings" chapter in the *Cisco Unity System Administration Guide*.

Public distribution lists correspond to groups in Domino and are listed in the Notes address book. To help prevent others from sending e-mail to Bridge subscribers, you may want to create lists that contain only Bridge subscribers, and add text similar to "Voice Mail Only" to the list names. Additionally, you may also want to exclude Bridge subscribers from the All Subscribers distribution list or any other distribution list that contains regular subscribers.

5. **Subscriber Templates**

In the Cisco Unity Administrator, you can specify settings for a group of subscribers by using a subscriber template. Subscriber templates contain settings that are applicable for subscribers of a particular type, such as a department. The settings from the template you choose are applied to subscriber accounts as the accounts are created. Cisco Unity comes with a default subscriber template, which you can modify, and you can create an unlimited number of additional templates. For more details, refer to the "Subscriber Template Settings" chapter in the *Cisco Unity System Administration Guide*.

Bridge subscribers have corresponding Domino Person documents that have "Other Internet Mail" set in the Mail System field, and they are listed in the Notes address book. To help prevent others from sending e-mail to Bridge subscribers, you may want to add text similar to "Voice Mail Only" to the Bridge subscriber names.

You may want to use the {Bridge Subscriber} template. By default, Bridge subscribers created with the {Bridge Subscriber} template are not added to any distribution lists and are not listed in the Cisco Unity phone directory. By default, the {Bridge Subscriber} template is used for automatically created Bridge subscribers.

Note The *Cisco Unity System Administration Guide* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Approaches to Creating Bridge Subscribers

This section summarizes the general approaches to creating Bridge subscribers on the Cisco Unity bridgehead server.

Approach A: Creating Bridge Subscribers in Cisco Unity

If you want the extensions that you assign to Bridge subscribers to fit in with your numbering plan, create the Bridge subscriber accounts in Cisco Unity. See the following sections:

- Using the Cisco Unity Bulk Import Wizard to Create Multiple Bridge Subscriber Accounts, page 2-30
- Using the Cisco Unity Administrator to Create Bridge Subscriber Accounts, page 2-33

Note that the Bridge subscribers will be subject to name aging deletion (if enabled), and the recorded voice names for the Bridge subscribers will be retrieved from the Octel system the first time a Cisco Unity subscriber sends each Bridge subscriber a message. For more details, see the "Creating Bridge Subscribers in Cisco Unity" section on page 1-19.

Approach B: Creating Permanent Directory Entries on the Bridge Server

If you want the Bridge subscribers to always have recorded voice names and not be subject to name aging deletion, create permanent directory entries on the Bridge server. See the following sections:

- Using the Bridge Administrator to Create Permanent Directory Entries, page 2-33
- Using the Cisco Unity Bridge Mailbox Import Tool to Create Permanent Directory Entries, page 2-34

The Bridge retrieves the text and voice names from the Octel system for the directory entries and passes this information to Cisco Unity so that it is used when the Bridge subscribers are created. Each auto-created Bridge subscriber will be assigned an extension that consists of the delivery location dial ID followed by the remote mailbox number. For more details, see the "Creating Permanent Directory Entries on the Bridge Server" section on page 1-19.

Approach C: Creating Bridge Subscribers and Then Creating Corresponding Permanent Directory Entries

If you want the benefits of both approaches, first create the Bridge subscribers on the Cisco Unity server, and then create corresponding directory entries on the Bridge server. When set up this way, the Bridge subscribers will have the extensions that you assign, they will not be subject to name aging deletion, and the Bridge subscriber accounts will automatically be updated with the text and voice names retrieved from the Octel system. For more details, see the "Creating Bridge Subscribers and Then Creating Corresponding Permanent Directory Entries" section on page 1-20.

Using the Cisco Unity Bulk Import Wizard to Create Multiple Bridge Subscriber Accounts

The Cisco Unity Bulk Import wizard allows you to create multiple subscriber accounts at the same time by importing user data from a comma-separated value (CSV) file. CSV is a common text file format for moving data from one data store to another. As long as user data contained in the CSV file is formatted correctly, you can use it to create new Person documents at the same time that you create subscriber accounts, or you can use it to create Bridge subscribers with existing Person documents. (The corresponding Person documents have "Other Internet Mail" set in the Mail System field.)

If you choose to create Bridge subscriber accounts with existing Person document data, note that the Forwarding address field in the Person documents for the imported users is overwritten with the extension address that is used for addressing voice messages to the remote voice messaging systems. Thus, the imported objects can no longer be used for outbound message addressing to remote e-mail addresses.

Use the following procedure to prepare your CSV file. To learn more about preparing a CSV file for use with the Cisco Unity Bulk Import wizard—including information on the required and optional column headers for your CSV file—refer to the Cisco Unity Bulk Import wizard Help.

To Prepare a CSV File for Creating Bridge Subscriber Accounts

Step 1 Save the data which you will use to create Cisco Unity accounts as a CSV file.

As a best practice, do not include more than 7,500 records in a single CSV file, as you may encounter unexpected results when the Cisco Unity Bulk Import wizard imports the data.

Step 2 Copy the CSV file to the Cisco Unity bridgehead server or to a directory that you can browse to from the server.

Step 3 Open the CSV file in a spreadsheet application or another application with which you can edit and reorganize the data. Do the following:

- Confirm that the data is separated by commas, and no tabs, spaces, or semicolons separate the data in the file.

- If any data includes a space, quotes, or commas, contain the characters within quotes.

Step 4 Rearrange the data so that the columns are in the same order as the column headers that you will add in Step 5. The order of the column headers does not matter, though it is good practice to set up your CSV file as indicated here. For example, the columns of data in this sample are sorted so that the last name of the user is followed by the first name, the short name, the extension (DTMF_ACCESS_ID), and then by the remote mailbox number (REMOTE_USER_ID):

```
Abade,Alex,aabade,2001,3000
Bader,Kelly,kbader,2002,3100
Campbell,Terry,tcampbell,2003,3200
Cho,Li,lcho,2004,3300
```

Step 5 Enter the required column headers above the first row of data. Column headers must be in uppercase, separated by commas, and spelled as indicated below:

```
LAST_NAME,FIRST_NAME,SHORT_NAME,DTMF_ACCESS_ID,REMOTE_USER_ID
```

Note The examples in this procedure illustrate how to set up a CSV file so that the Cisco Unity Bulk Import wizard creates subscriber accounts and new Person documents at the same time. If you choose to create new subscriber accounts with existing Person document data, you must remove the LAST_NAME and FIRST_NAME column headers and data in your CSV file.

Step 6 If desired, add optional column headers to the first row, and the corresponding data that you want to import in the subsequent rows below. As you do so, confirm that:

- Column headers and data are separated by commas. Note that every row does not have to contain data for any optional column header(s).
- Any data that includes a space, quotes, or commas is contained within quotes.

Step 7 To associate the Bridge subscribers in the CSV file with a delivery location, you can either choose from the list of defined delivery locations presented by the Cisco Unity Bulk Import wizard during the import, or you can add the DELIVERY_LOCATION_ID column to the CSV file.

The DELIVERY_LOCATION_ID column contains the dial ID of a delivery location with which the external subscriber will be associated. This value corresponds to the Dial ID field on the Network > Delivery Locations > Profile Page in the Cisco Unity Administrator. If this column header is omitted, or if a row does not contain a value, the delivery location that the Cisco Unity Bulk Import wizard prompts for is used as a default. You can import external subscribers for multiple delivery locations by using one CSV file.

Step 8 If your CSV file contains columns of data that you do not want to import, delete the columns. Alternatively, you can title one column **NOTES**. The Cisco Unity Bulk Import wizard ignores data beneath any NOTES column header, but the wizard does not support more than one NOTES column in a CSV file.

Step 9 Confirm that each row contains the appropriate data corresponding to each column header.

Step 10 Save the file as a CSV file.

Step 11 Continue with the following "To Create Bridge Subscriber Accounts by Using the Cisco Unity Bulk Import Wizard" procedure.

To Create Bridge Subscriber Accounts by Using the Cisco Unity Bulk Import Wizard

Step 1 Disable virus-scanning services and intrusion-detection software on the bridgehead Cisco Unity server, if applicable. Otherwise, the Cisco Unity Bulk Import wizard may run slowly. Refer to the Cisco Unity Bulk Import wizard Help for procedures.

Step 2 On the bridgehead Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Bulk Import**.

Step 3 Follow the on-screen instructions.

To learn more about the options presented in the dialog boxes that appear as the wizard proceeds, click **Help**.

Step 4 When prompted to choose the type of subscriber that you want to create, click **Bridge**.

Step 5 Click **Next**, and proceed through the wizard. If the wizard reports any errors, you can:

- Click **OK** to continue with the import, and fix the errors later.
- Fix the errors. See the "Correcting CSV Import Errors" section on page 2-32 for details.

Step 6 When the subscriber accounts are created, click **Finish**.

Step 7 If you had import errors, but in Step 5 you chose to correct them later, see the "Correcting CSV Import Errors" section on page 2-32.

If you had no import errors, or if all errors have now been corrected, see the "After Creating Subscriber Accounts" section on page 2-35.

Correcting CSV Import Errors

The error log file contains data that the Cisco Unity Bulk Import wizard could not import. The wizard reports the first error it detects in a row in a CSV file. When you have corrected that error, the wizard may detect additional errors in the same row when the data is imported again. Thus, you may need to repeat the correction process—running the Cisco Unity Bulk Import wizard and correcting an error—several times to find and correct all errors.

The output log file contains all the records that were not imported. You can save it as a CSV file, and use it when you run the Cisco Unity Bulk Import wizard again. Note that each time you run the Cisco Unity Bulk Import wizard, the error and output log files are overwritten (unless you specify new names for the files).

To correct import errors, do the following procedure.

To Correct Errors That Occurred When Importing Data from a CSV File

Step 1 Browse to the directory that contains the error log file you specified during the import. (The default location and file name is C:\Error.log.)

Step 2 Use a text editor to open the error log file. You will use the error codes in the file to make corrections.

Step 3 Browse to the directory location of the output log file you specified during the import. (The default location and file name is C:\Output.log.)

Step 4 Use a text editor to open the output log file.

Step 5 Correct any records in the output file that are listed as errors in the error log file.

Step 6 When you have finished editing the output log file, save it as a CSV file with a new name.

Step 7 Run the Cisco Unity Bulk Import wizard again with the CSV file that you saved in Step 6.

Step 8 Repeat this procedure until all subscriber accounts are created without error, and then proceed to the "After Creating Subscriber Accounts" section on page 2-35.

Using the Cisco Unity Administrator to Create Bridge Subscriber Accounts

By using the Cisco Unity Administrator, you can create Bridge subscriber accounts one at a time. When you add a new Bridge subscriber account, a corresponding Person document that has "Other Internet Mail" set in the Mail System field is created in the Domino directory.

To create a Bridge subscriber account, do the following procedure.

To Add a New Bridge Subscriber by Using the Cisco Unity Administrator

Step 1 In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile** page.

Step 2 Click the **Add** icon.

Step 3 Click **New** and select **Bridge** from the list.

Step 4 Enter the First Name and Last Name.

Step 5 Enter the Extension of the Bridge subscriber on Cisco Unity. This is the number that Cisco Unity subscribers use when addressing a message to this Bridge subscriber.

Step 6 Select the Subscriber Template to use.

Step 7 Enter the Remote Mailbox Number, which is the number that the remote voice messaging system uses to route messages to this Bridge subscriber.

Step 8 Select the Delivery Location with which the subscriber is associated.

Step 9 Click **Add**.

Step 10 On the subscriber record, customize settings as applicable, and then click the **Save** icon.

Using the Bridge Administrator to Create Permanent Directory Entries

You can use the Bridge Administrator to create permanent directory entries one at a time. The Bridge retrieves the text and voice names from the Octel system for the directory entries. This data is passed to Cisco Unity and is used to create the corresponding Bridge subscriber accounts and Person documents automatically. The permanent directory entries and the Bridge subscriber accounts created in this way are not subject to name aging.

Like any auto-created Bridge subscribers, these subscriber accounts are created with the subscriber template specified on the Bridge Subscriber Creation Options page in the Cisco Unity Administrator. By default, the predefined {Bridge Subscriber} template is used.

To Add a New Bridge Subscriber by Using the Bridge Administrator

Step 1 If necessary, access the Cisco Unity Bridge server as described in the "Accessing the Bridge for Administration" section on page 8-1.

Step 2 On the Configuration menu, click **Octel Nodes**.

Step 3 Select the Octel node to which you want to add directory entries, and click **Edit**.

Step 4 On the Octel Node page, click **Directory**.

Step 5 On the Directory List page, click **Add**.

Step 6 On the Directory Entry page, enter the subscriber mailbox number in the Mailbox Number box.

Step 7 Optionally, enter the subscriber name in the Name box. If you enter a name here, it will be overwritten by the name retrieved from the Octel node.

Step 8 Click **Save**.

The Bridge server makes an administrative call to the Octel node to obtain the text and recorded voice name for the directory entry and the corresponding Bridge subscriber. Note that if corresponding Bridge subscriber accounts have already been created for the directory entries, the existing Bridge subscriber accounts are updated with the text and voice names retrieved from the Octel system.

Using the Cisco Unity Bridge Mailbox Import Tool to Create Permanent Directory Entries

The Cisco Unity Bridge Mailbox Import tool (MBUpload.exe) is a console application on the Bridge server that allows you to create, modify, or delete multiple permanent directory entries at once by importing user data from a comma-separated value (CSV) file. CSV is a common text file format for moving data from one data store to another.

The Bridge retrieves the text and voice names from the Octel system for the directory entries. This data is passed to Cisco Unity and is used to create the corresponding Bridge subscriber accounts and Person documents automatically. The permanent directory entries and the Bridge subscriber accounts created in this way are not subject to name aging.

Like any auto-created Bridge subscribers, these subscriber accounts are created with the subscriber template specified on the Bridge Subscriber Creation Options page in the Cisco Unity Administrator. By default, the predefined {Bridge Subscriber} template is used.

Note that if corresponding Bridge subscriber accounts have already been created for the directory entries, the existing Bridge subscriber accounts are updated with the text and voice names retrieved from the Octel system.

To Prepare a CSV File for Use with MBUpload

Step 1 Save the data which you will use to create the directory entries as a CSV file. At a minimum, you need the serial numbers and remote mailbox numbers for the subscribers; text names are optional because they will be retrieved from the Octel server.

Step 2 Copy the CSV file to the Bridge server or to a directory that you can browse to from the server.

Step 3 Open the CSV file in a spreadsheet application or another application with which you can edit and reorganize the data. Confirm that the data is separated by commas in the file.

Step 4 Rearrange the data as necessary. Each directory entry should appear on a separate line. Although the CSV file does not contain column headers, the columns must contain the following data in the order listed below:

a. Serial number of the system where the mailbox resides.

b. Remote mailbox number.

c. <Reserved for future use; this column must remain empty.> Note, however, that you must still enter a comma as if there was data in the column.

d. Action to perform: enter **A** to add, **C** to change, or **D** to delete.

e. Text Name. Note that this column is optional, because the text name will be retrieved from the Octel server.

For example, the file may look like the following:

```
12345,4001,,A,Alex Abade
12345,4002,,A,Kelly Bader
12345,4003,,A,Terry Campbell
12345,4004,,A,
12345,4005,,A,
```

Confirm that each row contains the applicable data, and save the file as a CSV file.

Step 5 Continue with the "To Run MBUpload" procedure.

To Run MBUpload

Step 1 On the Bridge server, open a command prompt window.

Step 2 Set the working drive to that on which the Bridge software is installed.

Step 3 Enter **cd \bridge\starfish\bin** to change to the directory where MBUpdate.exe is located.

Step 4 Run MBUpload with the following command line:

MBUpload [/I:<InFile>] [/O:<OutFile>] <DB Path>

Note the following:

- <InFile>—Optional. Specifies the input CSV file name. The file can reside in any directory that is accessible to MBUpload.exe. If a value for InFile is not specified, the default file MBUploadIn.csv in the working directory is used. If the path contains spaces, put quotation marks around them.
- <OutFile>—Optional. Specifies the output file which will contain exception reports. If a value for OutFile is not specified, the default file MBUploadOut.csv in the working directory is used. As MBUpload processes each record, it copies the row from the InFile to the OutFile and appends "Successful" if the operation was a success. If the path contains spaces, put quotation marks around them.
- <DB Path>—Required. Specifies the full path name to the Bridge database file. The path is usually D:\Bridge\Starfish\DB\Starfish.MDB. If the path contains spaces, put quotation marks around it.

For example, to specify the Input.csv and Output.csv in the C:\CSVfiles directory, enter:

MBUpload /I:C:\CSVfiles\Input.csv /O:C:\CSVfiles\Output.csv D:\Bridge\starfish\db\starfish.mdb

To use the default MBUploadIn.csv and MBUploadOut.csv, enter:

MBUpload D:\Bridge\starfish\db\starfish.mdb

After Creating Subscriber Accounts

After creating Bridge subscriber accounts, consider the following:

- It takes a few minutes for the newly-created subscriber account to be available to receive messages.

- You can make changes to subscriber settings for individual accounts in the Cisco Unity Administrator. For details, refer to the "Subscriber Settings" chapter in the applicable version of the *Cisco Unity System Administration Guide*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.
- When you want to modify unique subscriber settings—such as primary or alternate extensions—for multiple subscribers at once, you can (re)run the Cisco Unity Bulk Import wizard. To learn more, refer to the Cisco Unity Bulk Import wizard Help.
- When a subscriber leaves the organization or otherwise no longer needs a Cisco Unity account, you can delete the subscriber account.

  See the "Deleting Bridge Subscribers" section on page 1-22 for details.

Extending Identified Subscriber Messaging to Include Bridge Subscribers

You can extend identified subscriber messaging to include Bridge subscribers. (Note that this is optional.)

When a person on a remote voice messaging system who has a corresponding Bridge subscriber account calls a Cisco Unity subscriber and leaves a message, by default Cisco Unity will not identify the message as being from the Bridge subscriber. For Cisco Unity to identify callers whose calling number matches the extension or alternate extension of a Bridge subscriber, identified subscriber messaging (ISM) must be extended to include Bridge subscribers. See the following sections as applicable to your installation.

Installation with Multiple Cisco Unity Servers Networked via Digital Networking

In installations with multiple Cisco Unity servers networked via Digital Networking, enabling ISM to include Bridge subscribers requires the following:

1. The Cisco Unity servers must be connected to the same phone system or phone system network as described in the "Dialing Domains" section of the "Digital Networking" chapter in the *Networking in Cisco Unity Guide* (Release 4.0(4) or later), available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
2. The Cisco Unity servers must be configured to be in the same dialing domain, as described in the "Customizing the Primary Location" section on page 2-37.
3. The automated attendant search scope on each server must be set to the dialing domain as described in the "Setting the Automated Attendant Search Scope" section on page 2-37.
4. Identified subscriber messaging on each server must be enabled as described in the "To Enable Identified Subscriber Messaging" section on page 2-38.
5. Identified subscriber messaging on each server must be extended to include Bridge subscribers as described in the "To Extend Identified Messaging" section on page 2-38.

Single-Server Installations

In installations with only one Cisco Unity server, enabling ISM to include Bridge subscribers requires the following:

1. The server must be configured with a dialing domain name, as described in the "Customizing the Primary Location" section on page 2-37.

2. Identified subscriber messaging must be enabled as described in the "To Enable Identified Subscriber Messaging" section on page 2-38.
3. Identified subscriber messaging must be enabled for Bridge subscribers as described in the "To Extend Identified Messaging" section on page 2-38.

Customizing the Primary Location

If your installation consists of multiple Cisco Unity servers networked via Digital Networking, you may have already customized the primary location.

For detailed information about the settings, see the "Primary Location Profile Settings" section on page 9-1.

To Customize the Primary Location

Step 1 In the Cisco Unity Administrator, go to the **Network > Primary Location > Profile** page.

Step 2 Enter a meaningful name for the location.

Step 3 Enter a Dial ID. The Dial ID identifies this location to Cisco Unity.

Step 4 Record a voice name for the location.

Step 5 For the Dialing Domain name:

- If your installation consists of only one Cisco Unity server, and if you plan to enable identified subscriber messaging to include Bridge subscribers, enter a dialing domain name.
- If your installation consists of multiple Cisco Unity servers networked via Digital Networking, and if this server is integrated with the same phone system as other networked Cisco Unity servers, you may have already added this server to a dialing domain. If not, enter the dialing domain name, or select it from the available list. The list contains names of dialing domain names already configured on at least one other Cisco Unity server in the network.

  Note that the dialing domain name is case sensitive and must be entered exactly the same on all of the servers. To ensure that all servers are correctly added to the same dialing domain, enter the dialing domain name on one Cisco Unity server and wait for the name to replicate to the other Cisco Unity servers. By doing so, you also confirm that replication is working correctly among the servers. The time that it takes for the primary location data from other Cisco Unity servers to be reflected on the local server depends on your network configuration and replication schedule.

Step 6 Click the **Save** icon.

Setting the Automated Attendant Search Scope

If your installation consists of multiple Cisco Unity servers networked via Digital Networking, the auto attendant search scope must be set

To Set the Automated Attendant Search Scope

Step 1 On the Cisco Unity 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 **Networking—Set Auto Attendant Search Scope**.

Step 4 In the New Value list, click **1**, and then click **Set** so that Cisco Unity searches for subscribers within the dialing domain.

Step 5 When prompted, click **OK**.

You do not need to restart Cisco Unity to enable the change.

Step 6 Click **Exit**.

Enabling Identified Subscriber Messaging

Note If the system is using failover, you must make this change on both the primary and secondary servers because the setting is stored in the registry.

To Enable Identified Subscriber Messaging

Step 1 In the Cisco Unity Administrator, go to the **System > Configuration Settings** page.

Step 2 In the Identified Subscriber Messaging section, uncheck the **Subscribers Are Identified as Message Senders Only if They Log On** check box.

Identified subscriber messaging for subscribers on the same Cisco Unity server is enabled when the check box is unchecked. By default, the box is unchecked.

Step 3 Click the **Save** icon.

Extending Identified Subscriber Messaging

After identified subscriber messaging has been enabled, you must extend it to include Bridge subscribers.

To Extend Identified Messaging

Step 1 On the Cisco Unity 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 **Networking – Enable Identified Subscriber Messaging (ISM) for AMIS, Bridge, and VPIM Subscribers**.

Step 4 In the **New Value** list, click **1**, then click **Set**.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

Step 7 Restart Cisco Unity for the registry setting to take effect.

Enabling the Bridge Server to Send Extended-Absence Delivery Receipts

For Cisco Unity subscribers to receive delivery receipts, when the extended-absence greeting for an Octel subscriber is enabled and the mailbox is accepting messages, you need to modify a configuration setting on the Bridge server. See one of the following procedures as applicable for your version of the Bridge:

- To Enable the Bridge to Send Extended-Absence Delivery Receipts (Cisco Unity Bridge 3.0(6)), page 2-39
- To Enable the Bridge to Send Extended-Absence Delivery Receipts (Cisco Unity Bridge 3.0(5)), page 2-39

To Enable the Bridge to Send Extended-Absence Delivery Receipts (Cisco Unity Bridge 3.0(6))

Step 1 On the Configuration Menu in the Bridge Administrator, click **Digital Networking**.

Step 2 Check the **Enable Extended Absence Notifications** check box.

Step 3 Click **Save**.

To Enable the Bridge to Send Extended-Absence Delivery Receipts (Cisco Unity Bridge 3.0(5))

Step 1 On the Bridge server, make a backup copy of the file **<Bridge Path>\Vpim\Vpim.cfg**.

Step 2 Open the file **<Bridge Path>\Vpim\Vpim.cfg** with Notepad.

Step 3 Search for **EnableExtAbsenceNotifications**. You should see text similar to:

```
[config]
POP3_SERVER_ID=
ESMTP_SERVER_ID=
InetRecvProtocol=1
POP3_POLL_INTERVAL_MS=600000
OUTDIAL_INTERVAL_MS=600000
CALLX_IN_POLL_INTERVAL_MS=30000
PROXY_MAILBOX_MESSAGE=IMCEAOMNI-AvVoiceMessage
PROXY_MAILBOX_DIRECTORY=IMCEAOMNI-AvVoiceAddress
EnableExtAbsenceNotifications=0
SMTP_PORT=25
```

Step 4 Go to the line containing **EnableExtAbsenceNotifications=0**, and change the **0** to a **1**.

Step 5 Save and close the file.

Step 6 Restart the Digital Networking service for the setting to take effect:

a. On the Windows Start menu, click **Programs > Administrative Tools > Services**.

b. In the right pane, right-click **Digital Networking**, and click **Restart**.

c. Close the Services console.

Enabling the Bridge to Accept Requests to Push Mailbox Information (Bridge 3.0(6) and Later)

Some remote systems provide the capability to push name information to other nodes; version 3.0(6) of the Bridge provides the capability to accept this mailbox information and use it to update the Bridge directory and the Bridge subscriber directory in Cisco Unity.

By default, the Bridge will reject an attempt by the remote node to push mailbox information (but the call will proceed and the remote node will be able to continue with any additional tasks). When the accept remote push functionality is enabled, the Bridge will accept all administrative name push requests from any remote node, and will process the directory information even if the recorded voice name is not included in the transmission. If the mailbox information sent by the remote node does not match any existing mailbox in the Bridge directory, a new usage-based entry is added to the directory. If the information pertains to a mailbox that already exists in the Bridge directory, the Bridge will modify the directory entry; if the text name is blank or no recorded name is transmitted, the corresponding field will be removed from the directory entry.

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

To Enable the Bridge to Accept Requests to Push Mailbox Information

Step 1 On the Configuration Menu in the Bridge Administrator, click **System Settings**.

Step 2 Check the **Accept Remote Push** check box.

Step 3 Click **Save**.