Cisco Unity Bridge Networking Guide (With IBM Lotus Domino)

Cisco Unity Bridge, Release 3.0
May 6, 2005

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7399-01

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

Preface i

Purpose i

Audience i

Documentation Conventions i

Cisco Unity Documentation ii

Obtaining Documentation ii

Cisco.com ii

Ordering Documentation iii

Documentation Feedback iii

Obtaining Technical Assistance iii

Cisco Technical Support Website iii

Submitting a Service Request iv

Definitions of Service Request Severity iv

Obtaining Additional Publications and Information v

CHAPTER 1 **About Bridge Networking** 1-1

New and Changed Functionality—Cisco Unity 4.0(5) 1-1

Acceptance of Requests to Push Mailbox Information to the Bridge (Bridge 3.0(6) and Later) 1-2

Enable Extended Absence Notification Setting Added to the Bridge Administrator (Bridge 3.0(6) and Later) 1-2

Retrieving or Confirming Octel Serial Numbers (Bridge 3.0(6) and Later) 1-3

Silence Detection and Trimming for Audio Received From Remote Systems (Bridge 3.0(6) and Later) 1-3

Cisco Unity with Domino Supported for Bridge Networking (Bridge 3.0(5) and Later) 1-3

Overview of Bridge Networking 1-3

Messaging Between the Bridge and Cisco Unity 1-4

Messaging Between the Bridge and Octel 1-5

Bridgehead Server 1-6

Nodes on the Octel Analog Network 1-7

How Nodes Are Represented on the Bridge Server 1-7

How Octel Nodes Are Represented on the Cisco Unity Bridgehead Server 1-8

How Unity Nodes Are Represented in Cisco Unity 1-9

Directory Information Sharing 1-10

Bridge Participation in NameNet 1-10

How Octel Node Directory Entries Are Represented in Cisco Unity 1-11
UOmni Account 1-12
Directory Synchronization of the Cisco Unity and Bridge Directories 1-12
Maintaining the Logical Octel Network Topology Within the Cisco Unity Directory 1-13
Retaining the Octel Network Identity 1-14
Independent Numbering Plans 1-14
Collapsing Multiple Octel Nodes 1-15
Interop Gateway and Bridge Networking 1-15
Message Addressing Options 1-16
Messaging Similarities and Limitations 1-16
Blind Addressing and Bridge Networking 1-17
Bridge Subscribers 1-18
How Bridge Subscribers Are Created 1-19
Creating Bridge Subscribers in Cisco Unity 1-19
Creating Permanent Directory Entries on the Bridge Server 1-19
Creating Bridge Subscribers and Then Creating Corresponding Permanent Directory Entries 1-20
Extension Addresses 1-20
Subscriber Experience with Bridge Subscribers 1-21
Identified Subscriber Messaging (Cisco Unity 4.0(4) or Later) 1-21
Live Reply to Bridge Subscribers (Cisco Unity 4.0(4) and Later) 1-22
Deleting Bridge Subscribers 1-22
Disabling the Automatic Creation, Modification, and Deletion of Bridge Subscribers 1-23
Controlling How Text Names Are Parsed for Auto-Created Bridge Subscribers 1-24
Determining How Bridge Subscribers Appear in the Notes Address Book 1-24
Controlling the Extensions Assigned to Auto-Created Bridge Subscribers 1-25
Preventing Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant 1-25
Supported Codecs 1-26
Notable Behavior 1-26
Call Transfer Settings and Bridge Subscribers 1-27
Directory Lookups of Asian and European Names May Fail 1-28
Distribution Lists 1-28
Inbound Search Scope 1-29
Some Messages to Cisco Unity Are Delayed 1-29
Automatic Gain Control Applied to Messages Sent from the Bridge to Cisco Unity (Bridge 3.0(5) and Later) 1-29
Cisco Unity Subscribers Receive Extended-Absence Notification from Octel Servers (Cisco Unity 4.0(4) and Later) 1-29
Additional Bridge-Related Documentation 1-30

CHAPTER 2 **Setting Up Cisco Unity and the Bridge for Networking** 2-1

Prerequisites 2-1

Task List: Setting Up Cisco Unity and the Bridge for Networking 2-2

Making Design Decisions and Gathering Needed Information 2-4

Determining the Domain Name 2-5

Optional: Gathering or Confirming Octel Node Serial Numbers (Bridge 3.0(6) or Later) 2-5

Preparing the Network 2-6

Resolving Names and IP Addresses 2-6

Configuring the Interop Gateway 2-7

Configuring the Cisco Unity Server Designated as the Bridgehead 2-9

Designating the Bridgehead Server 2-9

Setting Bridge Options 2-10

Configuring the Subscriber Template That Will Be Used for Auto-Created Bridge Subscribers 2-10

Creating and Configuring Bridge Delivery Locations 2-11

Creating New or Modifying Existing Subscriber Accounts for Testing Purposes 2-14

Configuring the Bridge Server 2-15

Configuring the Bridge and Testing the Configuration 2-15

Configuring the Octel Servers 2-22

Testing the Octel Analog Network 2-22

Testing the Setup 2-24

Finishing the Setup 2-25

Finishing the Creation and Configuration of Bridge Delivery Locations 2-25

Adding the Serial Number and Mailbox ID to Cisco Unity Subscriber Accounts 2-25

Setting the Serial Number and Mailbox ID for Unidentified Callers 2-27

Creating Bridge Subscriber Accounts 2-27

Extending Identified Subscriber Messaging to Include Bridge Subscribers 2-36

Enabling the Bridge Server to Send Extended-Absence Delivery Receipts 2-39

Enabling the Bridge to Accept Requests to Push Mailbox Information (Bridge 3.0(6) and Later) 2-40

CHAPTER 3 **Monitoring and Maintaining Bridge Networking** 3-1

Controlling the Number of Ports Used for Outgoing Messages 3-1

Determining Optimal Values for Queued Call Threshold and Max Ports Per Node 3-2

Bridge Analog Network and Node Analyzer (BANANA) 3-3

Getting Started Using the BANANA admin to Monitor Analog Activity 3-4

Bridge Traffic Analyzer 3-5

Backing Up and Restoring a Bridge Server 3-6

Backing Up the Bridge Server 3-6

Replacing a Bridge Server and Restoring Data 3-7

Changing the Interop Gateway Foreign Domain Name 3-9
Moving the Interop Gateway Mail File 3-11
Moving the UOmni Mail File 3-12
Monitoring Recommendations 3-12

CHAPTER 4 **Troubleshooting Bridge Networking** 4-1
Overview: Bridge Troubleshooting 4-1
Configuration Problems 4-1
Procedures for Troubleshooting Configuration Problems 4-3
Overview of Troubleshooting Logs, Traces, and Tools 4-4
Tools for Troubleshooting Communication Problems Between the Bridge and the Octel Nodes 4-4
Tools for Troubleshooting Communication Problems Between the Bridge and Cisco Unity 4-5
Tools for Troubleshooting Problems with the Interop Gateway 4-6
Tools for Troubleshooting Directory Synchronization Problems on the Cisco Unity Server 4-6
Messages Are Not Delivered from Cisco Unity to Octel 4-7
Troubleshooting Why Messages Are Not Delivered from Cisco Unity to Octel 4-9
Enabling Logs and Traces 4-10
Do Messages from Cisco Unity Get to the Bridge? 4-11
Are Outbound Calls Attempted? 4-12
Troubleshooting Why Outbound Calls Are Failing 4-14
Are Outbound Messages Routed to the Interop Gateway Mail File? 4-19
After You Finish Troubleshooting 4-23
Messages Are Not Delivered from Octel to Cisco Unity 4-24
Bridge In and Out Directories 4-25
Troubleshooting Why Messages Are Not Delivered from Octel to Cisco Unity 4-26
Enabling Logs and Traces 4-27
Does the Bridge Receive Inbound Calls? 4-29
Are Inbound Calls Failing? 4-31
Are Inbound Messages Routed to the Domino Network? 4-37
Are Inbound Messages Routed to the Interop Gateway Mail File? 4-39
After You Finish Troubleshooting 4-41
Directory Messages Are Not Processed 4-42
CsBridgeConnector Traces 4-44
Full Synchronization of Bridge Subscribers with Octel Node Directories 4-45
Full Synchronization of Cisco Unity Subscribers with the Unity Node Directories 4-46

CHAPTER 5 **Advanced Troubleshooting Topics** 5-1
Enabling and Interpreting Traces for the Brooktrout TR114 on the Bridge 5-1

Enabling Debug Traces for the Brooktrout TR114 5-1
Disabling Debug Traces for the Brooktrout TR114 5-2
Interpreting Debug Traces for the Brooktrout TR114 5-2
Using the Call Traces to Troubleshoot Why Messages Are Not Delivered from the Bridge to the Octels 5-14
Are Calls Attempted? 5-14
Are Dialouts Successful? 5-16
Are Handshakes Successful? 5-17
Are Any Messages Transmitted Successfully? 5-18
Using the Call Traces to Troubleshoot Why Messages Are Not Delivered from the Octel Node to the Bridge Server 5-19
BANANA admin Call States, and Reasons for Communication Errors 5-21
Bridge Compensates for Echoed Digits in Wakeup Packets 5-23

CHAPTER 6 **Uninstalling Bridge Networking Components** 6-1
Overview 6-1
Completely Removing Bridge Networking 6-1
Making Another Cisco Unity Server the Bridgehead 6-2
Uninstalling the Bridge Software from the Bridge Server 6-5

CHAPTER 7 **Reference: Bridge Settings on the Cisco Unity Server** 7-1
Bridge Delivery Locations Profile Settings 7-1
Bridge Delivery Locations Prefixes 7-4
Bridge Delivery Locations Subscriber Creation Settings 7-5
Bridge Options Subscriber Creation Settings 7-6
Bridge Options Synchronization Settings 7-7
Bridge Options Unknown Caller Settings 7-9

CHAPTER 8 **Reference: Settings on the Bridge Server** 8-1
System Settings 8-1
Digital Networking 8-6
Unity Nodes 8-9
Unity Node Configuration 8-10
Octel Nodes 8-12
Octel Node Configuration 8-12
Directory List 8-14
Directory Entry 8-15
Line Status 8-16

Queue Status 8-18

CHAPTER 9 **Primary Location Settings 9-1**

Overview: Primary Location Settings 9-1

Primary Location Profile Settings 9-1

Assigning Dial IDs 9-1

Primary Location Addressing Option Settings 9-5

Subscriber Addressing Options 9-6

Location Addressing Options Settings 9-12

GLOSSARY

INDEX

Preface

This preface describes the purpose, audience, and conventions of the *Cisco Unity Bridge Networking Guide*, and provides information on how to obtain related documentation.

Purpose

The *Cisco Unity Bridge Networking Guide* contains detailed discussions of and instructions for configuring, maintaining, and troubleshooting Bridge Networking on Cisco Unity and the Cisco Unity Bridge.

The *Cisco Unity Bridge Networking Guide* focuses on Cisco Unity. It does not provide information on Microsoft Exchange, Microsoft Windows 2000, IBM Lotus Domino, or on configuring other voice messaging systems.

Audience

The *Cisco Unity Bridge Networking Guide* is intended for system administrators and others responsible for setting up and managing Cisco Unity and the Cisco Unity Bridge. You need a working knowledge of Exchange and Windows NT/2000, and of the message store (Domino, Exchange 2000, Exchange 2003, or Exchange 5.5) in which voice messages are stored, as well as a working knowledge of Octel analog networking and the Octel voice messaging system with which Cisco Unity will network.

Documentation Conventions

Table 1 Cisco Unity Bridge Networking Guide Conventions

Convention	Description
boldfaced text	Boldfaced text is used for: • Key and button names. (Example: Click **OK.**) • Information that you enter. (Example: Enter **Administrator** in the User Name box.)
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter **ping <IP address>**.)

Table 1 Cisco Unity Bridge Networking Guide Conventions (continued)

Convention	Description
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press **Ctrl-Alt-Delete.)**
> (right angle bracket)	A right angle bracket is used to separate selections that you make: • On menus. (Example: On the Windows Start menu, click **Settings > Control Panel > Phone and Modem Options**.) • In the navigation bar of the Cisco Unity Administrator. (Example: Go to the **System > Configuration > Settings** page.)

The *Cisco Unity Bridge Networking Guide* also uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Cisco Unity Documentation

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

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

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

  http://www.cisco.com/ipj

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

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

About Bridge Networking

The Cisco Unity Bridge acts as a networking gateway between Cisco Unity and Avaya Octel systems or Avaya Interchange, which are on an Octel analog network. With the Bridge, Cisco Unity subscribers can send messages to and receive messages from Octel subscribers.

This chapter explains how networking with the Bridge works, and describes the various Cisco Unity components involved with Bridge Networking. See the following sections for more information:

- New and Changed Functionality—Cisco Unity 4.0(5), page 1-1
- Overview of Bridge Networking, page 1-3
- Nodes on the Octel Analog Network, page 1-7
- Directory Information Sharing, page 1-10
- Maintaining the Logical Octel Network Topology Within the Cisco Unity Directory, page 1-13
- Message Addressing Options, page 1-16
- Blind Addressing and Bridge Networking, page 1-17
- Bridge Subscribers, page 1-18
- Supported Codecs, page 1-26
- Notable Behavior, page 1-26
- Additional Bridge-Related Documentation, page 1-30

Detailed information about Bridge Networking settings in Cisco Unity and the Cisco Unity Bridge can be found in the following chapters: "Reference: Bridge Settings on the Cisco Unity Server," "Reference: Settings on the Bridge Server," and "Primary Location Settings."

New and Changed Functionality—Cisco Unity 4.0(5)

This section provides information about the new and changed functionality introduced in Cisco Unity 4.0(5) that is related to Bridge Networking. For information about new and changed functionality for all of Cisco Unity, refer to the *Release Notes for Cisco Unity Release 4.0(5)*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/relnote/cu405rn.htm.

See the following sections:

- Acceptance of Requests to Push Mailbox Information to the Bridge (Bridge 3.0(6) and Later), page 1-2
- Enable Extended Absence Notification Setting Added to the Bridge Administrator (Bridge 3.0(6) and Later), page 1-2

- Retrieving or Confirming Octel Serial Numbers (Bridge 3.0(6) and Later), page 1-3
- Silence Detection and Trimming for Audio Received From Remote Systems (Bridge 3.0(6) and Later), page 1-3
- Cisco Unity with Domino Supported for Bridge Networking (Bridge 3.0(5) and Later), page 1-3

Acceptance of Requests to Push Mailbox Information to the Bridge (Bridge 3.0(6) and Later)

By default, the Bridge will attempt to retrieve name information for remote Octel subscribers when needed. Some remote systems may also provide the capability to push name information to other nodes; version 3.0(6) of the Bridge provides the capability to accept this mailbox information and update the Bridge directory and the Bridge subscriber directory in Cisco Unity.

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

When the Accept Remote Push check box is checked, the Bridge will accept all administrative name push requests from any remote node, and will process the directory information even if the recorded voice name is not included in the transmission. If the mailbox information sent by the remote node does not match an 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.

Before enabling this feature, you should be familiar with the voice messaging system models, versions, and configuration, and with the 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.

Enable Extended Absence Notification Setting Added to the Bridge Administrator (Bridge 3.0(6) and Later)

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

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

Retrieving or Confirming Octel Serial Numbers (Bridge 3.0(6) and Later)

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

The utility is located in the <Bridge>\Starfish\bin directory, and it must be run from this directory. You must stop the Unity Bridge service prior to running the utility. To get the serial number of an Octel system, run GetSN and specify the phone number for the system on the command line. Commas can be used in the dial string to specify a pause. For example, GetSN 9,5552900.

Silence Detection and Trimming for Audio Received From Remote Systems (Bridge 3.0(6) and Later)

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

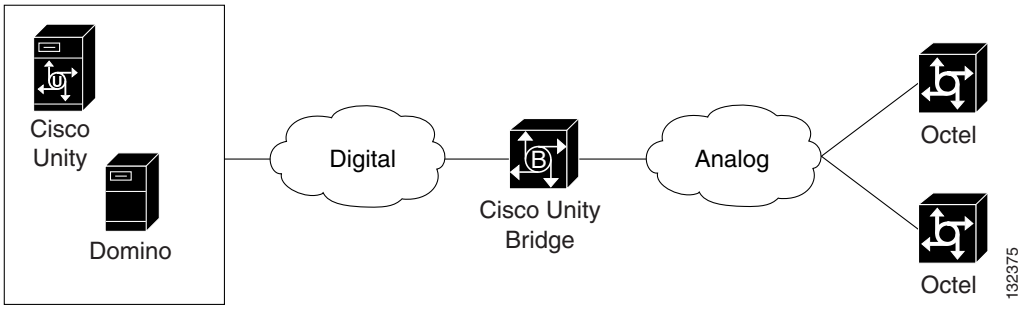
Cisco Unity with Domino Supported for Bridge Networking (Bridge 3.0(5) and Later)

Cisco Unity 4.0(5) and later with IBM Lotus Domino is supported for networking with Cisco Unity Bridge version 3.0(5) and later.

Overview of Bridge Networking

The Cisco Unity Bridge acts as a networking gateway between Cisco Unity and Avaya Octel systems or Avaya Interchange on an Octel analog network. The Bridge server is connected to a phone system and communicates with Octel servers by using the Octel analog networking protocol. The Bridge server sends messages to Cisco Unity by using a digital protocol that is based on the Voice Profile for Internet Mail (VPIM) protocol, with proprietary extensions. The Bridge must be installed on a separate and dedicated platform, and it can communicate with up to 998 Octel servers. Figure 1-1 depicts—at a high level—the role of the Bridge server.

Figure 1-1 Bridge Communication Is Digital with Cisco Unity, and Analog with the Octel Servers



See the following sections for additional information:

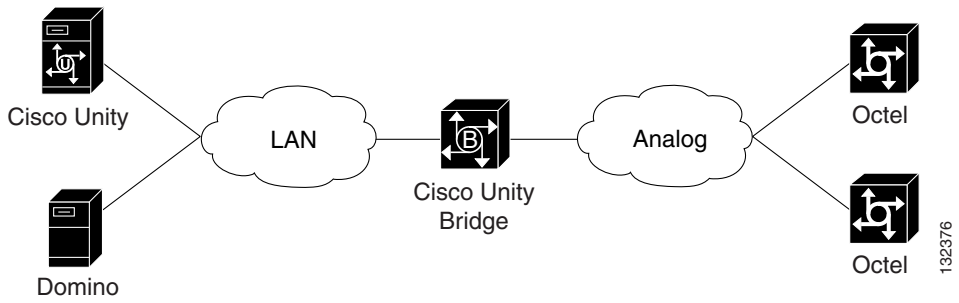
- Messaging Between the Bridge and Cisco Unity, page 1-4
- Messaging Between the Bridge and Octel, page 1-5
- Bridgehead Server, page 1-6

Messaging Between the Bridge and Cisco Unity

Messaging between the Bridge and Cisco Unity is done over the Internet or any TCP/IP network by using SMTP. The Bridge sends messages to an SMTP server that you specify when configuring the Bridge server. (The SMTP server may be a Domino server or another server configured to relay SMTP messages.) The SMTP server then routes messages to Domino, which delivers messages to recipient mail files.

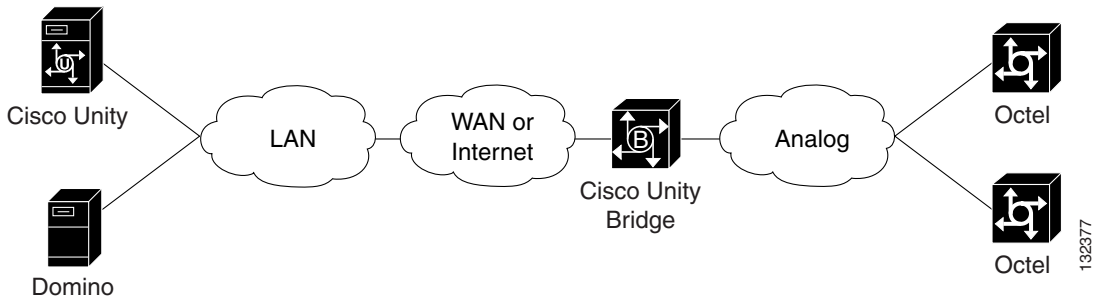
The Bridge server can be connected to the same LAN that Cisco Unity and Domino are connected to, as depicted in Figure 1-2.

Figure 1-2 Bridge Server Can Be on the Same LAN as Cisco Unity and Domino



However, as Figure 1-3 illustrates, the Bridge server can be located in a different location from Cisco Unity and Domino, in which case messages are sent through the Internet or a WAN.

Figure 1-3 Bridge Server Can Be Located in a Different Location



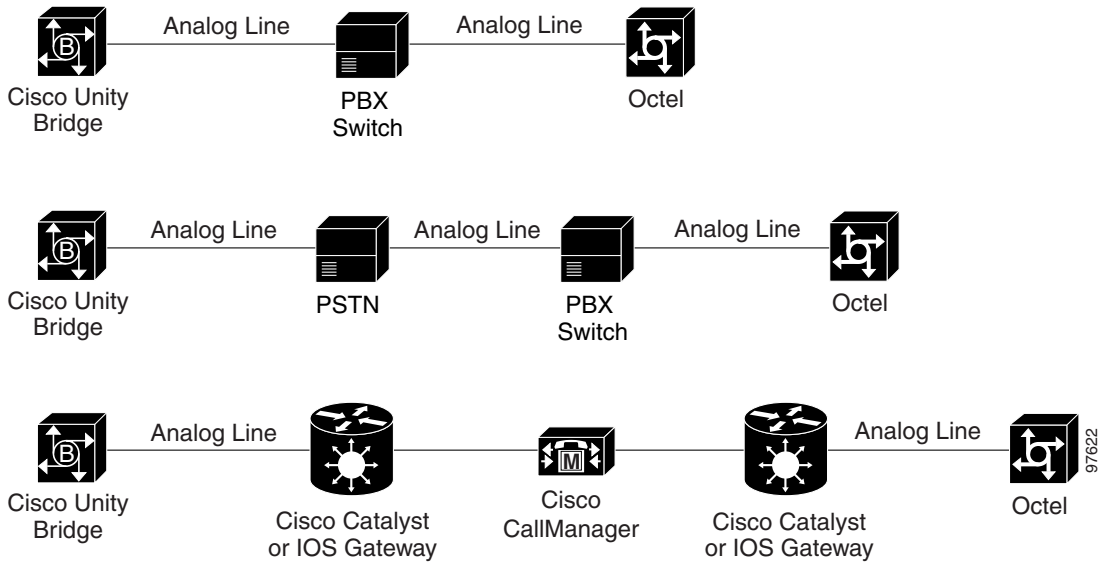
Messaging Between the Bridge and Octel

Messaging between the Bridge and the Octel servers is done via Octel analog networking. The Bridge masquerades as one or more nodes on the Octel analog network. Voice messages are transmitted between nodes by using ordinary phone connections. When one node calls another by dialing a specified phone number, the originating node transmits a sequence of DTMF tones to identify itself as an Octel node. The destination node then transmits DTMF tones in reply. If the destination node accepts the call, the originating node transmits each voice message by using analog playback, and the destination node records each message and delivers it. To the Octel servers, the Bridge behaves like any other Octel node on the Octel analog network.

Connecting the Bridge Server to the Phone System

The Bridge server needs to place phone calls to, and receive phone calls from, all Octel servers with which it will communicate. The Bridge server contains voice-fax cards that are connected to a phone system. The Bridge analog ports have no relation to the voice ports on the Cisco Unity system. In fact, the Bridge may or may not use the same phone system as Cisco Unity or the Octel servers. The only requirement for the Bridge ports is that they be provided with an analog dial tone from a source that allows connection to the phone number(s) of the Octel server(s) with which the Bridge will communicate. Figure 1-4 illustrates some of the methods for providing analog connectivity to the Bridge server.

Figure 1-4 Methods for Providing Analog Connectivity to the Bridge Server



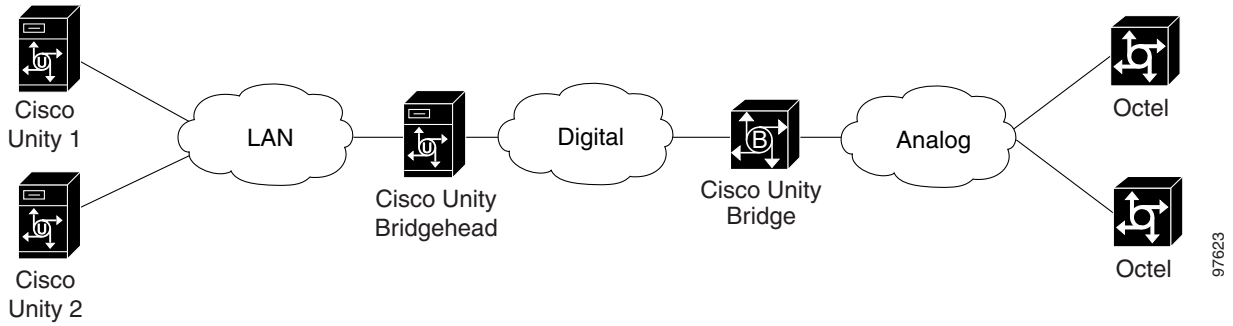
The voice-fax cards in the Bridge server are an FXO interface. If the Bridge will place and receive phone calls via a Cisco CallManager phone system, an FXS card in an IP gateway is required. Supported Cisco IP gateways for use with the Bridge are listed in the "Supported Cisco Gateways" section of the *Cisco Unity Bridge System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm.

The phone system to which the Bridge connects must be configured with a phone number, known as the pilot number, to direct inbound calls to any available line on the Bridge. When more than one Bridge is deployed, each Bridge must have its own pilot number.

Bridgehead Server

In installations with multiple Cisco Unity servers digitally networked together, only one Cisco Unity server in the network needs to be configured for networking with the Bridge. This server acts as the "bridgehead" server for the other Cisco Unity servers in the network, as Figure 1-5 illustrates. If allowed by the primary location addressing options, all subscribers, no matter which Cisco Unity server they are associated with, can send messages to Octel subscribers.

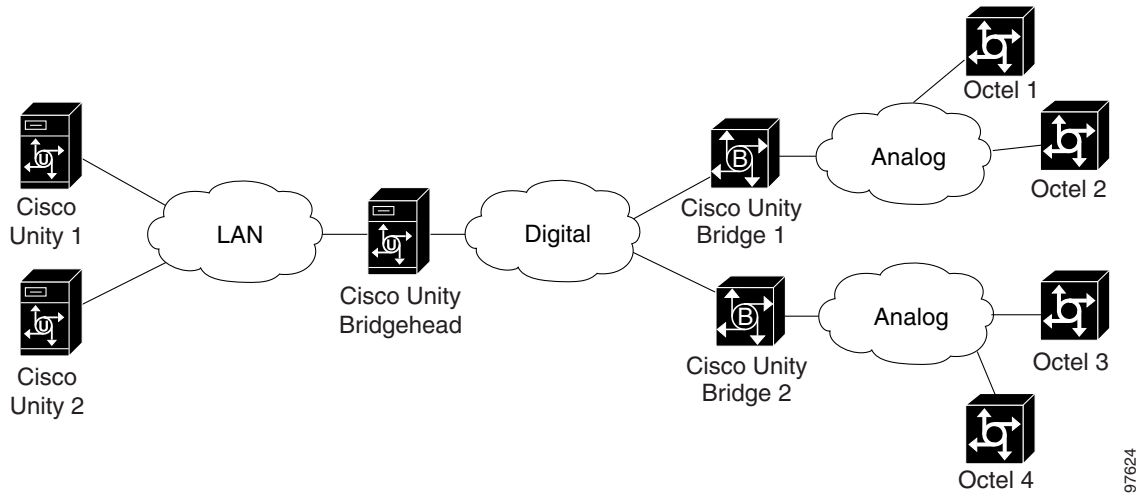
Figure 1-5 Cisco Unity Bridgehead Server



Because the analog transmission of messages to the Octel servers is much slower than digital transmission to Cisco Unity, the bridgehead server can be configured for networking with additional Bridge servers, as needed, to provide sufficient analog ports for messaging with the Octel servers.

For installations with more than one Bridge server, each Bridge server is configured for messaging with a subset of the Octel servers. For example, Figure 1-6 illustrates an installation where Bridge 1 is configured for messaging with Octel 1 and Octel 2, and Bridge 2 is configured for messaging with Octel 3 and Octel 4.

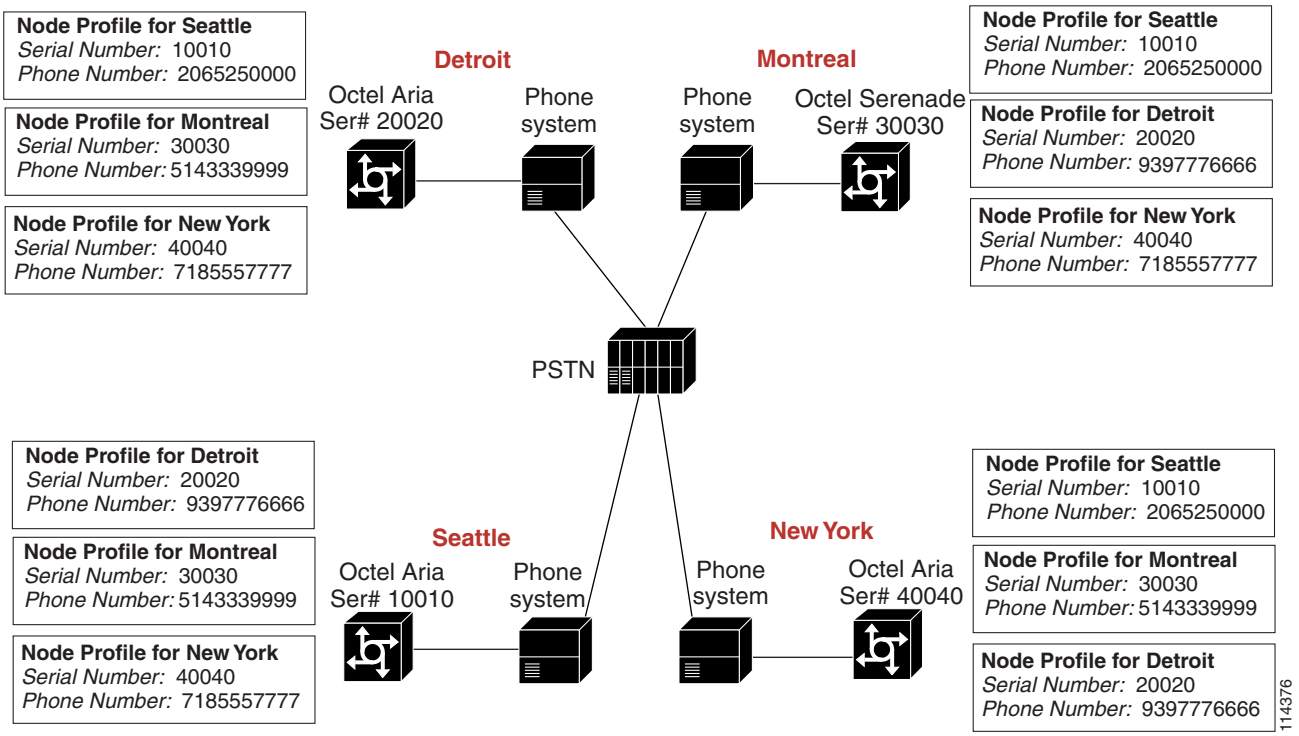
Figure 1-6 One Bridgehead Server Can Communicate with Multiple Bridge Servers



Nodes on the Octel Analog Network

Each Octel server represents a node in the Octel analog network. In Octel analog networking, each node is assigned a unique serial number, which identifies the node. As Figure 1-7 illustrates, each Octel server is configured with a node profile—which includes the serial number and phone number—for every other node in the network.

Figure 1-7 Octel Nodes in the Network



The Bridge and Cisco Unity bridgehead servers can represent one or more nodes in the network. Both the Bridge and Cisco Unity bridgehead servers must be configured with information about the other Octel nodes. The Bridge and Cisco Unity bridgehead servers must also be configured with information that identifies the nodes that they represent.

See the following sections for additional information:

- How Nodes Are Represented on the Bridge Server, page 1-7
- How Octel Nodes Are Represented on the Cisco Unity Bridgehead Server, page 1-8
- How Unity Nodes Are Represented in Cisco Unity, page 1-9

How Nodes Are Represented on the Bridge Server

The Bridge server contains a database in which information about every node in the network is stored. On the Bridge server, you add an Octel Node object for each node with which the Bridge communicates. The Octel Node object contains the Octel server name, unique serial number, and phone number. You also define a schedule that controls when messages are sent to the node from the Bridge.

If there are multiple Bridge servers, the Octel nodes are divided among the Bridge servers, as shown in Figure 1-6.

A Cisco Unity bridgehead server combined with a Bridge server (or servers) can represent the serial number of each Octel server whose subscribers have migrated to Cisco Unity. Up to 998 nodes can be represented. On the Bridge server, you add a Unity Node object for each node that the Cisco Unity bridgehead and Bridge servers represent in the network. The Unity Node object contains the serial number and other information needed for routing messages between the Octel and Cisco Unity servers.

By using the information that you supply, the Bridge server can receive a message from an Octel node, look up the routing information from the Unity node table, reformat the message for the destination Unity node, and then send the message to the Unity node. A message coming from a Unity node and going to an Octel node goes through a similar process, but this time the Bridge server uses the Octel node table to find the routing information.

How Octel Nodes Are Represented on the Cisco Unity Bridgehead Server

Octel nodes correspond to Bridge delivery locations in Cisco Unity. A Bridge delivery location contains a dial ID (which Cisco Unity uses as an identifier), the serial number of the corresponding Octel node, and other information that Cisco Unity needs to send messages to and receive messages from the Octel node via the Bridge. When setting up Bridge Networking, you create a delivery location to correspond to each Octel node with which Cisco Unity will communicate. You create the delivery locations by using the Cisco Unity Administrator.

In organizations with multiple Cisco Unity servers networked together, the delivery locations should be created only on the Cisco Unity bridgehead server.

Mailbox Lengths and Prefixes

When you create a Bridge delivery location, you must specify a mailbox length. In most cases, the mailbox numbers of subscribers on an Octel server all have the same length. However, an Octel server can be configured to support different mailbox lengths. In this case, you create multiple delivery locations for the same Octel node and specify a different mailbox length on each location. For example, assume that an Octel server is configured such that some subscribers have 4-digit mailboxes and some have 5-digit mailboxes. When configuring Cisco Unity, you create two delivery locations for the same Octel node; on one location you specify a mailbox length of 4, and on the other, you specify a mailbox length of 5. Note, however, that you create only one Octel node on the Bridge server.

When Octel subscribers send messages to subscribers on other nodes in the Octel analog network, they enter a network address as the message destination. A network address consists of a node prefix, which identifies the remote server, and the mailbox number of the recipient. In many cases, the prefix is identical either to the area code where the destination node is located, or the prefix(es) defined in the phone system dialing plan. This allows subscribers to use the same number when addressing a network message that they use when calling directly. As needed to accommodate the Octel numbering plan, you can specify a prefix or prefixes for a Bridge delivery location. This allows Cisco Unity subscribers who have migrated from an Octel node to continue addressing messages to subscribers on other Octel nodes by using the same number that they used before they were migrated.

In Cisco Unity, prefixes are optional, depending on your numbering plan. Prefixes are not needed when Cisco Unity subscribers can send messages to Octel subscribers by entering the dial ID of the location followed by the recipient mailbox number. For example, assume that an Octel node has 4-digit mailboxes, and subscribers on other nodes in the Octel network enter 425xxxx when sending messages to the node. In Cisco Unity, you can create a delivery location with 425 as the dial ID and no prefix is needed.

A prefix may or may not overlap with digits in a remote mailbox number. If you specify a prefix (or prefixes) for the location, the value that you entered for the remote mailbox length is used to determine the recipient mailbox number. For example, assume that a delivery location has been defined with the following values:

Dial ID = 504
Prefix = 256
Remote Mailbox Length = 5

Also assume that there is an Octel subscriber with the mailbox 63452 on the Octel node that corresponds to the above delivery location, and that the Octel node has only 5-digit mailboxes.

1. A subscriber logs on to Cisco Unity and sends a message to the Octel subscriber by entering 2563452. Cisco Unity searches the directory and does not find a matching subscriber extension. Cisco Unity parses the number and finds a delivery location with the prefix 256. Because the subscriber entered a prefix, Cisco Unity uses the remote mailbox length to determine the mailbox number from the entered number: 25**63452**. To determine the mailbox number, Cisco Unity starts at the end of the entered number, and keeps including digits until the number of digits equals the remote mailbox length. In this example, the last digit in the prefix overlaps with the first digit of the mailbox number, but the remote mailbox length allows Cisco Unity to correctly determine the mailbox number of the recipient so that the message will be delivered.
2. A subscriber logs on to Cisco Unity and sends a message to the Octel subscriber by entering 5043452. Cisco Unity searches the directory and does not find a matching subscriber extension. Cisco Unity parses the number and finds a delivery location with a dial ID of 504. In this case the remote mailbox length is ignored because the match was on the dial ID, and not the prefix. Cisco Unity determines that the mailbox number is the remaining digits of the entered number after the dial ID, 504**3452**. Because 4-digit mailboxes are not allowed on the Octel node, the message will be returned to the sender with a non-delivery receipt.

How Unity Nodes Are Represented in Cisco Unity

The serial numbers of the nodes in the Octel analog network that the Cisco Unity bridgehead and Bridge servers represent are configured for Cisco Unity subscribers (and not for locations). Each Cisco Unity subscriber is configured with the serial number that represents a node in the Octel network together with the legacy mailbox ID of the subscriber, which identifies the subscriber in the Octel network. Combined, these numbers form a unique identifier for each subscriber. For each serial number that you configure for a group of Cisco Unity subscribers, you create a corresponding Unity node on the Bridge server.

For example, assume that Octel servers with the serial numbers 5555 and 8888 have been removed, and that the Cisco Unity Bridge now represents those nodes in the Octel network. On the Bridge, you would create the nodes shown in Table 1-1.

Table 1-1 Unity Nodes on the Bridge Server

Node Name	Node Serial Number
Paris	5555
London	8888

In this example, you would then configure the subscriber accounts in Cisco Unity with the serial numbers and mailbox IDs shown in Table 1-2.

Table 1-2 Cisco Unity Subscribers

Cisco Unity Subscriber Name	Node Serial Number	Mailbox ID
Jean	5555	3042
Claude	5555	3043
Francois	5555	3044
William	8888	8295
Elizabeth	8888	8296

The unique identifier created for each subscriber is thus made up of the Node Serial Number and the Mailbox ID. For example, the Cisco Unity subscriber Jean, shown in Table 1-2, would have the unique identifier 55553042.

Directory Information Sharing

Octel analog networking provides a feature called NameNet, which allows subscribers to:

- Address messages to people at other nodes by spelling the recipient names.
- Hear recorded name confirmation when addressing a message to someone on another node.

To provide these features to subscribers, each node needs access to the text and voice name of subscribers on other nodes. Each Octel node has a permanent directory of the subscribers associated with the node. Each directory entry includes the subscriber name, extension, and recorded voice name. Additionally, each Octel node has another directory, called the NameNet directory, with entries containing the names, mailbox numbers, and voice names of subscribers on other nodes.

There are two types of directory entries in the NameNet directory:

- **Permanent**—Permanent entries remain in the NameNet directory after they have been added, unless explicitly deleted.
- **Usage-Based**—Usage-based entries remain in the NameNet directory temporarily, depending on the network message traffic to the entry.

See the following sections for additional information:

- Bridge Participation in NameNet, page 1-10
- How Octel Node Directory Entries Are Represented in Cisco Unity, page 1-11
- UOmni Account, page 1-12
- Directory Synchronization of the Cisco Unity and Bridge Directories, page 1-12

Bridge Participation in NameNet

The Bridge participates in NameNet as follows:

- The Bridge maintains a permanent directory of Cisco Unity subscribers for each configured Unity node. In the Bridge Administrator, you can view the directory entries from the Unity Node page.
- The Bridge maintains a NameNet directory of Octel subscribers for each configured Octel node. In the Bridge Administrator, you can view the directory entries of each Octel node.

- The Bridge automatically adds usage-based directory entries to each Octel node directory.
- In the Bridge Administrator, the Name Aging field on the System Settings page allows you to specify how long usage-based directory entries are kept when they are not referenced. You can also disable name aging, so that the directory entries are permanent unless explicitly deleted.
- In the Bridge Administrator, you can add permanent directory entries to the Octel node directory.

Usage-Based Entries in NameNet

The first time any Cisco Unity subscriber sends a message to an Octel subscriber, the Bridge may not have an entry in its Octel node directory for the recipient. In this case, the Bridge sends the message, and in addition makes an administrative call to the destination Octel node to obtain the name and the recorded voice name of the Octel subscriber. The Bridge then adds a usage-based directory entry to the Octel node directory. If name aging is enabled, each time a message is sent to a usage-based entry, the aging counter for the entry is reset. If the Octel subscriber does not receive any messages within the specified period of time (the default is 30 days), the Bridge deletes the directory entry. If at a later date a Cisco Unity subscriber sends a message to an Octel user whose directory entry has been deleted, the process starts again.

In Cisco Unity Bridge version 3.0(6), the Bridge can also be configured to accept directory information that is sent by the remote Octel node in a ‘push’ request. 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 an existing usage-based entry in the Bridge directory, the Bridge modifies the directory entry and resets the aging counter.

Permanent Entries in NameNet

Permanent entries are not governed by the aging period. You can add new Octel node directory entries manually by using the Bridge Administrator or the Cisco Unity Bridge Mailbox Import tool. When a permanent directory entry is created, the Bridge node places an administrative call to the Octel node to obtain the name and recorded voice name. There are conditions under which a permanent entry will be deleted automatically, such as when the Bridge attempts message delivery to a mailbox and the Octel system indicates that the mailbox does not (or no longer) exists, or when a text name mismatch occurs (in which case the Bridge deletes the entry, makes a subsequent call to request the new name information, and then creates a new usage-based entry based on the information received).

If the Bridge is configured to accept ‘push’ requests, and new mailbox information that is sent by a remote Octel node in a ‘push’ pertains to an existing permanent entry, the text name and/or recorded voice name is updated, and the entry remains permanent.

For each Octel node, you define a schedule that controls when administrative calls to the node are made. Additionally, there are system-wide settings that allow you to control how often the Bridge attempts to retrieve spoken names that were not yet available when the text name was retrieved.

How Octel Node Directory Entries Are Represented in Cisco Unity

In Cisco Unity, Octel node directory entries are represented as Bridge subscribers. A Bridge subscriber is a representation in Cisco Unity of a subscriber on an Octel node. Bridge subscribers are created in Cisco Unity to enable regular Cisco Unity subscribers to find them in the directory and send messages to them as they would to any other subscriber. Each Bridge subscriber is associated with a delivery location and has a Domino Person document. Mailbox greetings and voice names can be individually recorded for each Bridge subscriber. Messages sent to a Bridge subscriber are sent through the Bridge server to the applicable mailbox on the Octel system. Bridge subscribers do not have messages stored locally; their messages are stored on the Octel messaging system.

After a directory entry (either usage-based or permanent) is added to an Octel node directory, the Bridge sends an Add User request to Cisco Unity to create a Bridge subscriber account. The Bridge sends a text name, mailbox number, and recorded voice name for Cisco Unity to use when it creates the Bridge subscriber. If configured to do so, Cisco Unity automatically creates a Bridge subscriber and a corresponding Person Document with the information provided by the Bridge.When the Bridge deletes a directory entry, it sends a Delete User request to Cisco Unity, and if configured to do so, Cisco Unity automatically deletes both the Bridge subscriber account and the Domino Person document.

You can also manually create Bridge subscribers in Cisco Unity by using the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard.

The Cisco Unity Administrator provides settings that allow you to control whether Cisco Unity should automatically create, modify, and delete Bridge subscribers. Additionally, there are settings based on delivery location that you can specify to control how extensions and names are generated for auto-created Bridge subscribers.

UOmni Account

Directory messages from the Bridge to create, modify, or delete Bridge subscribers are routed by the Interop Gateway to a special Domino mail file called UOmni_<Servername>. The Bridge Connector (a Cisco Unity component that runs as a Windows 2000 service called CsBridgeConnector) monitors the UOmni mail file. When the CsBridgeConnector detects a message, it parses the data in the message and sends a request to the Cisco Unity database component to make the necessary change (create, modify, or delete) to the Bridge subscriber account.

In organizations with multiple Cisco Unity servers networked together, the UOmni account needs to be created only on the Cisco Unity bridgehead server. The mail file for the UOmni account is located on the Domino server that was selected in the Message Store Configuration wizard during Cisco Unity setup.

The UOmni mail file can be moved and deleted just like any other Domino mail file, by using the Domino Administrator. Be sure to let everyone who administers Domino know about the UOmni account so that it is not moved or deleted by mistake.

For information on moving the UOmni mail file to another Domino server, refer to the “UOmni Mail File” section in the “Cisco Unity Data and Log Files” chapter in the *Cisco Unity Maintenance Guide*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/maint/maint405/dom/index.htm.

Directory Synchronization of the Cisco Unity and Bridge Directories

Cisco Unity keeps its subscriber directory synchronized with the subscriber directory on the Bridge. The CsBridgeConnector, running as a Windows 2000 service, watches for changes to Cisco Unity subscriber data by monitoring the SQL database on the Cisco Unity bridgehead server. This database includes Cisco Unity subscriber data of all Cisco Unity servers in the directory. If a change is detected, the CsBridgeConnector sends the updated data to the Bridge. The CsBridgeConnector also monitors the UOmni mailbox for changes from the Bridge so that the necessary changes to the Bridge subscriber accounts are made.

Cisco Unity does not send information about Internet, AMIS, Bridge, or VPIM subscribers to the Bridge; only information about “regular” Cisco Unity subscribers is sent to the Bridge. In the other direction, the Bridge sends information to Cisco Unity about Bridge subscribers.

Directory synchronization does not affect messaging. Subscribers can still send and receive messages when the directories are not synchronized. If Cisco Unity subscriber information is missing from the Bridge directory, the Octel system cannot retrieve the voice name when an Octel subscriber addresses a message to that Cisco Unity subscriber, but the message is still delivered.

When Cisco Unity and the Bridge are initially configured, all Cisco Unity subscriber data is sent to the Bridge automatically if the configuration was done in the exact sequence specified in the "Task List: Setting Up Cisco Unity and the Bridge for Networking" section on page 2-2. If necessary, you can force a full synchronization after the initial configuration. Subsequently, if there is a change to Cisco Unity subscriber data, only the changed data is sent to the Bridge.

For directory data about newly-created subscribers to be automatically sent to the Bridge, you first create the subscribers in Cisco Unity with Unity node serial numbers and legacy mailbox IDs defined, and then create corresponding Unity Node(s) on the Bridge. If you do the reverse and create a Unity Node on the Bridge before creating any subscribers with the same serial number, you will have to force a synchronization to send directory data to the Bridge, or delete and then add back the Unity Node on the Bridge. Subsequently, if you add more subscribers with the same serial number, Cisco Unity automatically sends the directory information to the Bridge.

Failover and Directory Synchronization

When a Cisco Unity server is configured for failover, the Cisco Unity subscriber directory is not synchronized with the Bridge directory while the secondary server is active. When the primary server becomes active again, synchronization resumes automatically. Failover provides for replication of subscriber data between the primary and secondary Cisco Unity servers, so existing directory information will be available to subscribers no matter which server is active.

When the secondary server is active, subscribers on Cisco Unity and on the Octel system can still send and receive messages, but changes to Cisco Unity subscriber accounts will not be replicated to the Bridge immediately. For example, if you add subscriber accounts on the active secondary server, this information is not replicated to the Bridge until the primary server becomes active again.

Time Required for a Full Synchronization

The amount of time necessary for a full synchronization depends on many factors, such as the network connection to the Bridge, the size of the directory, whether subscribers have recorded voice names, and the codec used to record the voice names. (Voice name data is large in comparison with the other subscriber information that is sent to the Bridge.) When the number of Cisco Unity subscribers in the network is 1,000 or fewer, the time required for a full directory synchronization is usually a matter of minutes. When the number of Cisco Unity subscribers in the network is 5,000 to 10,000 or above, and all have recorded voice names, the time required is usually a matter of hours.

Maintaining the Logical Octel Network Topology Within the Cisco Unity Directory

In Octel analog networking, the serial number assigned to each Octel node is used to identify the node in the network. Just as Cisco Unity has a delivery location for each Octel node in the network, and the Bridge has an Octel Node page for each Octel node in the network, each Octel node is configured with a node profile for all the other Octel nodes in the network. Each node profile contains the serial number of the corresponding Octel node.

The serial numbers of the sending and receiving Octel nodes are exchanged via DTMF tones at the beginning of a communication session. The receiving Octel node uses the serial number it receives to verify the network-node profile of the sending node. Before the sending node transmits a voice message, it sends the mailbox number of the recipient. The receiving Octel node verifies that there is a subscriber with that mailbox number before accepting the message.

In an Octel analog network, the combination of the node serial number and the subscriber mailbox number uniquely identifies the subscriber within the network.

See the following sections for additional information:

- Retaining the Octel Network Identity, page 1-14
- Independent Numbering Plans, page 1-14
- Collapsing Multiple Octel Nodes, page 1-15
- Interop Gateway and Bridge Networking, page 1-15

Retaining the Octel Network Identity

When migrating subscribers from Octel to Cisco Unity in stages, it is important that messages sent from Cisco Unity subscribers who are migrated Octel subscribers appear to come from their former Octel server, so that reconfiguration of the network nodes on the existing Octel servers is minimized. To this end, each Cisco Unity subscriber account must be configured with a serial number and a legacy mailbox number. This also allows the remaining Octel subscribers to address messages by using the same number that they used before the subscriber migrated to Cisco Unity.

When a Cisco Unity subscriber sends a message to an Octel subscriber, the legacy serial number and mailbox number are included in the message header. When the Bridge transmits the message to the Octel node, it transmits the serial number in the message header to identify the sending node, and transmits the mailbox number to identify the sending subscriber. The receiving Octel node recognizes the serial number and accepts the message.

Independent Numbering Plans

All Cisco Unity subscribers must be assigned a serial number and legacy mailbox number in order to send messages to and receive messages from Octel subscribers. If you will be creating Cisco Unity subscriber accounts for users who previously existed on an Octel system, use the serial number of the Octel server that the subscriber migrated from and the mailbox number that the subscriber had on the Octel system. If you will be creating Cisco Unity subscriber accounts for new users who were never subscribers on an Octel system, choose a serial number and a mailbox number that are not already in use.

The serial numbers and legacy mailbox numbers are stored in the Domino directory along with a subset of other subscriber data. For each serial number, the legacy mailbox number must be unique within the Domino directory. Depending on your Cisco Unity numbering plan, the legacy mailbox number may or may not be the same as the primary extension for the Cisco Unity subscriber.

The serial numbers and legacy mailbox numbers allow you to maintain a logical Octel analog networking topology within the Cisco Unity directory. With this scheme, Cisco Unity subscribers can maintain their previous Octel node serial number and mailbox number identities for messaging with Octel subscribers, while still allowing you to use whatever numbering plan best suits the new Cisco Unity topology.

Collapsing Multiple Octel Nodes

When migrating to Cisco Unity in stages, you typically will migrate all the Octel subscribers from a particular node to Cisco Unity and then decommission the Octel node. The Cisco Unity bridgehead and Bridge servers represent the serial number of the Octel node whose subscribers migrated to Cisco Unity. The Cisco Unity bridgehead and Bridge servers can emulate multiple nodes in the Octel analog network.

In installations with multiple Cisco Unity servers, it does not matter whether the Cisco Unity subscribers who have migrated from one Octel server are grouped together as subscribers on one Cisco Unity server, or if they are distributed among multiple Cisco Unity servers. Because the Cisco Unity subscribers are configured with the legacy serial and mailbox numbers, their identities are the same as before the migration to the remaining Octel servers.

Interop Gateway and Bridge Networking

The Interop Gateway for Domino is a Cisco Unity service (called CsDomInteropGty) that enables messaging between Cisco Unity and other voice messaging systems. The Interop Gateway files are copied to the Cisco Unity server during setup; however, the Interop Gateway is not installed as a service until you run the Interop Gateway Configuration wizard when configuring Cisco Unity for Bridge Networking. The Interop Gateway Configuration wizard configures and starts the service. In the Interop Gateway Configuration wizard, you specify a Domino Foreign domain name (for example, “voicemail.domain.com”) and mail file that Bridge messages will be routed through.

When subscribers use the phone to address a message to a Bridge recipient, Cisco Unity constructs a “to” address in the form OMNI:<Location Dial ID>_<Remote Mailbox>@<ForeignDomain> for the message. Domino routes the message to the mail file that you specified in the Interop Gateway Configuration wizard. The Interop Gateway monitors this mail file. For an outbound message to a Bridge recipient, the Interop Gateway constructs a MIME message, and hands the message back to Domino for delivery to the Bridge via SMTP.

Messages from the Bridge that are received by the Domino server with the SMTP Listener service are routed to the Interop Gateway mail file for processing, after which the Interop Gateway sends the message back to Domino, which routes it to the subscriber mail file.

Choosing the Interop Gateway Foreign Domain Name

The Foreign domain name to be used by the Interop Gateway can be whatever you would like it to be. As a best practice, however, we recommend that you use a name that follows the format <Name>.<DomainName>, where <Name> is a descriptive term and <DomainName> is the domain name of your organization, for example, UnityBridge.mydomain.com. By following this convention, you will be able to add a mail exchange (MX) record in DNS using the Interop Gateway foreign domain name and the IP address of the Domino server that handles incoming SMTP messages.

The Foreign domain name must be unique, meaning there can be no other Domain documents in Domino that have a domain name that matches what you choose for the Interop Gateway Foreign domain name. Additionally, the Foreign domain must not be used by any other program, such as a fax server. (Typically, fax servers use Foreign domains for processing and routing faxes.)

See the “Configuring the Interop Gateway” section on page 2-7 for information on running the Interop Gateway Configuration wizard.

Message Addressing Options

Cisco Unity provides the following message addressing options for addressing messages to Octel subscribers:

- Blind addressing
- Entering the extension of a Bridge subscriber
- Spelling the name of a Bridge subscriber

Messaging Similarities and Limitations

For the most part, messaging between Cisco Unity and Octel subscribers is the same as messaging between Cisco Unity subscribers. For example:

- Messages marked urgent when they are sent are marked urgent when they are retrieved by the recipient.
- Messages marked private when they are sent are marked private when they are retrieved by the recipient.
- The future delivery of messages to Octel recipients is supported.
- Cisco Unity subscribers can send messages to Cisco Unity distribution lists that include Bridge subscribers.
- A message from a Cisco Unity subscriber addressed to multiple Octel recipients who are on the same Octel server is transmitted once to the Bridge. If all of the recipients are on the same Octel node, the Bridge makes only one phone call to the node and transmits only one message, which then is delivered to each recipient. If the recipients are on multiple Octel nodes, the Bridge makes only one phone call to each node and transmits only one message, which then is delivered to each recipient on that node.
- Fax messages can be sent, depending on Octel support.

Note the following exceptions:

- Requests for both read receipt and delivery receipt messages are returned simply as “delivery receipts.” The receipt is delivered to the sender when the message is sent from the Bridge to the Octel node, not when the Octel system places the message in the subscriber mailbox or when the message is actually read.
- E-mail messages cannot be delivered to Octel recipients even though subscribers can address and send messages to them from Notes. Instead of being delivered, e-mail messages that are sent to Octel recipients are returned to the sender as non-delivery receipts (NDRs).
- When subscribers send voice messages from Notes and mark them as low importance, the messages are treated the same as regular messages.
- If the remote Octel system is configured to send the recorded voice name in messages, Cisco Unity will play it as part of the message. When a Cisco Unity subscriber listens to a message from someone on an Octel node, if there is a matching Bridge subscriber with a recorded voice name, and if the subscriber conversation settings are configured to play the sender’s information, the voice name of the sender will be played twice.

Cisco Unity subscribers who have used the Octel phone menus will notice differences when they hear the standard Cisco Unity conversation. As an alternative to the standard Cisco Unity conversation, you can activate Cisco Unity Optional Conversation 1 so that subscribers hear message-retrieval menus that may more closely resemble the choices that they are familiar with. Note however that other

menus—those that unidentified callers and Cisco Unity subscribers use to send and manage messages, as well as the menus that subscribers use to change their Cisco Unity settings—are the same as those in the Cisco Unity standard conversation.

For more information on Optional Conversation 1 and other customizations that you may want to make to the Cisco Unity conversation, refer to the "Cisco Unity Conversation" chapter of the *Cisco Unity System Administration Guide*. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag405/dom/index.htm.

Blind Addressing and Bridge Networking

Blind addressing is one of the methods that Cisco Unity provides for addressing messages to Octel users. Blind addressing allows Cisco Unity to address messages to a subscriber on an Octel node when there is no corresponding Bridge subscriber in the directory.

To address a message to someone on another node, subscribers enter a blind address, which could be either of the following:

- A Bridge delivery location dial ID and the remote mailbox number of the recipient.
- A prefix defined on a Bridge delivery location and a remote mailbox number. Note that a prefix can overlap with digits in the remote mailbox number. See the "Mailbox Lengths and Prefixes" section on page 1-8 for additional information.

When a subscriber addresses a message by entering a number, Cisco Unity performs a complex search. During the blind addressing phase of the search, Cisco Unity parses the number that the subscriber entered and searches for a matching delivery location prefix or dial ID. If a matching delivery location is found, Cisco Unity addresses the message without verifying that the remote mailbox number exists. Cisco Unity does provide voice name confirmation that the delivery location exists before addressing the message (assuming a voice name was recorded for the delivery location). If Cisco Unity does not find a matching location, it reports the error to the sender and does not address the message.

Because the Bridge supports NameNet, blind addressing is really only "blind"—meaning there is no corresponding Bridge subscriber in the directory and thus, no voice name confirmation—the first time a Cisco Unity subscriber sends a message to an Octel subscriber. Subsequently, if configured to do so, Cisco Unity creates a Bridge subscriber by using the text name, mailbox number, and voice name of the recipient that the Bridge retrieved from the Octel node.

For administrators of Cisco Unity, blind addressing is the option that requires the least amount of work to set up. However, the first time a message is sent to an Octel user, or when the aging period for the usage-based directory entry expires (if name aging is enabled), subscribers encounter the limitations of blind addressing:

- Subscribers can address a message only by using number mode.
- Cisco Unity cannot verify that the number entered is correct, so subscribers may inadvertently address a message to the wrong person or to a non-existent mailbox.

In Cisco Unity 4.0(5) and later, subscribers can use the Cisco Unity conversation to add and delete blind addresses in their private distribution lists. In contrast, subscribers cannot use the Cisco Unity Assistant to add blind addresses to their private lists, though they can use it to view list members and to delete any blind addresses that were added by phone. The Cisco Unity Administrator also does not allow you to add blind addresses to private lists, but you can use it to view and delete list members.

Bridge Subscribers

Bridge subscribers are a representation in Cisco Unity of subscribers on the Octel system. 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. When you delete Bridge subscribers, the associated Person documents are deleted automatically. Cisco Unity subscribers address messages to Bridge subscribers just as they address messages to regular subscribers, but the messages are sent via the Bridge to the appropriate mailbox on an Octel system. Bridge subscribers can be included in Cisco Unity distribution lists, and outside callers can leave messages for them (if they are listed in the Cisco Unity phone directory).

Bridge subscribers do not require additional Domino client access licenses (CALs), and they do not consume Cisco Unity subscriber licenses. The Cisco Unity subscriber license count does not change when you create Bridge subscribers.

Other than receiving messages, Bridge subscribers do not have access to other Cisco Unity features, and some sections of the Cisco Unity Administrator are disabled for Bridge subscribers. Bridge subscribers:

- Cannot log on to Cisco Unity by phone to check or send messages.
- Cannot log on to Cisco Unity by phone—or use the Cisco Unity Assistant—to adjust personal settings.
- Cannot own private lists.
- Cannot set up or receive message notifications.
- Cannot receive message waiting indications.

See the following sections for additional information:

- How Bridge Subscribers Are Created, page 1-19
- Creating Bridge Subscribers in Cisco Unity, page 1-19
- Creating Permanent Directory Entries on the Bridge Server, page 1-19
- Creating Bridge Subscribers and Then Creating Corresponding Permanent Directory Entries, page 1-20
- Extension Addresses, page 1-20
- Subscriber Experience with Bridge Subscribers, page 1-21
- Identified Subscriber Messaging (Cisco Unity 4.0(4) or Later), page 1-21
- Live Reply to Bridge Subscribers (Cisco Unity 4.0(4) and Later), page 1-22
- Deleting Bridge Subscribers, page 1-22
- Disabling the Automatic Creation, Modification, and Deletion of Bridge Subscribers, page 1-23
- Controlling How Text Names Are Parsed for Auto-Created Bridge Subscribers, page 1-24
- Determining How Bridge Subscribers Appear in the Notes Address Book, page 1-24
- Controlling the Extensions Assigned to Auto-Created Bridge Subscribers, page 1-25
- Preventing Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant, page 1-25

How Bridge Subscribers Are Created

Before Bridge subscribers can be created, you first must create a Bridge delivery location that corresponds to each Octel node with which Cisco Unity communicates.

Bridge subscribers are automatically created when the Bridge creates usage-based directory entries for the Octel users. You can also create Bridge subscribers manually in Cisco Unity, or create permanent directory entries on the Bridge server, which results in the automatic creation of Bridge subscribers.

Note that information for creating, updating, and deleting Bridge subscribers is pushed from the Bridge server to Cisco Unity, never the reverse.

If you decide that you want to control the creation of Bridge subscriber accounts, use one of the following approaches:

- Create Bridge subscribers in Cisco Unity by using the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard.
- Create permanent directory entries on the Bridge server by using the Bridge Administrator or the Cisco Unity Bridge Mailbox Import tool.
- First create the Bridge subscribers in Cisco Unity, and then create corresponding permanent directory entries on the Bridge.

Creating Bridge Subscribers in Cisco Unity

If you want the extensions that you assign to Bridge subscribers to fit in with your numbering plan, you may need to manually create Bridge subscribers in Cisco Unity. The extension is the number that Cisco Unity subscribers enter when addressing messages to Bridge subscribers.

When creating Bridge subscribers, you specify the remote mailbox number of the user on the Octel node. The remote mailbox number may or may not be the same as the extension. You also select a Bridge delivery location with which to associate the subscriber. In organizations with multiple Cisco Unity servers, Bridge subscribers can be associated only with Bridge delivery locations that were created on the same Cisco Unity bridgehead server.

Note the following about Bridge subscribers that you manually create:

- A corresponding Octel node usage-based directory entry on the Bridge is created only when a Cisco Unity subscriber first sends a message to the Bridge subscriber. At that time, the Bridge obtains the text and recorded voice name from the Octel node, and sends this information to Cisco Unity. If configured to do so, Cisco Unity updates the Bridge subscriber account with the text and recorded voice name from the Bridge. If you have already recorded a voice name for the Bridge subscriber, it is replaced by the voice name sent by the Bridge.
- These subscribers are subject to name aging deletion. If name aging is enabled, the name aging period starts when a corresponding Octel node directory entry is created on the Bridge.
- A corresponding Domino Person document that has “Other Internet Mail” set in the Mail System field is created at the same time the Bridge subscriber account is created.

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, you should create permanent directory entries on the Bridge server. When you create a permanent Octel node directory entry, the Bridge places an administrative call to the Octel node to obtain

the name and recorded voice name. The directory entry is updated with this data. The Bridge sends the data along with a request to Cisco Unity to create a corresponding Bridge subscriber account (also referred to as auto-created Bridge subscribers).

Note the following:

- The {Bridge Subscriber} Template is the default template used for auto-created Bridge subscribers. You specify the template to be used for auto-created Bridge subscribers in the Cisco Unity Administrator.
- By default, the extension assigned to an auto-created Bridge subscriber is the delivery location dial ID with the remote mailbox number added to the end (for example, if the delivery location dial ID is 111, and the remote mailbox number is 2222, the extension assigned will be 1112222).
- The auto-created Bridge subscriber that corresponds to a permanent directory entry is not subject to name-aging deletion.
- When the Bridge subscriber account is created, a corresponding Domino Person document that has "Other Internet Mail" set in the Mail System field is also created automatically.

Creating Bridge Subscribers and Then Creating Corresponding Permanent Directory Entries

If you need the flexibility to specify extensions when Bridge subscribers are created—so that they fit with your numbering plan—and if you want the text and recorded voice names to be automatically obtained from the Octel system, you first create Bridge subscribers in Cisco Unity and then create the permanent directory entries on the Bridge server. When you create a permanent Octel node directory entry, the Bridge places an administrative call (according to the schedule defined in the Bridge Administrator for the Octel Node) to the Octel node to obtain the name and recorded voice name. The directory entry is updated with this data. The Bridge sends the data along with a request to Cisco Unity to create a corresponding Bridge subscriber account. Because you first created Bridge subscribers in Cisco Unity, a Bridge subscriber already exists that matches the Octel node and remote mailbox number of the directory entry, so the existing Bridge subscriber account is updated with the text and voice name.

Extension Addresses

When you create a Bridge subscriber, Cisco Unity adds to the Forwarding Address field of the associated Person document an address in the following format:

OMNI:<Delivery Location Dial ID>_<Remote Mailbox Number>@<ForeignDomain>

This special e-mail address is called an extension address or a remote address. The extension address is a combination of the delivery location Dial ID with which the Bridge subscriber is associated, the Remote Mailbox Number of the Bridge subscriber, and the Interop Gateway foreign domain name.

When subscribers use the phone to address messages to a Bridge subscriber, they dial an extension. Cisco Unity recognizes the recipient as a Bridge subscriber and retrieves the extension address from the SQL database on the Cisco Unity server.

Extension addresses are generated automatically when you create Bridge subscribers. Extension addresses are updated automatically when you change the remote mailbox number and the Dial ID of a delivery location.

Subscriber Experience with Bridge Subscribers

Provided that Bridge subscribers have had voice names recorded for them:

- Subscribers can address messages to Bridge subscribers by using the phone, or the DUC-enabled Notes client.
- Bridge subscribers are listed in the Notes address book.
- When using the phone, subscribers can address messages to Bridge subscribers in spelled-name mode (if enabled on the system) or by extension.
- Subscribers get voice name confirmation when addressing a message to a Bridge subscriber.
- When a subscriber uses the phone to listen to a message from someone on the Octel system with a corresponding Bridge subscriber account in Cisco Unity, Cisco Unity announces who the message is from.
- Bridge subscribers can be added to Cisco Unity distribution lists.

Identified Subscriber Messaging (Cisco Unity 4.0(4) or Later)

Identified subscriber messaging (ISM) affects what subscribers hear when they call other subscribers from their primary or alternate extensions and are forwarded to the greetings of the subscribers they call. If they then leave a message, ISM affects what the called subscriber hears and can do when listening to the message. When ISM is enabled, Cisco Unity recognizes that the calling extension is associated with a subscriber and accordingly plays the internal greeting of the called subscriber. Additionally, when the called subscriber later listens to the message, Cisco Unity plays the recorded voice name of the subscriber who left the message and allows the called subscriber to record a reply.

When a call to a Cisco Unity subscriber is forwarded to the subscriber greeting and ISM is enabled, Cisco Unity compares the calling number (ANI or caller ID) to the primary and alternate extensions of subscribers. If a match is found, Cisco Unity identifies the caller as a subscriber. When Cisco Unity compares the calling number to extensions, by default, only “regular” Cisco Unity subscribers on the local system are included in the comparison. Beginning with Cisco Unity 4.0(3), ISM can be expanded to include all Cisco Unity subscribers throughout a dialing domain.

You can enable ISM for AMIS, Bridge, and VPIM subscribers (collectively referred to as external subscribers), so that Cisco Unity will include them when comparing calling numbers to extensions. Note the following:

- After enabling ISM for external subscribers, Cisco Unity must be restarted.
- If multiple Cisco Unity servers are networked via Digital Networking, ISM functionality can be made available only on the Cisco Unity servers that are in the same dialing domain as the bridgehead server.
- You must enable ISM for external subscribers for each Cisco Unity server on which the functionality is desired.
- If a single Cisco Unity server is in use, the Cisco Unity server must be a member of a dialing domain for this functionality to be used.

Note the difference between leaving a messaging and sending a message. When a person on the remote voice messaging system with a corresponding external subscriber account records and sends a message to a Cisco Unity subscriber (as opposed to calling and leaving a message), all versions of Cisco Unity identify the message as being from the corresponding external subscriber.

The phone system provides the calling number to Cisco Unity. The number of digits included in the calling number is configurable in most phone systems. For Cisco Unity to find a matching subscriber extension, the phone system must be configured to provide the applicable number of digits in the calling number. You may also need to add alternate extensions to the subscriber accounts to match the calling number. Additionally, there may be other phone system-specific issues that prevent Cisco Unity from matching the calling number to a subscriber extension. Refer to your phone system documentation and the applicable Cisco Unity integration guide for details about the call information provided by the phone system.

See the "Extending Identified Subscriber Messaging to Include Bridge Subscribers" section on page 2-36 for details.

Live Reply to Bridge Subscribers (Cisco Unity 4.0(4) and Later)

Live reply allows subscribers who listen to their messages by phone to respond to messages from other subscribers by calling them. When live reply is enabled, subscribers listening to messages by phone can reply to a subscriber message by pressing 4-4 to have Cisco Unity call the subscriber directly. (Subscribers using Optional Conversation 1 press 8-8 for live reply.) Note that whether subscribers have access to the live reply feature depends on their class of service settings. (Live reply is enabled on the Subscribers > Class of Service > Messages page in the Cisco Unity Administrator.)

Subscribers can live reply to messages from subscribers on other voice messaging systems who have corresponding Bridge subscriber accounts in Cisco Unity. In order for the live reply call to be successfully transferred, a call transfer number must be configured for the Bridge subscribers.

Note that a live reply to a Bridge subscriber is always done via a release to phone system transfer, even when both the Cisco Unity subscriber who is replying to a message and the Bridge subscriber have accounts on the same Cisco Unity server. On a release to switch transfer, Cisco Unity dials the call transfer number configured for the Bridge subscriber and hangs up, leaving the phone system to handle the call. Note the following limitations with release to switch transfers:

- The Bridge subscriber call screening, call holding, and announce features are ignored.
- The call transfer setting "No (Send Directly to Subscriber's Greeting)" is ignored. Cisco Unity dials the Bridge subscriber extension and hangs up. If the subscriber extension is a valid extension on the phone system that Cisco Unity is integrated with, then the subscriber phone rings. If the subscriber extension is not a valid phone extension, what happens to the call after that depends on the phone system and how it is configured. If you do not configure the phone system to handle calls to the subscriber extensions, the caller may be disconnected.

Note the following:

- Live reply to Bridge subscribers is enabled automatically, and cannot be disabled.
- Live replies to Bridge subscribers with accounts on other Cisco Unity servers do not use the cross-server live reply functionality that can be used to live reply to Cisco Unity subscribers with accounts on other Cisco Unity servers. However, for live reply to be offered when a Cisco Unity subscriber replies to a message from a Bridge subscriber with a subscriber account on another Cisco Unity server, the servers must be in the same dialing domain.

Deleting Bridge Subscribers

Each Bridge subscriber is associated with a Domino Person document. When Bridge subscribers are deleted, the associated Person documents are automatically deleted.

You can delete Bridge subscribers one at a time in the Cisco Unity Administrator. As a subscriber is deleted in the Cisco Unity Administrator, the associated Person document is automatically deleted as well. This is true for both auto-created Bridge subscribers and Bridge subscribers that have been manually created.

To delete all of the Bridge subscribers associated with a delivery location, the underlying Person documents associated with the subscribers, and the delivery location itself, use the Global Subscriber Manager, available in Tools Depot.

If you delete the corresponding directory entries on the Bridge server by using the Bridge Administrator or the Cisco Unity Bridge Mailbox Import tool, both the Bridge subscribers in Cisco Unity and the Domino Person documents are deleted automatically. The Person documents are also deleted when the Bridge sends a deletion request to Cisco Unity to delete a Bridge subscriber because the name aging period has expired or because there was an indication on message delivery to an Octel system that the target recipient no longer exists. Note that when a parent Octel Node profile is deleted from the Bridge, deletion requests for any remaining directory entries associated with that Octel Node will not be sent to Cisco Unity. Any remaining Bridge subscribers and Person documents associated with this Octel Node will not be deleted automatically.

Disabling the Automatic Creation, Modification, and Deletion of Bridge Subscribers

The automatic synchronization of directory information between the Bridge and Cisco Unity is performed by the CsBridgeConnector service on the Cisco Unity bridgehead server. The CsBridgeConnector service:

- Monitors the Cisco Unity subscriber database for changes and sends updates to the Bridge so that the Bridge can update its directory of Cisco Unity subscribers. By doing so, the Bridge can respond to remote Octel node requests for Cisco Unity subscriber voice and text names.
- Handles change requests sent from the Bridge after it retrieves voice and text names of remote Octel node subscribers. The CsBridgeConnector service adds, deletes, and modifies Bridge subscribers and their associated Domino Person documents. This allows Cisco Unity subscribers to address remote Octel node subscribers by spelled name, and provides spoken name confirmation of the addressee when selected. It also allows these remote Octel subscribers to be added to private and public Cisco Unity distribution lists.

The CsBridgeConnector service should never be disabled on a Cisco Unity bridgehead server. Doing so could result in a backlog of directory messages from the Bridge, consuming large amounts of Domino storage, and preventing Cisco Unity subscriber voice and text names from being available to the remote Octel nodes upon request.

However, there may be situations where you want to disable the automatic creation, deletion, and/or modification of Bridge subscribers and Person documents by the CsBridgeConnector. For example, you may want to disable this functionality for one of the following reasons:

- You may want to have control over the text and voice names for Bridge subscribers. Disabling CsBridgeConnector auto-synchronization of these properties ensures that the changes you make to Bridge subscribers will not be overwritten by directory information propagated from remote Octel nodes via the Bridge.
- You may not want to create Bridge subscribers at all; instead, you may want Cisco Unity subscribers to use blind addressing when addressing messages to subscribers on the Octel system.

Caution Disabling any CsBridgeConnector auto-synchronization functionality requires manual maintenance of any Bridge subscribers and their associated Person documents. Failure to keep Bridge subscriber information current can result in Cisco Unity subscribers sending voice messages to unintended recipients, or not finding remote Octel subscribers in the directory as expected.

You can control the creation, modification, and deletion of auto-created Bridge subscribers in the Cisco Unity Administrator.

Controlling How Text Names Are Parsed for Auto-Created Bridge Subscribers

In Cisco Unity, the first and last names of subscribers are stored as distinct fields in the directory, which allows directory lookups to be configured by either the last or the first name. However, Octel subscriber names are stored as one single name. To comply with Octel analog networking, when the Bridge and remote Octel systems exchange directory information, only a single field is passed for the text name. The CsBridgeConnector service on the Cisco Unity bridgehead server parses the text name sent from an Octel system via the Bridge into separate first and last name fields when the accounts for auto-created Bridge subscribers are created or updated.

If the text name includes one or more comma characters, the CsBridgeConnector service parses the text name as follows:

- All characters after the first comma in the string are saved as the first name.
- All characters before the first comma in the string are saved as the last name.

For example, if “Bader, Kelly” is the text name, “Kelly” is saved as the first name and “Bader” is saved as the last name.

In some cases, the text names on the Octel systems do not include a comma. In this case, you can control how the CsBridgeConnector service parses the text name on a delivery location basis with the setting “If the Octel Text Name Has No Comma.”

Determining How Bridge Subscribers Appear in the Notes Address Book

Depending on your installation, the users of the remote voice messaging system may already have Domino user accounts that they use for e-mail. Therefore, when Bridge subscriber accounts are created for them, the Notes address book will contain duplicate listings—the existing user account that is used for e-mail, and a new one associated with the Bridge subscriber that is used only for voice mail. Both listings are included in the Notes address book. This means that people may inadvertently send e-mail messages to the Bridge subscribers, which should be used only for addressing voice messages.

To discourage people from inadvertently sending e-mail messages to Bridge subscribers, you can append text to either the first or last name so that subscribers can distinguish the Bridge subscriber from a user account. In this way, you can reduce the number of e-mail messages inadvertently sent to Bridge subscribers and simplify addressing for those who send voice messages to them at the same time. For example, you could append “ - Voice mail” to the first name of each Bridge subscriber, and the names would appear in the Notes address book as follows:

Abade, Alex
Abade, Alex - Voice mail
Bader, Kelly
Bader, Kelly - Voice mail
Campbell, Terry

Campbell, Terry - Voice mail
Cho, Li
Cho, Li - Voice mail

In this way, subscribers can easily determine which address is appropriate to use when they send voice messages to Bridge subscribers. Additionally, when subscribers use the Notes to address a voice message to a Bridge subscriber, they can be confident that the address is formatted correctly.

Controlling the Extensions Assigned to Auto-Created Bridge Subscribers

By default, the primary extension assigned to an auto-created Bridge subscriber consists of the delivery location dial ID followed by the remote mailbox number. If you prefer that the dial ID not be included in the extensions for auto-created Bridge subscribers, you can change the setting in the Cisco Unity Administrator.

Preventing Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant

In the transition from a legacy voice messaging system to Cisco Unity, your organization may choose to migrate users to Cisco Unity in phases. As a result, Cisco Unity will likely support both regular subscribers and "external" subscribers—Bridge, AMIS, or VPIM contacts (as applicable)—at the same time. Regular subscribers can send messages to external subscribers, and even add them to their private distribution lists during the transition.

However, once external subscribers are converted into regular Cisco Unity subscribers, they are automatically removed from all private lists without notifying private list owners. When this occurs, subscribers may continue to send messages to their private lists without realizing that some of their intended recipients no longer receive them.

When convenient and practical, Cisco Unity administrators should notify subscribers when external subscribers are converted to regular subscribers, notifying subscribers that they should re-add the newly migrated subscribers to existing private lists, as applicable. During the migration phase, you may also want to consider preventing subscribers from adding subscribers to their private lists in the Cisco Unity Assistant, and asking them not to use the Cisco Unity phone menus to do so—at least until the migration process is complete.

Use the following procedure to prevent all subscribers associated with the Cisco Unity server from adding individual subscribers to their private lists in the Cisco Unity Assistant. The procedure does not prevent subscribers from using the Cisco Unity phone menus to add regular and external subscribers to their private lists, nor does it prevent subscribers from addressing messages to regular and external subscribers.

To Prevent Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant

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 **Unity Assistant—Do Not Allow Subscribers to Add Subscribers to Private Lists**.

Step 4 In the New Value list, click **1**, and then click **Set** so that when subscribers add members to their lists in the Cisco Unity Assistant, the Find Names dialog box does not display the Subscribers tab. (Subscribers can continue to add distribution lists to their lists from the Distribution Lists tab.)

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

Step 6 Click **Exit**.

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

Supported Codecs

On the Unity Node Configuration page in the Bridge Administrator, you can select which codec will be used to encode voice messages when they are sent from the Bridge to Cisco Unity subscribers: either the G.711 or the G.729a codec. The default codec is G.711.

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. For example, assume that the three Unity Nodes show in Table 1-3 have been created, and that UnityGroup1 is listed first on the Unity Nodes page.

Table 1-3 Codec Example

Name	Serial Number	Codec
UnityGroup1	9000	G.711
UnityGroup2	90000	G.729a
UnityGroup3	9001	G.729a

In this example, all recorded voice names for all Octel node directory entries will be sent from this Bridge server to the Cisco Unity bridgehead server by using the G.711 codec.

We recommend that the same codec setting be used for all Unity Nodes configured on the Bridge server.

Voice messages that are sent from Cisco Unity to the Bridge can also be recorded with either the G.711 or the G.729a codec. The default is the G.711 codec. Although Cisco Unity supports other codecs, the Bridge supports only G.711 or G.729a.

Notable Behavior

This section describes notable behavior of Bridge Networking. See the following sections for more information:

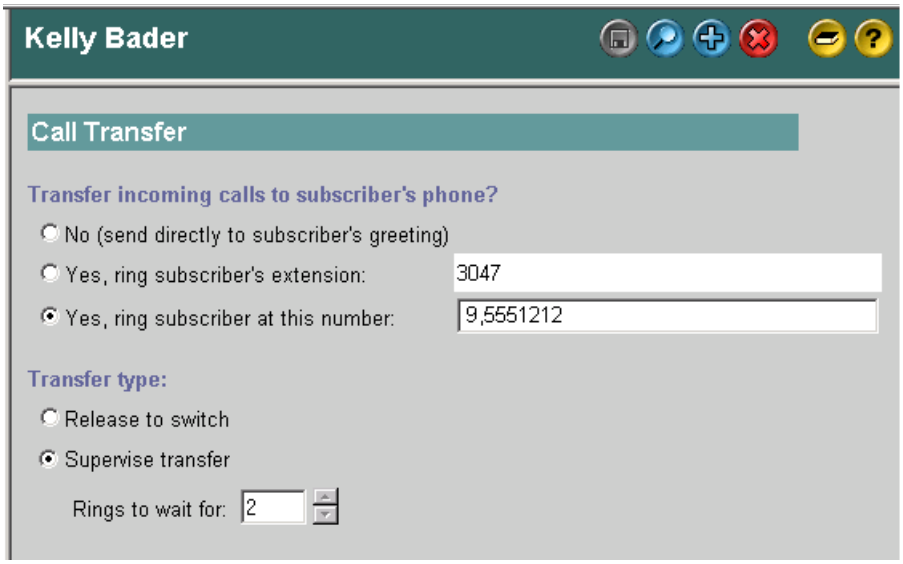
- Call Transfer Settings and Bridge Subscribers, page 1-27
- Directory Lookups of Asian and European Names May Fail, page 1-28
- Distribution Lists, page 1-28
- Inbound Search Scope, page 1-29
- Some Messages to Cisco Unity Are Delayed, page 1-29

- Automatic Gain Control Applied to Messages Sent from the Bridge to Cisco Unity (Bridge 3.0(5) and Later), page 1-29
- Cisco Unity Subscribers Receive Extended-Absence Notification from Octel Servers (Cisco Unity 4.0(4) and Later), page 1-29

Call Transfer Settings and Bridge Subscribers

In installations with multiple Cisco Unity servers networked via Digital Networking, the number that Cisco Unity uses for call transfers to a subscriber is the only number replicated among the Cisco Unity servers; none of the other settings on the Subscriber > Call Transfer page in the Cisco Unity Administrator are replicated. For example, in Figure 1-8, call transfers are set to ring the subscriber at the number 9,5551212. The only call transfer setting that is replicated to other Cisco Unity servers is the call transfer number 9,5551212. If the setting was "Yes, ring subscriber's extension" instead, the number 3047 would be replicated.

Figure 1-8 Only the Call Transfer Number Is Replicated



When the call transfer setting is set to "No (send directly to subscriber's greeting)," the call transfer number is automatically set to the subscriber extension (3047 in the example above), which is replicated to the other networked Cisco Unity servers.

Call transfers to Bridge subscribers created on other Cisco Unity servers are always handled by the phone system (release to switch)—rather than by Cisco Unity (supervised transfer)—even if the subscribers are set up for supervised transfers (as in the above example). The release to switch call transfers happen when:

- A Cisco Unity subscriber chooses to call the sender (live reply) after listening to a message left by a Bridge subscriber. (Live replies to Bridge subscribers are always done release to switch, even when the reply is to a Bridge subscriber on the same Cisco Unity server.)
- A caller enters the extension of a Bridge subscriber from the automated attendant (for example from the opening greeting), and the Bridge subscriber account is on another Cisco Unity server.

- A caller spells the name of a Bridge subscriber from a directory handler, and the Bridge subscriber account is on another Cisco Unity server.

On a release to switch transfer, Cisco Unity dials the call transfer number configured for the Bridge subscriber and hangs up, leaving the phone system to handle the call. Note the following limitations with release to switch transfers:

- The Bridge subscriber call screening, call holding, and announce features are ignored.
- The call transfer setting "No (Send Directly to Subscriber's Greeting)" is ignored. Cisco Unity dials the Bridge subscriber extension and hangs up. If the subscriber extension is a valid extension on the phone system that Cisco Unity is integrated with, then the subscriber phone rings. If the subscriber extension is not a valid phone extension, what happens to the call after that depends on the phone system and how it is configured. If you do not configure the phone system to handle calls to the subscriber extensions, the caller may be disconnected.

Directory Lookups of Asian and European Names May Fail

Octel voice messaging systems and the Bridge encode subscriber text names in 7-bit ASCII format, which can represent only 128 unique characters. Some European languages need 8 bits to represent certain characters, expanding the character range from 128 to 255. Additionally, languages such as Japanese Kanji include many more characters and require two bytes (16 bits) to represent each character.

Cisco Unity uses the industry-standard Unicode, which employs a 16-bit coding scheme that allows for 65,536 distinct characters—more than enough to represent the characters necessary to any European or Asian language.

The Bridge maintains a permanent directory of Cisco Unity subscribers, including text name, extension, and voice name. Cisco Unity keeps its subscriber directory in synch with the subscriber directory on the Bridge. However, before sending subscriber data to the Bridge, Cisco Unity converts the subscriber text names, which it stores in Unicode, to 7-bit ASCII. Because the first 128 characters in Unicode map exactly to the 128 characters in 7-bit ASCII, English-language names and most European names are converted exactly.

However, European- and Asian-language names that include characters from the extended range cannot be represented in 7-bit ASCII. Therefore, directory lookups by name on Octel systems may fail to find Cisco Unity subscribers whose names include characters that cannot be represented in 7-bit ASCII. This means that Octel subscribers cannot address messages to a Cisco Unity subscriber by spelled-name if the Cisco Unity subscriber name includes characters that cannot be represented in 7-bit ASCII. In this circumstance, Octel subscribers can still address messages by entering the subscriber extension, which finds the subscriber data in the directory, and the Octel subscribers will still get voice name confirmation.

Distribution Lists

Cisco Unity requires that messages from the Bridge be addressed to subscribers only, and not to distribution lists. Therefore, Octel subscribers cannot address messages to Cisco Unity distribution lists.

This is true in the other direction as well—Octel analog networking does not allow subscribers to address messages to a distribution list that was created on remote Octel nodes. Therefore, Cisco Unity subscribers cannot address messages to Octel distribution lists.

However, you can mitigate this situation as follows:

- Add Bridge subscribers to private or public distribution lists on Cisco Unity.
- Add blind addresses to private lists.

- Add the remote addresses of Cisco Unity subscribers to Octel distribution lists. (Note that these addresses do not have to already exist in the NameNet directory.)

Inbound Search Scope

In installations with multiple Cisco Unity servers networked together, the search scope for a matching subscriber for inbound messages sent from the Bridge is set to the global directory. It is not possible to limit the inbound search scope to either a dialing domain or to the local Cisco Unity server. Typically, this is not an issue because the serial number and legacy mailbox number are used for routing messages from Octel subscribers to Cisco Unity subscribers.

Although the combination of serial number and legacy mailbox number should be unique within the global directory, it is possible that you could inadvertently create or modify a subscriber account with non-unique numbers due to directory replication lag time. If two (or more) Cisco Unity subscribers have identical serial numbers and legacy mailbox numbers, messages from Octel subscribers will not be delivered by the Interop Gateway to any of the Cisco Unity subscribers with the duplicate numbers.

Some Messages to Cisco Unity Are Delayed

Messaging between Cisco Unity and the Bridge is done by using SMTP through Domino. If the SMTP connection between the Bridge and Domino goes down, messages arriving at the Bridge from Octel subscribers cannot be delivered. The Bridge stores the messages that cannot be delivered and attempts to send them 20 minutes later. This 20-minute retry interval is not configurable.

When the SMTP connection comes back up, new messages coming from Octel subscribers are delivered immediately. However, the Bridge does not send the messages that previously could not be delivered until the end of the retry interval. Therefore, it is possible that some messages could be stored on the Bridge for up to 20 minutes before they are delivered, even though other messages are delivered immediately.

Automatic Gain Control Applied to Messages Sent from the Bridge to Cisco Unity (Bridge 3.0(5) and Later)

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

The AGC feature makes the volume level of messages from Octel and Cisco Unity subscribers consistent. Before the Bridge sends messages from Octel to Cisco Unity, the gain level is set to the same default level that Cisco Unity uses.

Cisco Unity Subscribers Receive Extended-Absence Notification from Octel Servers (Cisco Unity 4.0(4) and Later)

In Cisco Unity 4.0(4) and later, Cisco Unity subscribers are notified when an Octel recipient has enabled an extended-absence greeting, and are notified whether or not the message was accepted.

An extended-absence greeting can be enabled to override all other greetings. When an Octel subscriber with an enabled extended-absence greeting receives a message from another node on the Octel analog network—including the Cisco Unity Bridge—the receiving Octel server will do one of the following (depending on the Octel subscriber class of service settings):

- Deliver the message to the Octel subscriber mailbox, and send a delivery receipt to the sender explaining that the message was delivered even though the extended-absence greeting of the recipient is enabled.
- Reject the message, and send a nondelivery receipt to the sender explaining that the message was not delivered because the Octel subscriber has an extended-absence greeting enabled.

The Bridge passes along the notification (either the delivery receipt or the nondelivery receipt) to the Interop Gateway, which sets a predetermined reason code in the receipt. The reason code in the receipt is interpreted by the Cisco Unity conversation—also known as the TUI (telephone user interface)—to provide Cisco Unity subscribers with notification of the extended absence. The reason code in the receipt is not interpreted by the DUC-enabled Notes client, so subscribers who use Notes are not provided with notification of the extended absence.

This functionality requires that you enable the Bridge server to send the delivery receipt, as described in the "Enabling the Bridge Server to Send Extended-Absence Delivery Receipts" section on page 2-39.

Additional Bridge-Related Documentation

In addition to this guide, refer to the following documentation for information related to Bridge Networking:

- For information on the initial design using the Bridge and 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/index.htm.
- For information on setting up the Bridge server, refer to the *Cisco Unity Bridge Installation Guide (With IBM Lotus Domino), Release 3.0*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/big/dom/index.htm.
- For a list of Octel voice messaging systems that the Bridge supports, and requirements for the Bridge server, refer to *Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm.
- For version requirements and other information, refer to the "Bridge Networking Requirements" section of *Cisco Unity Networking Options Requirements (With Microsoft Exchange),* available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/netrq.htm.

For information on changes in functionality, support, and requirements, refer to the following release notes:

- *Release Notes for Cisco Unity Bridge*, versions 3.0(1) through 3.0(6).
- *Release Notes for Cisco Unity*.

All referenced release notes are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

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, page 2-15
- Configuring the Bridge, page 2-16
- Adding Password Protection to the Bridge Administrator, page 2-18
- Testing Networking and SMTP Connectivity, page 2-18

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, page 2-19
- To Verify SMTP Connectivity, page 2-19
- To Set Permissions to Access the Interop Gateway Mail File, page 2-20
- To Send a Test Message to the Interop Gateway Mail File, page 2-20

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

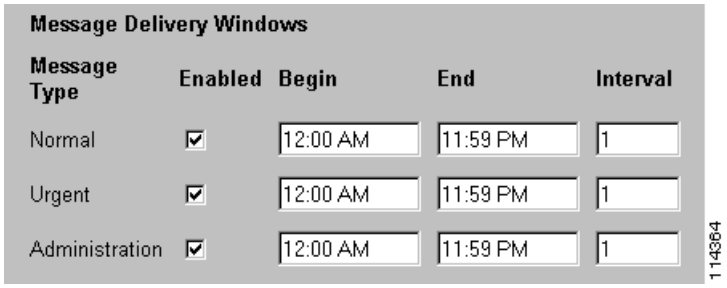
Note The most up-to-date version of BANANA is available at http://www.CiscoUnityTools.com. When you start BANANA, it checks the CiscoUnityTools website to see if a newer version is available, and if so, prompts you about upgrading.

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, page 2-27
- Approaches to Creating Bridge Subscribers, page 2-29
- 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
- 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
- After Creating Subscriber Accounts, page 2-35

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, page 2-36
- Single-Server Installations, page 2-36

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**.

Monitoring and Maintaining Bridge Networking

This chapter provides information on monitoring and maintaining Bridge Networking. See the following sections for more information:

- Controlling the Number of Ports Used for Outgoing Messages, page 3-1
- Bridge Analog Network and Node Analyzer (BANANA), page 3-3
- Bridge Traffic Analyzer, page 3-5
- Backing Up and Restoring a Bridge Server, page 3-6
- Changing the Interop Gateway Foreign Domain Name, page 3-9
- Moving the Interop Gateway Mail File, page 3-11
- Moving the UOmni Mail File, page 3-12
- Monitoring Recommendations, page 3-12

Controlling the Number of Ports Used for Outgoing Messages

Outgoing messages from the Bridge to an Octel node are placed in queues. The Bridge maintains three queues for each node—one queue each for normal and urgent messages, and a third for administrative tasks. Queued messages are processed in first-in-first-out (FIFO) order.

The Bridge can simultaneously use more than one port on the analog voice-fax card(s) in the Bridge server to send messages to a particular Octel node. For example, assume that there are several messages in the normal message queue for a specific node, and that the Bridge is using one port to transmit the messages. If an administrative or urgent message is then sent to that same node during the time that the normal message traffic is being transmitted, the Bridge will use another port to dial out to send the administrative or urgent message.

Two parameters on the System Settings page in the Bridge Administrator allow you to control the number of ports used for outgoing messages to a specific node: Queued Call Threshold and Max Ports Per Node. These values are applied to the normal and urgent outgoing message queues for each node. (Note that these values are not applied to administrative queues. Only one port at a time will ever be used for administrative calls to a particular node).

The value in Queued Call Threshold specifies the threshold number of messages that must be in the outgoing message queue of a specific node for an additional port to be used for message delivery. As the number of messages in the queue increases, an additional port is added when the number of messages in the queue reaches a multiple of this parameter.

For example, if the value of Queued Call Threshold is set to 10 (the default value), one port will be used for message delivery if there are fewer than 10 messages in the queue. For 10–19 messages, two ports will be used. For 20–29 messages, three ports will be used, and so on. The total number of ports used is limited by the Max Ports Per Node parameter.

Queued Call Threshold is also used to determine when to disconnect a port used for outgoing messages to a specific node. As the number of messages in the queue decreases, a port is disconnected when the number of messages in the queue is below the next lower multiple of this parameter. When only two ports are in use, as the number of messages in the queue drops below half of this parameter, the second port is disconnected.

For example, if the value of the Queued Call Threshold is set to 10, three ports will be used for message delivery if there are 20–29 messages in the queue. As the number of messages in the queue decreases, the third port is not disconnected until the number of messages in the queue drops to 10 or fewer. When the number of messages drops to 5 or fewer messages, the second port is disconnected, so only one port is used to transmit the remaining messages.

The Max Ports Per Node parameter allows you to specify the maximum number of ports that can be used simultaneously to deliver messages to a particular node. Again, this value is applied to each message queue. For example, if Max Ports Per Node is set to 4 (the default value), it is possible that 9 ports could be used simultaneously to send normal, urgent, and administrative messages to a specific node. In this example, up to 4 ports could be used for normal messages; up to 4 ports could be used for urgent messages; and 1 port would be used for administrative messages. (Outbound administrative calls to the same node are not placed simultaneously. Only one port at a time will ever be used for administrative calls to a particular node.)

Determining Optimal Values for Queued Call Threshold and Max Ports Per Node

The optimal values for Queued Call Threshold and Max Ports Per Node depend on the number of ports, the number of nodes, and on message traffic patterns. Start with the default values for these parameters, and use the Bridge Traffic Analyzer to observe message traffic patterns to see whether you need to adjust the settings. See the "Bridge Traffic Analyzer" section on page 3-5 for more information.

The default values should be appropriate for light message traffic because with light traffic, the thresholds for the parameters are never reached. The default values should also be sufficient for installations with medium traffic and a small to medium number of Octel nodes. However, installations with medium traffic and ten or more Octel nodes, or with high traffic, should carefully watch the reports generated by the Bridge Traffic Analyzer, and adjust the values for the parameters as necessary.

If you decide to adjust the values for Queued Call Threshold and Max Ports Per Node, keep in mind that the Bridge ports are used for both outgoing messages to Octel nodes and incoming messages to the Bridge. If message traffic is heavy enough, it is possible to adjust the values such that all the ports will be used for outgoing messages, leaving no ports available for incoming messages. If this is a concern, you may want to designate one or more ports to be used only for incoming calls. The Line Status page in the Bridge Administrator allows you to specify whether each line is to be used for both incoming and outgoing calls or only for incoming calls.

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.

If you have already installed BANANA, skip to the "Getting Started Using the BANANA admin to Monitor Analog Activity" section on page 3-4.

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 Cisco Unity Tools website to see if a newer version is available, and if so, prompts you about upgrading.

Getting Started Using the BANANA admin to Monitor Analog Activity

If the Bridge server sends and receives many messages, it is likely that when you view the call traces in BANANA admin, you will see some errors. Do not be alarmed; due to the nature of analog transmissions, some errors are to be expected. In order to send and receive messages between the Bridge and an Octel node, DTMF tones are exchanged in accordance with the Octel analog protocol. It is not uncommon for line noise to interfere with the transmission or reception of DTMF tones, particularly when the tones are transmitted over the PSTN. In an environment with Cisco CallManager and Cisco gateways, the circuit-switched calls are encoded and repackaged into IP packets. The transcoding must be precise. The DTMF duration and interdigit timing on the Cisco gateways or Cisco CallManager must be set to a value between 80 and 100 milliseconds. Incorrect settings will cause transmission problems.

When you first set up Bridge Networking, we recommend that you use the BANANA admin to frequently monitor the analog activity (at least daily, though more frequently if necessary) to find and fix problems. By monitoring the analog activity, you will become familiar with the message traffic patterns and learn what ratio of errors is within a "normal" range.

The following procedure will get you started using the BANANA admin. Refer to the BANANA Help file for details about how to do each task.

To Get Started Using the BANANA admin

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

Step 2 If you have not already done so, configure the log and output folder locations.

Step 3 Optionally, adjust the **Hours of Data to Retain in Database** setting.

You may want to increase the setting if there is sufficient disk space on the Bridge server. Be careful if you decrease the setting from the default because only the most recent call data will be retained after the call data is subsequently processed, and you could lose data that you need for troubleshooting a problem.

Step 4 Click **Process Call Data**.

BANANA processes the call traces and then displays information about incoming and outgoing calls in the Calls grid. Calls that resulted in errors are displayed in the Errors grid.

Step 5 Click **View Node Totals** to display the Totals per Octel Node dialog box.

This view of the data is useful for identifying communication problems with a particular Octel node. For example, if the ratio of errors to calls for a particular Octel node is significantly higher than for the other nodes, you can investigate the problem further by doing the following sub-steps:

a. Make note of the serial number of the Octel node with a high number of errors.

b. Click the main BANANA admin window, and then click the **octelserialnumber** column header in the Calls grid to sort the calls by Octel serial number.

c. In the Calls grid, click a row with the problematic serial number that has an exitcode other than OK. The corresponding record in the Errors grid is highlighted. This record provides specific details regarding the condition under which the call was terminated, including the state of the protocol that was in process, and the reason why the call could not be completed.

d. Click **View Call Detail for Selected Call**. This view of the data displays the mailboxes that were involved in the call, which is useful if someone notifies you that they received an NDR, or if you are tracking down a directory update problem that was logged in the Windows Event Viewer. You can also use this view of the data to verify that the message (or other action) involved in the failed call was repeated later in a successful call.

Step 6 Configure BANANA to monitor the call traces for error conditions, and to log warnings or errors to the Windows Event Viewer. As needed, you can adjust the notification settings.

Bridge Traffic Analyzer

The Bridge Traffic Analyzer is a report-generation utility that reads the call traces on the Bridge server, and generates a graph and a summary table that can be saved as a comma-separated value (CSV) file. The Bridge Traffic Analyzer is available for download at http://www.CiscoUnityTools.com.

The Bridge Traffic Analyzer generates reports by using the data in the call traces in the \Starfish\Log directory on the Bridge server. The Call Log Retention parameter on the System Settings page in the Bridge Administrator allows you to specify the number of days of call history to retain. For more information about the Call Log Retention setting, see the "System Settings" section on page 8-1.

In the reports, the direction of the queues is from the perspective of Cisco Unity:

- The inbound queue contains messages from Octel nodes that the Bridge sends to Cisco Unity. Messages in the inbound queue are sent to Cisco Unity by using SMTP. Therefore, unless Cisco Unity or Domino is down, messages move very quickly through the inbound queue.
- The outbound queue contains messages from Cisco Unity that the Bridge sends to the appropriate Octel nodes. Messages in the outbound queue are sent through the ports on the analog voice-fax card(s) on the Bridge server to the Octel nodes. Because the number of ports is a fixed resource, and because analog transmissions are slow in comparison to SMTP, it is possible that messages will back up in the outbound queue.

The Bridge Traffic Analyzer provides the following reports:

- **Port Availability**—Shows the availability of ports on the analog voice-fax card(s) on the Bridge server. You can choose to show how many ports were available to take calls from Octel nodes, how many ports were busy, or both. The summary CSV file presents a table with the maximum and minimum number of available ports for each hour during the day.
- **Message Queue Activity**—Shows how many messages and how much data is passing through the inbound and outbound message queues on the Bridge server. You can choose to show the number of messages, the message queue size in megabytes, or both. The summary CSV file presents a table with the maximum number of messages in the inbound and outbound queues, and the maximum message size of the inbound and outbound queues for each hour during the day.
- **Message Latency**—Shows the length of time that messages stayed in the outbound queue before being delivered to the Octel nodes. You can select a time range for the report (the default is 24 hours), and you can choose which Octel nodes to see in the report (by default, all nodes are shown). The Message Latency report shows only the outbound queue. Messages arrive quickly from Cisco Unity, but are delivered by analog lines to their target Octel node; therefore, it is possible for messages to back up in the queue waiting for an available port.
- **Node Message Traffic**—Shows how many messages and how much data is passing between different Cisco Unity and Octel nodes. For example, you can use this report to determine which Octel nodes a specific Cisco Unity server is messaging with most heavily. You can select one or more Cisco Unity nodes, one or more Octel nodes, and a time range for the report.

Refer to the Help file that comes with the Bridge Traffic Analyzer for more information about these reports.

Backing Up and Restoring a Bridge Server

This section explains how to backup data on the Bridge server, and how to restore that data to another Bridge server. See the following sections:

- Backing Up the Bridge Server, page 3-6
- Replacing a Bridge Server and Restoring Data, page 3-7

Backing Up the Bridge Server

Both offline and online backups are supported for the Cisco Unity Bridge server. When backing up the Bridge server, you need to back up only the configuration and data files; you do not need to back up the Bridge software because it is easy to reinstall the Bridge software on another server. The files that you back up on the Bridge server include:

- WAV files of voice names for Octel and Unity node directory entries
- A database that contains configuration data and information about Octel and Unity node directory entries
- Configuration files

For a list of backup and restore software supported for the Bridge server, refer to the "Supported Backup Software" section of *Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software,* available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm.

No unique software agents are required. We recommend that you do the backup during off-peak hours.

See the following procedures for step-by-step instructions:

- To Do an Online Backup of the Bridge Server by Using Third-Party Backup and Restore Software, page 3-6
- To Do an Offline Backup of the Bridge Server, page 3-7

To Do an Online Backup of the Bridge Server by Using Third-Party Backup and Restore Software

Step 1 Back up the following files and directories:

- SN (include all files and subdirectories)
- Starfish\Db\StarFish.mdb
- VPIM\Vpim.cfg
- VPIM\Propagation (include all files and subdirectories)

Note The paths above are relative to the drive and directory in which the Bridge software is installed. The default is D:\Bridge.

For detailed instructions, refer to the manufacturer documentation or Help.

To Do an Offline Backup of the Bridge Server

Step 1 On the Bridge server, on the Windows Start menu, click **Programs > Administrative Tools > Services**, and stop the following services:

- Digital Networking
- Unity Bridge

Any calls that are in progress are allowed to finish before the services are stopped.

Step 2 Back up the following directories:

- SN (include all files and subdirectories)
- Starfish\Db\StarFish.mdb
- VPIM\Vpim.cfg
- VPIM\Propagation (include all files and subdirectories)

Note The paths above are relative to the drive and directory in which the Bridge software is installed. The default is D:\Bridge.

Step 3 On the Windows Start menu, click **Programs > Administrative Tools > Services**, and start the following services:

- Digital Networking
- Unity Bridge

Step 4 Close the Services window.

Replacing a Bridge Server and Restoring Data

When replacing a Bridge server, you install the Bridge software and then restore the configuration and data files.

To Replace a Bridge Server and Restore Data

We recommend that you replace the Bridge server during off-peak hours. Note that the paths below are relative to the drive and directory in which the Bridge software is installed. The default is D:\Bridge.

Step 1 Install the new Bridge server according to the instructions in the "Overview of Mandatory Tasks for Installing the Cisco Unity Bridge" chapter of *Cisco Unity Bridge Installation Guide*, *Release 3.0*. The guide is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/big/dom/index.htm.

Step 2 After the post-installation restart of the new Bridge server, on the Windows Start menu, click **Programs > Administrative Tools > Services**, and stop the following services:

- Digital Networking
- Unity Bridge

Step 3 On the Cisco Unity server on which the Interop Gateway service is running, click **Programs > Administrative Tools > Services**, right-click **CsDomInteropGty**, and select **Stop**. Messages from Cisco Unity subscribers and from the Bridge will be held in the Interop Gateway mail file until you restart the service.

Step 4 If the old Bridge server has failed or is already offline, skip to Step 10. Otherwise, confirm that there are no more messages queued in the following directories on the Bridge server:

- VPIM\Xcode\Inbound
- VPIM\VM\In
- IN

Messages pass through these directories quickly, in the order listed, before reaching the analog queues.

Step 5 In the Bridge Administrator, click **Queue Status** to see if there are outgoing messages in the analog queues. Wait for all messages in the queues to be sent before proceeding. You can view call progress on the Line Status page to determine when the outbound calls have finished.

Step 6 On the Bridge server, on the Windows Start menu, click **Programs > Administrative Tools > Services**, right-click **Unity Bridge**, and select **Stop**. Any incoming calls that are in progress are allowed to finish before the service is stopped. When the Unity Bridge service has been stopped, the Bridge is unable to accept calls from the Octels.

Step 7 Confirm that there are no more messages queued in the following directories on the Bridge server:

- Starfish\Out
- Out
- VPIM\Xcode\Outbound
- VPIM\Internet\Out

Messages pass through these directories quickly, in the order listed, before being sent via SMTP to Domino.

Step 8 If you have a recent backup, skip to Step 9. Otherwise, back up the following directories:

- SN (include all files and subdirectories)
- Starfish\Db\StarFish.mdb
- VPIM\Vpim.cfg
- VPIM\Propagation (include all files and subdirectories)

Step 9 Shut down the old Bridge server.

Step 10 Restore the following directories from the backup medium to the new Bridge server:

- SN (include all files and subdirectories)
- Starfish\Db\StarFish.mdb
- VPIM\Vpim.cfg
- VPIM\Propagation (include all files and subdirectories)

Step 11 If the fully qualified domain name (FQDN) of the new Bridge server is the same as the old Bridge server, skip to Step 12. Otherwise, change the FQDN in the following places:

- In the Bridge delivery location(s) on the Cisco Unity bridgehead server.

  If there are only a few delivery locations, use the Cisco Unity Administrator to change the FQDN on each delivery location.

If there are many delivery locations, modify the delivery locations by using the Cisco Unity Bulk Import wizard. Refer to the section "Modifying Existing Delivery Locations" in the Cisco Unity Bulk Import wizard Help for details on preparing a CSV file and running the wizard.

- If you are using host files for name resolution with the Bridge, change the FQDN in the host file on the applicable Domino or SMTP relay server.
- If you are using DNS for name resolution with the Bridge, change the FQDN in the MX and A records on the DNS server.

Step 12 On the Windows Start menu, click **Programs > Administrative Tools > Services**, and start the following services:

- Digital Networking
- Unity Bridge

Step 13 Close the Services window on the Bridge server.

Step 14 On the Cisco Unity server on which the Interop Gateway service is running, click **Programs > Administrative Tools > Services**, right-click **CsDomInteropGty**, and select **Start**.

Step 15 Close the Services window.

Changing the Interop Gateway Foreign Domain Name

The following task list provides an overview of how to change the name of the Foreign domain used by the Interop Gateway. We recommend that you change the Foreign domain name after normal business hours when message traffic is light, because messages to AMIS recipients may be sent back as undeliverable until the Foreign domain name has been changed in every place that it is stored.

1. On the Cisco Unity server on which the Interop Gateway service—CsDomInteropGty—is running, rerun the Interop Gateway Configuration wizard and change the Foreign domain name. This updates settings stored in SQL and in the registry. (The settings in SQL will replicate to all other Cisco Unity servers in your installation, but the registry change must be made on each Cisco Unity server, as described in the next step.)
2. If your installation consists of multiple Cisco Unity servers (either Digitally Networked servers and/or secondary failover servers), you must change the Foreign domain name stored in the registry. Open the Advanced Settings Tool in Tools Depot to change the Foreign Domain name in the setting Networking – Change Interop Gateway Foreign Domain Name (Domino Only).
3. Restart Cisco Unity.
4. In Domino Designer, copy the agent from the CommServer\Utilities\Domino\Agents\UpdateRemoteSubscribers directory of a Cisco Unity server, and paste it in names.nsf on a "hub" Domino server that pushes out directory changes.
5. In the Domino Administrator, run the agent to change the Foreign domain name in the Forwarding Address field of each Person document that corresponds to an AMIS, Bridge, or VPIM subscriber.

The following procedure provides detailed steps.

To Change the Interop Gateway Foreign Domain Name

Step 1 On the Cisco Unity server on which the Interop Gateway service—CsDomInteropGty—is running, 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 AMIS messages to the Interop Gateway mail file. The Interop Gateway Configuration wizard creates a new Foreign domain document with the specified name.
- If you choose to use an existing Foreign domain, click the Foreign domain name on the list.

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** and 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.

Step 9 If your installation consists of only one Cisco Unity server, skip to Step 23.

Otherwise, log on to another Cisco Unity server (either a Digitally Networked server or a secondary failover server), and on the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 10 In the left pane of the Tools Depot window, expand **Administration Tools**, and double click **Advanced Settings Tool**.

Step 11 In the Unity Settings list, click **Networking – Change Interop Gateway Foreign Domain Name (Domino Only)**.

Step 12 Enter the new Foreign domain name in the New Value field, and click **Set**.

Step 13 Restart Cisco Unity.

Step 14 Repeat Step 9 through Step 13 on each Cisco Unity server.

Step 15 Optionally, copy the contents of the CommServer\Utilities\Domino\Agents\UpdateRemoteSubscriber directory on the Cisco Unity server to the Domino server where you will run Domino Designer. If you can browse to the Cisco Unity server from Domino Designer to open the agent, you can skip this step. Note that the UpdateRemoteSubscriber directory contains the files:

- Agent code to update interop foreign domain.txt
- UUIsFA.nsf

The following steps describe how to copy and run the agent UUIsFa.nsf. If you are familiar with working with Domino agents, you may prefer to create a new agent by using the code in the .txt file instead. Also note that the following steps are specific to Domino R6.5. Adjust them as needed for other Domino versions. Refer to your Domino documentation for additional information.

Step 16 Open Domino Designer, and click **Open an Existing Database**.

Step 17 Browse to UUIsFA.nsf, and click **Open**.

Step 18 Click **View > Go To > Agents**.

Step 19 In the right pane, right-click the agent, and click **Copy**.

Step 20 Click **File > Database > Open**, and open names.nsf on a hub Domino server that pushes out directory changes.

Step 21 Click **View > Go To > Agents**.

Step 22 Click **Edit > Paste** to add the agent to names.nsf.

Step 23 In the right pane, double-click **Update Unity Interop Subscriber Forwarding Address** to open the agent.

Step 24 Click the **Save** icon, close the agent dialog box, close the agent window, and exit Domino Designer.

Step 25 Open the Domino Administrator, click **File > Database > Open**, and open **names.nsf** on the hub Domino server.

Step 26 Click **Actions > Update Unity Interop Subscriber Forwarding Address** to run the agent. (The agent may be located on the Actions > Other menu.)

Step 27 In the Old Foreign Domain dialog box, enter the old Foreign domain name and click **OK**.

Step 28 In the New Foreign Domain dialog box, enter the new Foreign domain name and click **OK**.

The agent searches the Person documents that corresponds to AMIS, Bridge, and VPIM subscribers looking for the old Foreign domain name in the Forwarding Address field. When it finds a match, the agent changes the domain name portion of the Forwarding Address field to the new Foreign domain name.

Moving the Interop Gateway Mail File

To move the Interop Gateway mail file to another Domino server:

1. Move the mail file.
2. Update the Foreign domain document with the new Domino server name.
3. Rerun the Interop Gateway Configuration wizard, and use the existing Foreign domain.

The following procedure provides detailed steps.

To Move the Interop Gateway Mail File

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

Step 2 In the list in the right pane, right-click the Interop Gateway mail file, and click **Move**.

Step 3 In the Move Database dialog box, specify the destination Domino server, and click **OK**.

Step 4 Click the **Configuration** tab.

Step 5 In the left pane, expand **Messaging > Domain**.

Step 6 In the right pane, click the Foreign domain document used by the Interop Gateway, and click **Edit Domain**.

Step 7 In the Foreign domain document, click the **Mail Information** tab.

Step 8 In the Gateway Server Name field, enter the Domino server name where the Interop Gateway mail file was moved to.

Step 9 Click **Save and Close**.

Step 10 On the Cisco Unity server on which the Interop Gateway service is running, browse to the directory in which Cisco Unity is installed (the default location is C:\CommServer).

Step 11 Double-click **UnityDominoInterOpSetup.exe** to run the Interop Gateway Configuration wizard.

Step 12 On the Welcome screen, click **Next**.

Step 13 On the Configure the Interop Gateway screen, click **Use an Existing Foreign Domain**, and click **Next**.

Step 14 On the Domain screen, confirm that the new Domino server is listed in the Domino Server field, and click **Next**.

Step 15 On the Interop Gateway Log On Properties Screen, we recommend that you click **Log On as Local System Account**.

Step 16 Click **Next** to review the Foreign Domain settings, and then click **Finish**. When the wizard finishes, a message box displays to let you know whether the configuration was successful.

Moving the UOmni Mail File

For information on moving the UOmni mail file, refer to the "UOmni Mail File" section in the "Cisco Unity Data and Log Files" chapter in the *Cisco Unity Maintenance Guide*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/maint/maint405/dom/index.htm.)

Monitoring Recommendations

Refer to the *Unity and Bridge Monitoring Recommendations* spreadsheet, available on http://www.ciscounitytools.com/Documents.htm. This Excel spreadsheet contains tabs that include events, performance monitor counters, and services that we recommend for monitoring Cisco Unity and Bridge deployments.

Troubleshooting Bridge Networking

Overview: Bridge Troubleshooting

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

- Configuration Problems, page 4-1
- Overview of Troubleshooting Logs, Traces, and Tools, page 4-4
- Messages Are Not Delivered from Cisco Unity to Octel, page 4-7
- Messages Are Not Delivered from Octel to Cisco Unity, page 4-24
- Directory Messages Are Not Processed, page 4-42

Configuration Problems

If you have just configured Cisco Unity and the Bridge for networking, and you encounter problems, review the following list to verify that your configuration follows all of these basic guidelines. If needed, go to the "Messages Are Not Delivered from Cisco Unity to Octel" section on page 4-7 or the "Messages Are Not Delivered from Octel to Cisco Unity" section on page 4-24 as applicable for detailed troubleshooting steps.

Verify the following:

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

4. The Octel server(s) are running a supported protocol. The Octel servers must be running Octel analog networking. Neither Octel digital networking nor the VOICENET protocol is supported by the Bridge.
5. The name of the Bridge server can be resolved. If there are name resolution problems, you need to reconfigure DNS or add a reference to the Bridge server in the HOSTS file on the server that sends outbound SMTP messages to the Bridge server. See the "Configuring the Bridge and Testing the Configuration" section on page 2-15 for more information.
6. Use the Domino Administrator to confirm that the Interop Gateway Foreign domain document exists. Also verify that the Interop Gateway mail file itself exists on the Domino server and directory specified in the Foreign domain document. See the "To Confirm That the Interop Gateway Foreign Domain Document and Mail File Exist" procedure on page 4-3. Note that if Cisco Unity cannot find the Interop Gateway mail file, you should see errors in Event Viewer. In this case:
   - If the Interop Gateway Foreign domain document and/or mail file has been inadvertently deleted, reconfigure the Interop Gateway, as described in the "Configuring the Interop Gateway" section on page 2-7. Be sure to use the same Foreign domain name that you used previously.
   - If you suspect that the Interop Gateway mail file may have been inadvertently moved to another Domino server, see the "Moving the Interop Gateway Mail File" section on page 3-11 for information on how to move the mail file such that Cisco Unity is aware of the change.
7. Use the Domino Administrator to confirm that Interop Gateway Foreign domain name is correct. See the "To Confirm That the Foreign Domain Name Settings Are Correct" procedure on page 4-3.

   If you determine that the Foreign domain name has been changed in some but not all of the places where the name is stored, refer to the "Changing the Interop Gateway Foreign Domain Name" section on page 3-9 for information on how to change the foreign domain such that Cisco Unity is aware of the change.
8. A Cisco Unity server is configured as the bridgehead. If ConfigMgr has not been run on a Cisco Unity server:
   - The CsBridgeConnector service will fail to start.
   - The Bridge-related pages and fields in the Cisco Unity Administrator will not be accessible.

   See the "Designating the Bridgehead Server" section on page 2-9.
9. Search scopes include the Cisco Unity bridgehead server. The Subscriber and Blind Addressing search scopes (which are set on the Network > Primary Location > Addressing Options page in the Cisco Unity Administrator) must be set to either the dialing domain or global level. This must be done for each Cisco Unity server in the network. The search scopes for the auto-attendant and directory handlers (which are configured separately) must also include the Cisco Unity bridgehead server.
10. Each Bridge delivery location is correctly configured.
11. Each Unity node and Octel node on the Bridge server is correctly configured. To verify the serial number of an Octel node based on the phone number of the node, see the "Optional: Gathering or Confirming Octel Node Serial Numbers (Bridge 3.0(6) or Later)" section on page 2-5.
12. The correct serial number and legacy mailbox ID is assigned to each Cisco Unity subscriber.

Procedures for Troubleshooting Configuration Problems

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

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

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

Step 3 Open the Foreign domain document.

Step 4 Confirm that the Foreign domain name is correct.

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

Step 6 Close the Foreign domain document.

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

To Confirm That the Foreign Domain Name Settings Are Correct

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

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

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

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

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

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

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

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

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

e. Close the Person document.

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

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

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

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

Step 9 Close the Advanced Settings tool.

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

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

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

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

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

Step 15 Write down the name in the NodeValue column.

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

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

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

Overview of Troubleshooting Logs, Traces, and Tools

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

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

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

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

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

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

- **Bridge Analog Network And Node Analyzer (BANANA)**—BANANA is a stand-alone application that runs on the Bridge server. It is designed to assist with monitoring and troubleshooting analog communication between the Bridge and Octel nodes in the analog network. It also provides detail and summary call activity information. BANANA monitors and parses the call traces described below, and presents the data in a format that makes the call traces easier to understand. BANANA is available on the Bridge CD. We recommend that you install it.

- **Call Traces**—(Also referred to as the Starfish logs or SFLOGs.) The files are located on the Bridge server in the <Bridge Path>\Starfish\Log directory. To obtain information about messages coming from or going to Octel servers through the Bridge voice-fax card(s), you increase the Call Tracing Level on the System Settings page in the Bridge Administrator. The log records actions that the Bridge service attempts, notes whether those actions are completed successfully, and records the reasons for failed actions. Within the Log directory are files named SFLOG.YYYYMMDD.LOG, where YYYY is the year, MM is the month, and DD is the day. Each file contains log entries for one hour of the day; the filename indicates which hour. The directory also contains the log file SFLOG.LOG, to which the Bridge server adds current entries, and which is then saved to the applicable hour log. Log files that are older than 24 hours are overwritten.

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

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

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

- **Call Queue Logs**—Call Queue log files are located on the Bridge server in the <Bridge Path>\Starfish\Log directory. The Call Log Retention setting on the Systems Settings page allows you to specify the number of days that logs are saved. A separate file is used for each day. Files are named CallLog_YYYYMMDD.LOG where YYYY is the year, MM is the month and DD is the day. Call logs are used by the Bridge Traffic Analyzer for generating reports on Bridge activity.
- **Line Status Page**—The Line Status page in the Bridge Administrator allows you to monitor status information for the phone lines of the Bridge server as it communicates with Octel servers. It also allows you to enable or disable specific phone lines for the Bridge server.
- **Queue Status Page**—The Queue Status page in the Bridge Administrator allows you to monitor status information in the outbound message queue on the Bridge server.
- **Bridge Traffic Analyzer**—The Bridge Traffic Analyzer is a report generation utility that reads the call queue log files on the Bridge server and generates a graph and a summary table that can be saved as a comma-separated value (CSV) file. The Bridge Traffic Analyzer is available in Tools Depot on the Cisco Unity server, or you can download it from http://www.CiscoUnityTools.com. This tool typically is used for monitoring purposes and not for troubleshooting. However, if messages are not getting delivered in a timely manner, this tool will help you understand Bridge port utilization. See the "Bridge Traffic Analyzer" section on page 3-5 for more information.
- **Event Viewer**—The Bridge services record errors and warnings to the Windows Event Viewer application log. The Windows Event Viewer on the Bridge server should be one of the first places you look when troubleshooting.

Tools for Troubleshooting Communication Problems Between the Bridge and Cisco Unity

- **Event Viewer**—The Bridge services record errors to the Windows Event Viewer application log.

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

Tools for Troubleshooting Problems with the Interop Gateway

- Cisco Unity Diagnostic Tool—Because the Interop Gateway runs as a service on a Cisco Unity server, you can set traces for it by using the Cisco Unity Diagnostic tool. The "To Set Diagnostic Traces" procedure on page 4-11 provides details.
- Event Viewer—The Interop Gateway logs errors to the application log in Event Viewer.
- Domino Administrator—You can use the Domino Administrator for:
  - Opening the Interop Gateway mail file.
  - Viewing the Interop Gateway Foreign domain document.
  - Opening Log.nsf or using Domino Messaging Tracking

Tools for Troubleshooting Directory Synchronization Problems on the Cisco Unity Server

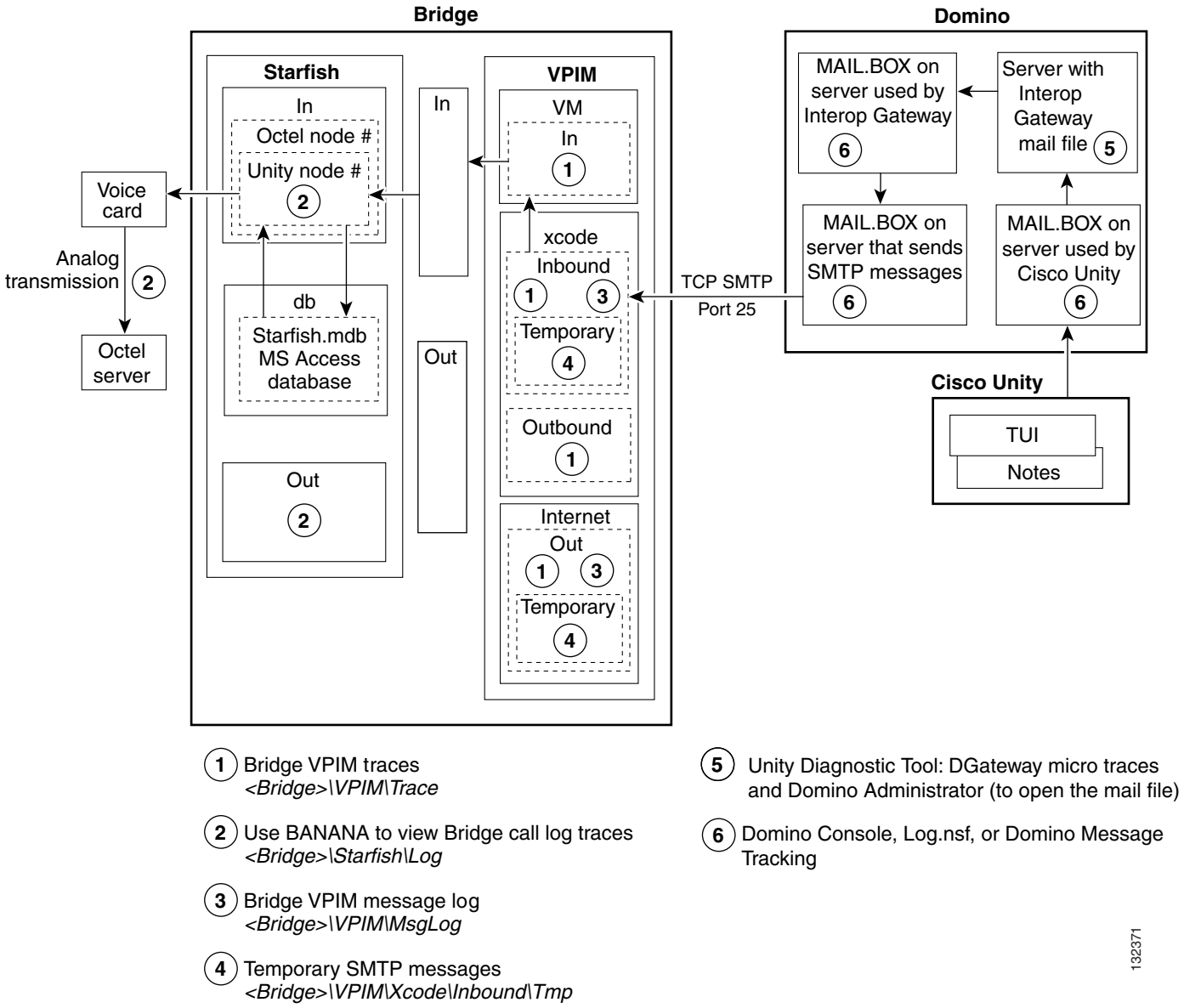
- **Event Viewer**—The CsBridgeConnector service, which is responsible for keeping the directories on the Bridge and Cisco Unity synchronized, logs several errors to the Windows Event Viewer application log on the Cisco Unity bridgehead server (that is, the Cisco Unity server that is configured for networking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

Messages Are Not Delivered from Cisco Unity to Octel

This section provides troubleshooting information to help you determine why voice messages from Cisco Unity are not received on an Octel system. When a Cisco Unity subscriber sends a voice message to an Octel subscriber, the message is passed by Cisco Unity to Domino, which routes the message to the Interop Gateway mail file. The Interop Gateway converts the message to VPIM format (with proprietary extensions) and hands it back to Domino to be sent to the Bridge via SMTP. The Bridge converts the received VPIM message to an Octel message and sends it to the Octel node via analog lines.

Figure 4-1 illustrates at a high level the message flow from Cisco Unity to Octel, and the troubleshooting logs, traces, and tools that you can use to determine where the problem is along the path. For simplicity, the illustration shows messages originating from MAIL.BOX on the Domino server used by Cisco Unity for mail delivery. (This is the Domino server on which the mail file of the Person document for the Cisco Unity server is located.) This is true when subscribers use the TUI to send messages, but when subscribers use the DUC-enabled Notes client, messages originate from the Domino server on which the mail file of the subscriber sending the message is located.

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



Bridge In and Out Directories

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

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

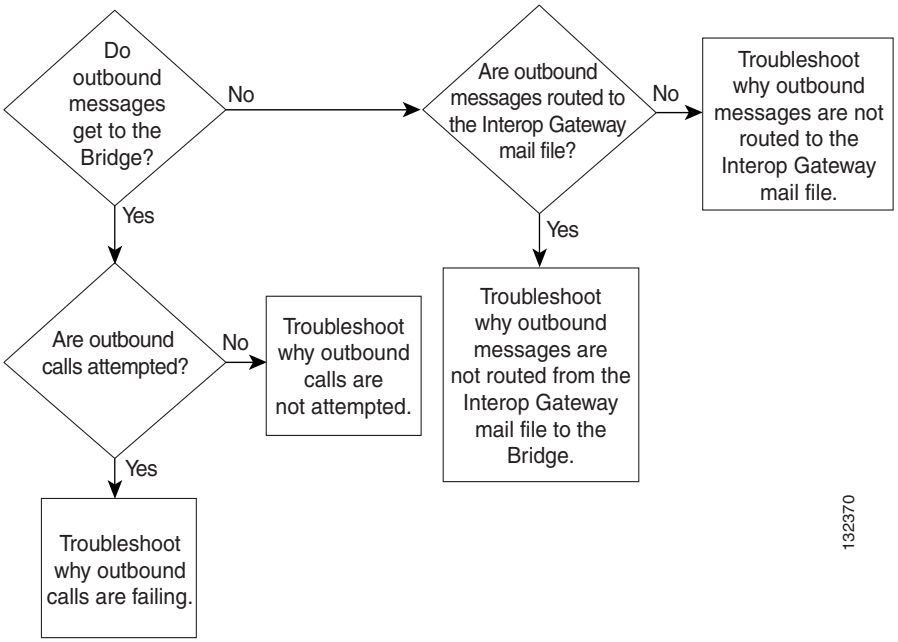
Table 4-1 Messages Queue Up When the Unity Bridge Service and/or the Digital Networking Service Stop

Digital Networking Service	Unity Bridge Service	Messages from Cisco Unity to the Octels...	Messages from the Octels to Cisco Unity...
Running	Not Running	Will queue up in the Bridge\In directory until the Unity Bridge service starts and picks them up.	Will queue up on the Octel servers.
Not Running	Running	Will be stuck in MAIL.BOX on the Domino server that sends outgoing SMTP messages.	Will queue up in the Bridge\Out directory until the Digital Networking service starts and picks them up.
Not Running	Not Running	Will be stuck in MAIL.BOX on the Domino server that sends outgoing SMTP messages.	Will queue up on the Octel servers.

Troubleshooting Why Messages Are Not Delivered from Cisco Unity to Octel

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

Figure 4-2 Troubleshooting Why Messages Are Not Delivered from Cisco Unity to Octel



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

1. Enable the various logs and traces as described in the "Enabling Logs and Traces" section on page 4-10.
2. If you are tracking down problems with messages that have already been sent, skip to the next step to begin troubleshooting. Otherwise, send a test message from a Cisco Unity subscriber to a remote Octel subscriber. Make a note of the serial number of the receiving Octel node.

3. Do Messages from Cisco Unity Get to the Bridge? If messages do not get to the Bridge, skip to Step 6.
4. Are Outbound Calls Attempted? If outbound calls are not attempted, go to the "Troubleshooting Why Outbound Calls Are Not Attempted" section on page 4-14.
5. Determine why calls from the Bridge to the Octels are failing. Go to the "Troubleshooting Why Outbound Calls Are Failing" section on page 4-14.
6. Are Outbound Messages Routed to the Interop Gateway Mail File?

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

   If messages are routed to the Interop Gateway mail file, go to the "Troubleshooting Why Outbound Messages Are Not Routed from the Interop Gateway Mail File to the Bridge" section on page 4-21.
7. Reset the logs and traces as described in the "After You Finish Troubleshooting" section on page 4-23.

Enabling Logs and Traces

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

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

To Install BANANA

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

Step 1 Disable virus scanning services and the Cisco Security Agent service, if applicable.

Step 2 Insert the Cisco Unity Bridge compact disc in the CD-ROM drive, and browse to the **BANANA** directory.

Step 3 Double-click **setup.exe**.

Step 4 Click **OK** at the welcome screen.

Step 5 If applicable, change the directory where BANANA will be installed.

Step 6 Click the **Installation** button.

Step 7 If applicable, change the program group where BANANA will appear.

Step 8 Click **Continue**.

Step 9 If a Version Conflict message box is displayed warning that a file being copied is not newer than the file on your system, click **Yes** to keep the existing file.

Step 10 When the installation is done, click **OK**.

Step 11 Enable virus-scanning and the Cisco Security Agent services, if applicable

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

To Enable Troubleshooting Logs and Traces on the Bridge Server

Step 1 In the Bridge Administrator, go to the **Digital Networking** page and set Retention Days For Temporary SMTP Messages to the number of days that you want to retain the messages.

Step 2 Set the Tracing Level to **Flow**.

Step 3 Click **Save**.

Step 4 Go to the **System Settings** page, and set the Call Tracing Level to **Verbose**.

Step 5 Click **Save**.

To Set Diagnostic Traces

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

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

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

Step 4 Scroll down and enable the following micro traces:

- DGateway
- MALLn
- NoteCommon

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

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

Do Messages from Cisco Unity Get to the Bridge?

To Determine Whether Outbound Messages Get to the Bridge

Step 1 On the Bridge server, browse to the **Bridge\Vpim\Xcode\Inbound\Tmp** directory.

Messages are saved in this directory when the Retention Days For Temporary SMTP Messages field on the Digital Networking page in the Bridge Administrator is set to a value greater than zero.

Step 2 If there are messages in this directory, SMTP messages are being successfully sent from Domino to the Bridge server. Go to the "Are Outbound Calls Attempted?" section on page 4-12.

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

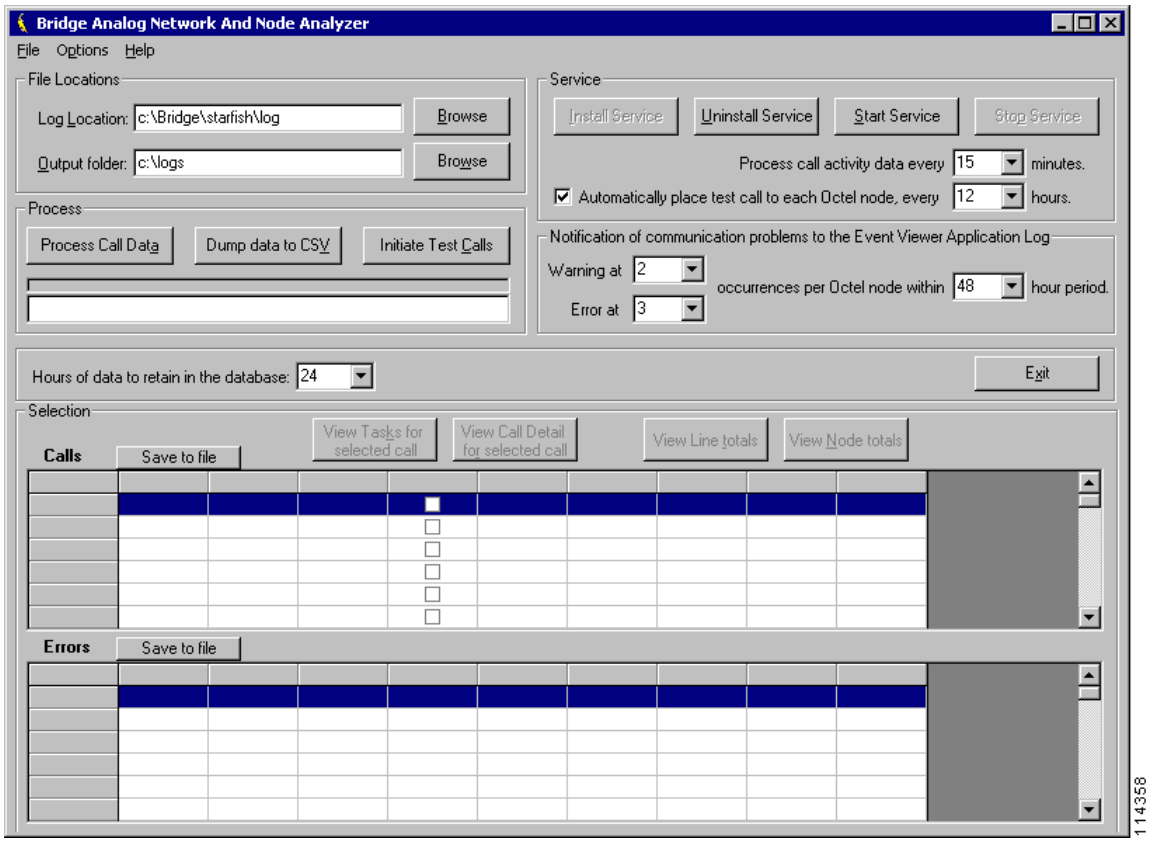
Are Outbound Calls Attempted?

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

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

To Determine Whether Calls Are Attempted

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

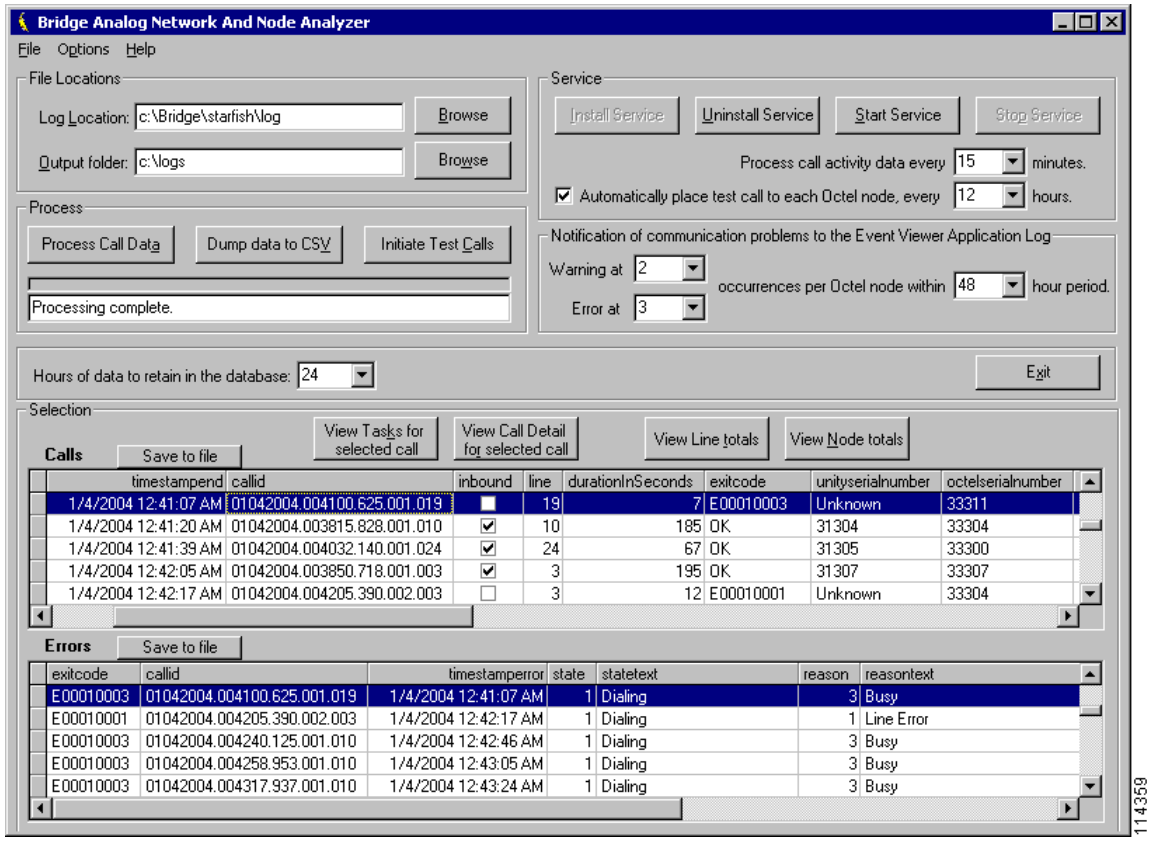


Step 2 If you have not already done so, set the Log Location and Output Folder location as described in the following sub-steps. If you have already set the locations, skip to Step 3.

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

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

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



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

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

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

Step 5 If you do not see any outbound calls, or if you were looking for a specific outbound call and do not see it, go to the "Troubleshooting Why Outbound Calls Are Not Attempted" section on page 4-14.

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

Troubleshooting Why Outbound Calls Are Not Attempted

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

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

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

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

Troubleshooting Why Outbound Calls Are Failing

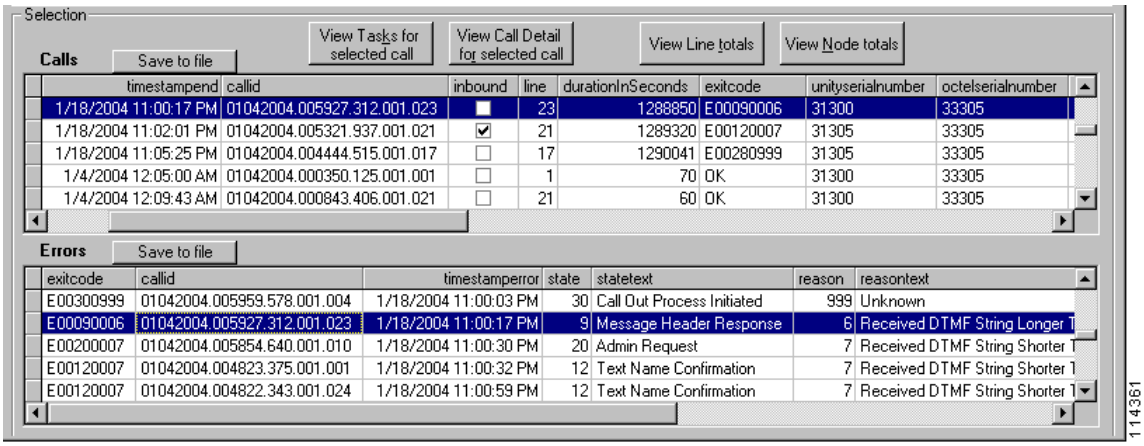
When the Bridge uses a Cisco gateway connected to Cisco CallManager for analog connectivity with the Octels, verify that:

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

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

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

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



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

Table 4-2 Configuration and Other Problems That Result in Outbound Call Failures

Error Code	Description
E00010001	A Line Error occurs when the Bridge detects a line problem after going off hook and prior to dialing a phone number. The most common cause of this condition is failure to receive dial tone on the line. Plug an analog phone into the source of one of the analog lines and verify that you hear dial tone, and can successfully dial a phone number.

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

Error Code	Description
E00010003	The Bridge detected a busy condition after dialing the specified phone number for this node. On busy analog networks, this condition can occur occasionally. However, repeated failures to contact the remote node because of busy line conditions can result in messages not being delivered in a timely manner. Repeated failures can also result in the messages being returned to the Cisco Unity senders, when the number of retries exceeds the Attempts If Busy setting on the Bridge System Settings page. Confirm that the phone number specified for the node being called is correct by dialing the phone number from a regular phone. If you verify that the phone number is correct, but continue to experience busy conditions with this node, contact the system administrator of this Octel system to see if there is a reason the system is often unavailable.
E00010004	The Bridge detected ringing on the line after dialing the specified phone number for this node, but the call was never answered. Confirm that the phone number specified for the node being called is correct, by dialing the phone number from a regular phone and verifying that the expected voice mail system answers.
E00020005	Verify that: • The Octel server(s) are supported. The only supported Octel servers are those listed in "Supported Voice Messaging Systems" section of the *Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm. • The Octel server(s) are running a supported protocol. The Octel servers must be running Octel analog networking. Neither Octel digital networking nor the VOICENET protocol is supported by the Bridge.
E00030005	On an outbound call, after the Bridge sends the BD handshake tones, it expects to receive the CDD handshake response. When an outbound call from the Bridge is answered, but no CDD is received, this may indicate: • That the call was not answered by an Octel that supports the Octel Analog Networking feature. Check the phone number for the Octel Node profile of the serial number that the Bridge was attempting to contact. • Poor line quality. If the line quality is such that the audio being sent to the Bridge is not clear, this is usually the first state in which you will observe problems. To determine what the Bridge may be experiencing when calling this number, plug an analog phone into the source of one of the analog lines and dial the phone number as configured for this Octel Node. • Failure to detect call progress, such as ringback or busy tone, on the analog line. If the Bridge is able to place a call successfully, but receives no further indication of the call progress within 20 seconds, it will assume the call has been answered and begin to send the BD wake up tones. If the call has not actually been answered, you may receive this error. To determine what the Bridge may be experiencing when calling this number, plug an analog phone into the source of one of the analog lines and dial the phone number as configured for this Octel Node. Also verify that: • The Octel server(s) are supported. The only supported Octel servers are those listed in "Supported Voice Messaging Systems" section of the *Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/bridge30/sysreq/30bsysrq.htm. • The Octel server(s) are running a supported protocol. The Octel servers must be running Octel analog networking. Neither Octel digital networking nor the VOICENET protocol is supported by the Bridge.

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

Error Code	Description
E00050005	On an outbound call from the Bridge to an Octel, after the Bridge sends the BD handshake tones and receives the CDD handshake response, it sends a string of 18 DTMF digits, including the serial number of the Octel that the Bridge is attempting to communicate with. If no response is received from the Octel, it is possible that the serial number sent from the Bridge did not match the serial number of the Octel that answered the call. Verify that the serial number and phone number for the Octel Node profile are correct.
E00070005	If observed repeatedly, this may indicate that the remote system does not have a location profile configured for the Unity Node serial number that the Bridge server is using. When the Bridge sends the session header, this packet includes the Unity Node serial number that the Bridge is calling as. If the remote system requires this serial number to be configured on a location profile, and it does not have one matching the serial number that the Bridge used in the session header, the remote system will disconnect without sending the session header response. Note that not all systems that support Octel analog networking require confirmation of the calling serial number at this stage. Also note that E00070005 will also be the exitcode if the remote system did not receive all of the session header DTMF digits as sent by the Bridge, even if location profiles on both systems are configured correctly.
E00160010	Confirm that the Octel node with which the Bridge communicates supports the fax feature.
E00160099	Confirm that all gateway and phone system devices between the Octel and the Bridge support fax transmission.
E00010017	Upon dialing the phone number of the remote system, the Bridge received intercept tones from the phone service provider, indicating the number dialed is out of service. The Bridge counts this condition against the Attempts If Busy threshold configured on the System Settings page. When the number of retries exceeds the Attempts If Busy setting, all messages queued for delivery to this remote system will be returned to the Cisco Unity senders as non-deliverable. Confirm that the phone number specified for the node being called is correct by dialing the phone number from a phone.

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

There are many reasons why the analog delivery of an outbound message can fail, for example, a bad connection caused by an interruption on the line or poor line quality. However, message-delivery failure can also occur as a result of problems delivering one particular message. In Cisco Unity Bridge 3.0(5) and later, the Max Play Attempts Per Message setting was added to the System Settings page in the Bridge Administrator to allow you to control how long the Bridge attempts to deliver a particular message before returning it to the sender as undeliverable. (See the "System Settings" section on page 8-1 for more information on the Max Play Attempts Per Message setting.)

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

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

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

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

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

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

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

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

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

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

- When the message sent from Cisco Unity contains a serial number that the Bridge does not recognize. Each Cisco Unity subscriber account must have a serial number and legacy mailbox ID in order to exchange messages with Octel subscribers. When a Cisco Unity subscriber sends a message to an Octel subscriber, the serial number of the Cisco Unity subscriber is added to the header of the message. The Bridge will not deliver a message when the serial number in the message header does not match a serial number of a Unity Node configured on the Bridge.

- When any of the analog delivery thresholds configured on the System Settings page has been hit. (The System Settings thresholds are: Attempts if Busy, Attempts on No Answer, Attempts on Bad Connection, Max Play Attempts Per Message, Max Retention Time - Normal, and Max Retention Time - Urgent.)
- When the message recording is in an invalid WAV file format (either the message was recorded using a codec that cannot be converted by the Bridge, or the WAV attachment contains no voice data).
- When the mailbox of the Octel recipient is full.
- When the recipient mailbox does not exist on the Octel node.

Are Outbound Messages Routed to the Interop Gateway Mail File?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For example:

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

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

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

1. Confirm that the following Domino servers are running:
   - The Domino server used by Cisco Unity for message delivery (or the Domino server on which the sending subscriber mail file is located).
   - The Domino server on which the Interop Gateway mail file is located.
   - All Domino servers used in message routing to the Domino server on which the Interop Gateway mail file is located.

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

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

3. Check to see if the message is stuck in MAIL.BOX on the Domino server used by the sending Cisco Unity for message delivery, or if the message is stuck in MAIL.BOX on any of the Domino servers that are involved in routing messages to the Domino server on which the Interop Gateway mail file is located. Refer to your Domino documentation for more information.
4. Check to see if there is a quota on the Interop Gateway mail file and if Domino is configured to not deliver messages if the mail file is over quota.
5. Check the Interop Gateway Foreign domain document to make sure that it contains the correct server name and mail file name.
6. Go to the "After You Finish Troubleshooting" section on page 4-23 for details on how to reset the logs and traces to default values, and if you were unable to solve the problem, instructions are provided on how to gather the necessary logs to provide to Cisco TAC.

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

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

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

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

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

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

For example:

5234@ParisBridge2.europe.cisco.com

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

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

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

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

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

Step 2 Click the **Files** tab.

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

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

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

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

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

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

DNS: Non-existent domain

---

2. Verify that the Bridge server full computer name is configured correctly, as follows:
   a. In the Cisco Unity Administrator, go to the Bridge Delivery Location page for the applicable remote Octel server on the Cisco Unity bridgehead server.
   b. Confirm that the name in the Bridge Server Full Computer Name field on the Bridge Delivery Location page of the Cisco Unity Administrator exactly matches the Bridge Server Full Computer Name field on the Digital Networking page in the Bridge Administrator on the Bridge server.
   c. Confirm that both settings match the Full Computer Name of the Bridge server as listed in the Windows System Control Panel on the Network Identification tab on the Bridge server.
3. Verify that the Bridge server full computer name resolves to the IP address of the Bridge.

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

   If using DNS is not an option, then confirm that there is an entry in the HOSTS file on the Domino server that handles outbound SMTP messages for your Domino network. (On servers running Microsoft Windows, the HOSTS file is located in the %windir%\System32\Drivers\Etc directory.)
   a. In a command prompt window on the Bridge server, enter the command ping <Bridge Server Full Computer Name>.
   b. If an IP address is returned, confirm that it is the IP address of the Bridge server.

      If the returned response is Unknown host <Bridge Server Full Computer Name>, then correct the IP address in DNS or the HOSTS file, as applicable.
4. Check to see if the message is stuck in MAIL.BOX on the Domino server used by the Interop Gateway for message delivery, or if the message is stuck in MAIL.BOX on any of the Domino servers that are involved in routing messages to the Domino server which sends outbound SMTP messages. Refer to your Domino documentation for more information.
5. Confirm that Domino server(s) used for relaying messages outside of the organization is not restricted from relaying messages to unknown servers, or if they are restricted, that relaying messages to the Bridge server IP address is explicitly allowed. Depending on your network configuration, you may need to manually enter a DNS MX record for the Bridge in order to allow SMTP message delivery to it, but usually this is not necessary.
6. If there is a firewall between the Bridge and the SMTP relay server, confirm that SMTP traffic is allowed on port 25.

7. Check to see whether e-mail leaving your Domino organization is re-routed to a smart host, non-Domino corporate SMTP relay server, secure e-mail server, or any other traffic filtering server that may not route SMTP messages to the Bridge server.
8. Go to the "After You Finish Troubleshooting" section on page 4-23 for details on how to reset the logs and traces to default values, and if you were unable to solve the problem, instructions are provided on how to gather the necessary logs to provide to Cisco TAC.

After You Finish Troubleshooting

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

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

Reset the following logs and traces:

- In the Bridge Administrator, on the Digital Networking page:
  - Reset the Retention Days For Temporary SMTP Messages back to 0 (zero). (These messages consume significant hard disk space, so you should always configure this setting to zero unless you are troubleshooting and also monitoring hard disk consumption.)
  - Reset the Tracing Level back to None. (Typically, these logs do not consume significant hard disk space, so you may choose to leave the Tracing Level set to Flow.)
- If you need to provide the Interop Gateway log file to Cisco TAC, do the "To Retrieve the Unity Diagnostic Tool Log File for the Interop Gateway" procedure on page 4-23 (which includes instructions for setting the traces back to the default).

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

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

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

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

Step 3 Click **Select Logs.**

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

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

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

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

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

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

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

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

Step 12 Exit the Cisco Unity Diagnostic tool.

To Reset the Unity Diagnostic Tool to Default Traces

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

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

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

Step 4 Exit the Cisco Unity Diagnostic tool.

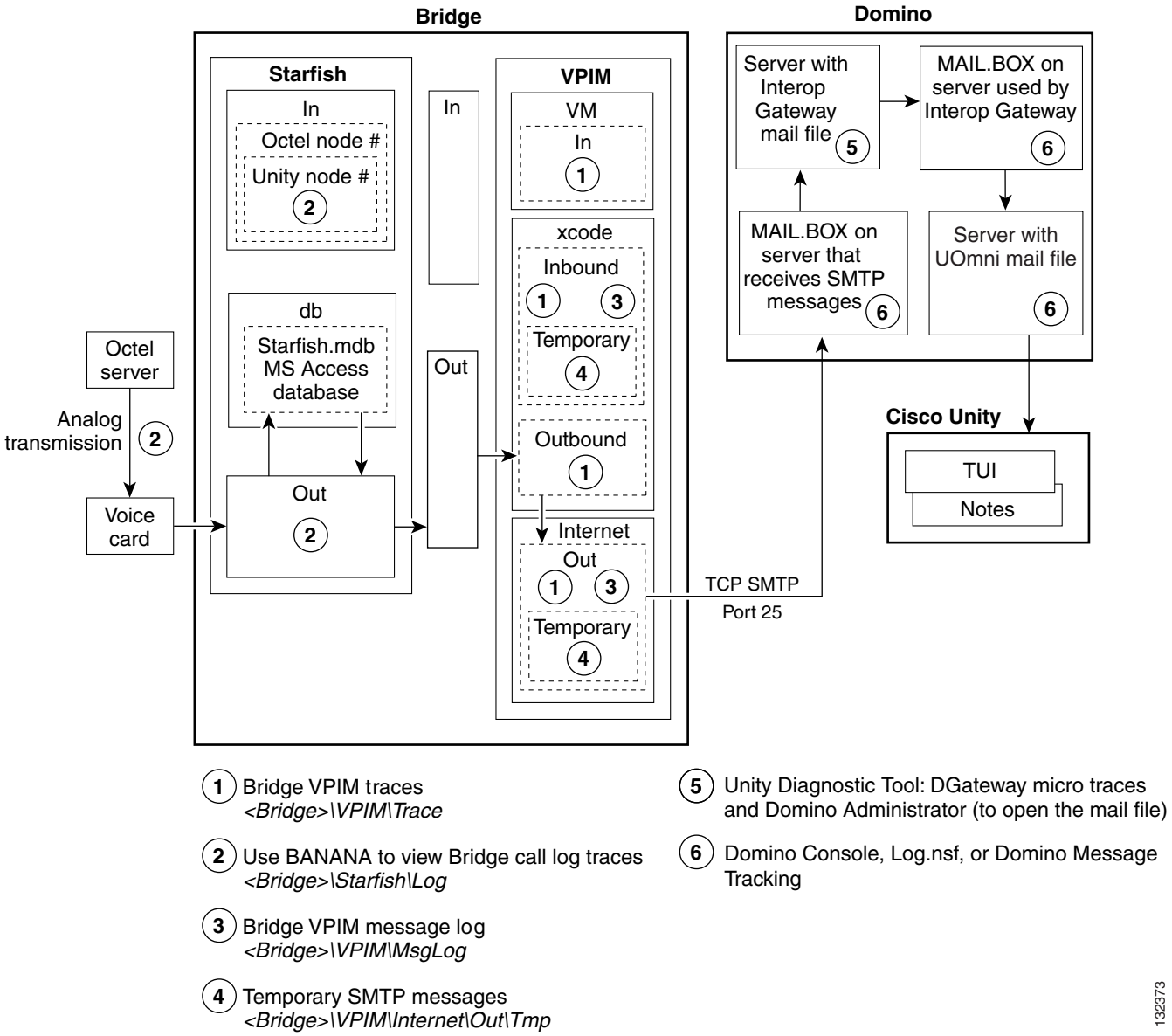
Messages Are Not Delivered from Octel to Cisco Unity

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

When an Octel subscriber sends a voice message to a Cisco Unity subscriber, the Octel node passes the message to the Cisco Unity Bridge via analog lines. The Bridge converts the received Octel message to a VPIM message (with proprietary extensions) and sends it via SMTP to the Interop Gateway mail file. The Interop Gateway converts the message to a WAV file and hands it back to Domino to be delivered to the Cisco Unity subscriber mail file. Note that the Cisco Unity server does not play a role in delivering voice messages from an Octel node to a Cisco Unity subscriber mailbox.

Figure 4-3 illustrates at a high level the message flow from Octel to Cisco Unity, and the troubleshooting logs, traces, and tools that you can use to determine where the problem is along the path.

Figure 4-3 Troubleshooting Message Flow from Octel to Cisco Unity



Bridge In and Out Directories

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

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

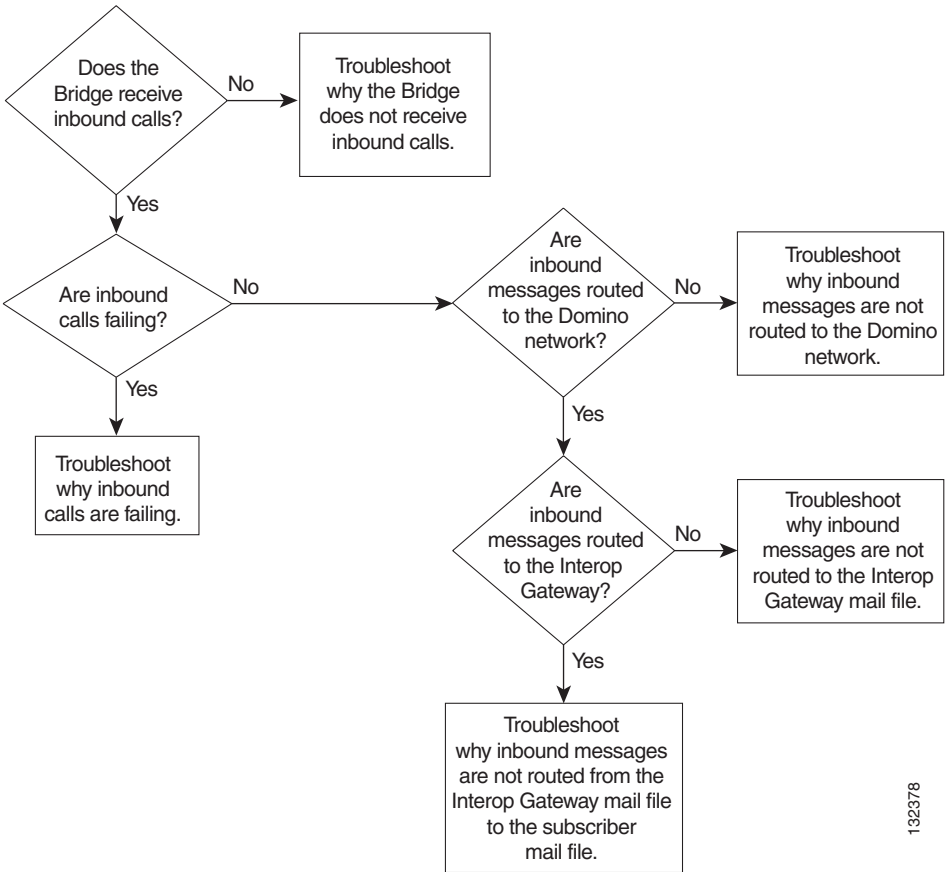
Table 4-3 Messages Queue Up When the Unity Bridge Service and/or the Digital Networking Service Stop

Digital Networking Service	Unity Bridge Service	Messages from Cisco Unity to the Octels...	Messages from the Octels to Cisco Unity...
Running	Not Running	Will queue up in the Bridge\In directory until the Unity Bridge service starts and picks them up.	Will queue up on the Octel servers.
Not Running	Running	Will be stuck in MAIL.BOX on the Domino server that sends outgoing SMTP messages.	Will queue up in the Bridge\Out directory until the Digital Networking service starts and picks them up.
Not Running	Not Running	Will be stuck in MAIL.BOX on the Domino server that sends outgoing SMTP messages.	Will queue up on the Octel servers.

Troubleshooting Why Messages Are Not Delivered from Octel to Cisco Unity

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

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



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

1. Enable the various logs and traces as described in the "Enabling Logs and Traces" section on page 4-27.
2. If you are tracking down problems with messages that have already been sent, skip to the next step to begin troubleshooting. Otherwise, send a test message from an Octel subscriber to a Cisco Unity subscriber. Make a note of the serial number of the sending and receiving nodes.
3. Does the Bridge Receive Inbound Calls? If the Bridge does not receive inbound calls, see the "Troubleshooting Why the Bridge Does Not Receive Inbound Calls" section on page 4-30.
4. Are Inbound Calls Failing? If inbound calls are failing, see the "Troubleshooting Why Inbound Calls Are Failing" section on page 4-32.
5. Are Inbound Messages Routed to the Domino Network? If inbound messages are not routed to the Domino Network, see the "Troubleshooting Why Inbound Messages Are Not Routed to the Domino Network" section on page 4-37.
6. Are Inbound Messages Routed to the Interop Gateway Mail File? If inbound messages are not routed to the Interop Gateway mail file see the "Troubleshooting Why Inbound Messages Are Not Routed to the Interop Gateway Mail File" section on page 4-40.

   Otherwise, see the "Troubleshooting Why Inbound Messages Are Not Routed from the Interop Gateway Mail File to the Subscriber Mail File" section on page 4-40.
7. Reset the logs and traces as described in the "After You Finish Troubleshooting" section on page 4-41.

Enabling Logs and Traces

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

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

To Install BANANA

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

Step 1 Disable virus scanning services and the Cisco Security Agent service, if applicable.

Step 2 Insert the Cisco Unity Bridge compact disc in the CD-ROM drive, and browse to the **BANANA** directory.

Step 3 Double-click **setup.exe**.

Step 4 Click **OK** at the welcome screen.

Step 5 If applicable, change the directory where BANANA will be installed.

Step 6 Click the **Installation** button.

Step 7 If applicable, change the program group where BANANA will appear.

Step 8 Click **Continue**.

Step 9 If a Version Conflict message box is displayed warning that a file being copied is not newer than the file on your system, click **Yes** to keep the existing file.

Step 10 When the installation is done, click **OK**.

Step 11 Enable virus-scanning and the Cisco Security Agent services, if applicable

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

To Enable Troubleshooting Logs and Traces on the Bridge Server

Step 1 In the Bridge Administrator, go to the **Digital Networking** page and set Retention Days For Temporary SMTP Messages to the number of days that you want to retain the messages.

Step 2 Set the Tracing Level to **Flow**.

Step 3 Click **Save**.

Step 4 Go to the **System Settings** page, and set the Call Tracing Level to **Verbose**.

Step 5 Click **Save**.

To Set Diagnostic Traces

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

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

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

Step 4 Scroll down and enable the following micro traces:

- DGateway
- MALLn
- NoteCommon

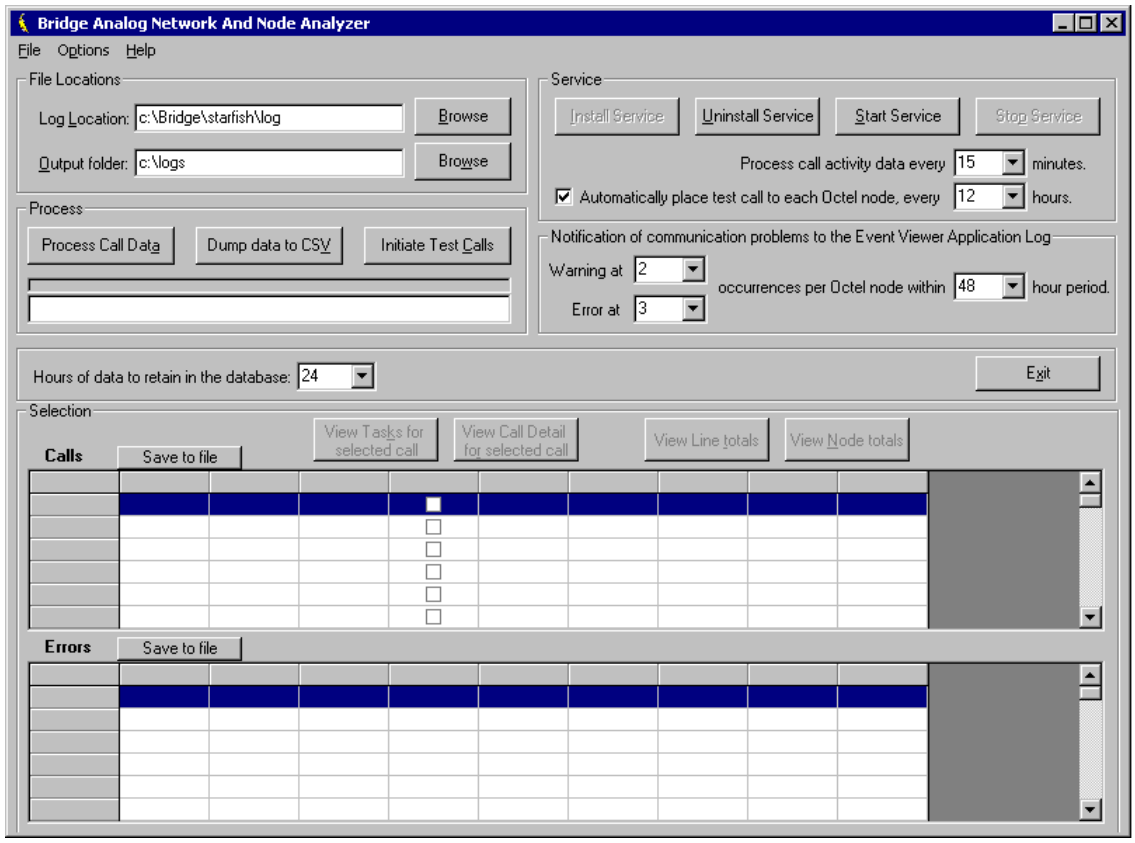
Step 5 Click **Next** and then click **Finish**.

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

Does the Bridge Receive Inbound Calls?

To Determine Whether Messages from the Octels Get to Bridge

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

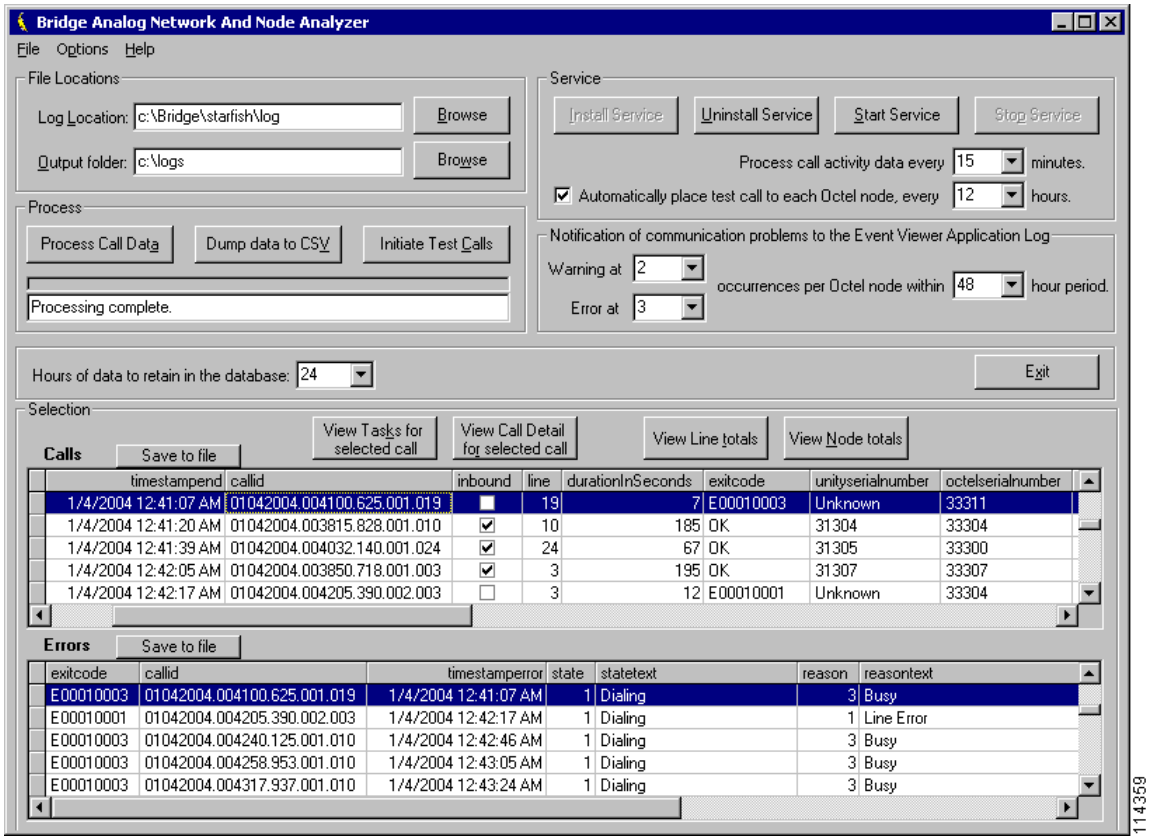


Step 2 If you have not already done so, set the Log Location and Output Folder location as described in the following sub-steps. If you have already set the locations, skip to Step 3.

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

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

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



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

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

Step 5 If you do not see any inbound calls, or if you were looking for a specific inbound call and do not see it, go to the "Troubleshooting Why the Bridge Does Not Receive Inbound Calls" section on page 4-30.

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

Troubleshooting Why the Bridge Does Not Receive Inbound Calls

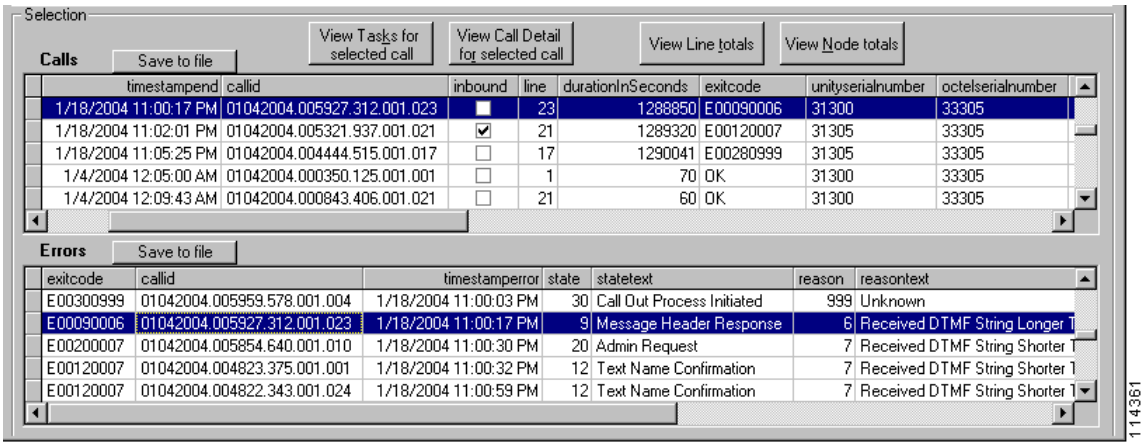
- Verify that the analog phone lines are plugged into the Bridge server and Octel servers.
- Verify the delivery phone number for the Bridge. Call the Bridge delivery phone number to see whether the Bridge answers. If the delivery phone number is correct and the Bridge answers, the inbound call will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

- If you have modified the default values for Queued Call Threshold and Max Ports Per Node on the System Settings page in the Bridge Administrator, and if message traffic is heavy enough, it is possible that all the ports will be used for outgoing messages, leaving no ports available for incoming messages. If this is a concern, you may want to designate one or more ports to be used only for incoming calls. The Line Status page in the Bridge Administrator allows you to specify whether each line is to be used for both incoming and outgoing calls or only for incoming calls. See the "Controlling the Number of Ports Used for Outgoing Messages" section on page 3-1 for more information.

Are Inbound Calls Failing?

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

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



If the inbound calls have error codes, or if you were looking for a specific inbound call and it has an error code, go to the "Troubleshooting Why Inbound Calls Are Failing" section on page 4-32.

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

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

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

Verify that the message appears in the Bridge\VPIM\Internet\Out\Tmp directory. If the message is there, go to the "Are Inbound Messages Routed to the Domino Network?" section on page 4-37.

Troubleshooting Why Inbound Calls Are Failing

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

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

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

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

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

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

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

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

Error Code	Description

E00040013	On an inbound call from an Octel to the Bridge, after the Bridge receives the BD handshake tones and sends the CDD handshake response, the Bridge expects to receive an encrypted string of 18 DTMF digits that includes the serial number of the node that the Octel is attempting to communicate with. If the Bridge hangs up without sending a response, it is possible that the serial number sent from the Octel did not match any of the Unity Node profiles configured on the Bridge.
	
	On the Bridge server, verify that the serial number on each Unity Node is correct, and that a Unity Node with the correct serial number has been created for each node that the Bridge represents within the Octel network.
	
	If the serial numbers in the Unity Node profiles on the Bridge are correct, then the calling Octel may be sending an incorrect serial number. At this point in the call, the Bridge does not know the serial number of the calling Octel server. The easiest way to find out which Octel called is to look at CallManager or PBX log files. If you do not have access to the phone system log files, and if there are only a few Octel servers in the network, then all of the node profiles on each Octel server can be checked for an incorrect serial number. However, when there are many Octel servers in the network, checking every node profile on every Octel server to find an incorrect serial number when you do not know the number you are looking for can be very time consuming. If this error appears repeatedly, the following steps may help to determine the serial number that the calling Octel was attempting to contact.
	
	1. Browse to the \Bridge\Starfish\Log directory on the Bridge server.
	2. In Notepad, open the sflog.*.log for the period during which the behavior has been observed.
	3. Search for the string Initial Handshake Failed. You should see a sequence of events similar to the following:
	
	`Line 4: Call Received.`
	`Line 4: Playing 1.sph`
	`Line 4: Received BD`
	`Line 4: Playing CDD`
	`Line 4: Received 12*D8#93697B08#CB*`
	`Line 4: Initial handshake failed. Received either bad data or a request to communicate with a node that is not yet configured on Bridge.`
	`Line 4: Received`
	`Line 4: Incoming Call Completed.`
	
	Because Octel analog networking packets are encrypted, you cannot determine the serial number of the node that the Octel is attempting to communicate with by looking at the DTMF packet. But there is a decryption utility on the Bridge server that can be used to determine the serial number. For the decryption utility to work, you will need to find two occurrences of this handshake failure in the log file.
	
	4. Copy the DTMF packet from the “Received” line that appears immediately after “Playing CDD” for both occurrences. (In the example above, you would copy the packet 12*D8#93697B08#CB*, and if the above example included another occurrence of the handshake failure, you would also copy that DTMF packet.)
	5. On the Bridge server, open a command prompt window and change to the directory where starfish.exe is located. (The default location is \Bridge\Starfish\Bin.)
	6. At the command line in the bin directory, enter the following command:
	
	starfish -p <packet1> <packet2>
	
	Where <packet1> is the DTMF packet copied from the “Received” line of the first occurrence and <packet2> is the DTMF packet copied from the “Received” line of the second occurrence.
	
	The utility returns the possible matches for the serial number of the node that is being called. It is possible that the utility will return 30 or more matches, but most of them can be eliminated as possibilities because they contain more than 5 digits. For example:

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

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

Are Inbound Messages Routed to the Domino Network?

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

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

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

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

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

Step 2 Click the **Files** tab.

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

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

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

Step 6 Search for a line similar to the following:

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

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

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

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

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

Troubleshooting Why Inbound Messages Are Not Routed to the Domino Network

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Verify that the address that the Bridge uses to establish a network connection is to a server that accepts incoming SMTP messages for your Domino organization. Depending on your network configuration, this could be a Domino server with the SMTP Listener task enabled, or an ESMTP e-mail host that acts as a relay server, which then routes the messages to a Domino server(s).
   a. In a command prompt window on the Bridge server, enter the command **ping <Foreign Domain Name>**, where <Foreign Domain Name> is the Interop Gateway Foreign domain name.
   b. If an IP address is returned, confirm that it is the IP address of a server that accepts incoming SMTP messages to your Domino network.

      If the returned response is **Unknown host <Foreign Domain Name>**, then correct the IP address in DNS or the HOSTS file, as applicable.
5. Verify SMTP Connectivity as follows:
   a. Open a command prompt window on the Bridge server.
   b. Enter **telnet <Address> <Port>**. In this command:

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

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

   You should see a response similar to the following:

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

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

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

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

Are Inbound Messages Routed to the Interop Gateway Mail File?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Open log.nsf or use Domino Message Tracking to see if any routing errors are reported.
2. Verify that the applicable Connection documents are in place so that the Domino server on which the Interop Gateway mail file is located can route messages to the Domino server on which the subscriber mail file is located.
3. Check to see if the message is stuck in MAIL.BOX on the Domino server used by the Interop Gateway for message delivery, or if the message is stuck in MAIL.BOX on any of the Domino servers that are involved in routing messages to the Domino server on which the subscriber mail file is located. Refer to your Domino documentation for more information.
4. Check to see if there is a quota on the subscriber mail file and if Domino is configured to not deliver messages to mail files that are over quota.

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

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

2. Check to see whether, after entering the SMTP server, e-mail entering your organization is re-routed to a smart host, non-Domino corporate SMTP relay server, secure e-mail server, or any other traffic filtering server that may not route incoming SMTP messages to Domino.
3. Verify that the applicable Connection documents are in place so that the Domino server that receives incoming SMTP messages can route messages to the Domino server on which the Interop Gateway mail file is located.
4. Check to see if the message is stuck in MAIL.BOX on any of the Domino servers that are involved in routing messages to the Domino server on which the Interop Gateway mail file is located. Refer to your Domino documentation for more information.
5. If a Domino server is used for routing incoming SMTP messages from the Bridge, verify that the SMTP Listener is enabled.

After You Finish Troubleshooting

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

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

Reset the following logs and traces:

- In the Bridge Administrator, on the Digital Networking page:
  - Reset the Retention Days For Temporary SMTP Messages back to 0 (zero). (These messages consume significant hard disk space, so you should always configure this setting to zero unless you are troubleshooting and also monitoring hard disk consumption.)
  - Reset the Tracing Level back to None. (Typically, these logs do not consume significant hard disk space, so you may choose to leave the Tracing Level set to Flow.)
- If you need to provide the Interop Gateway log file to Cisco TAC, do the "To Retrieve the Unity Diagnostic Tool Log File for the Interop Gateway" procedure on page 4-41 (which includes instructions for setting the traces back to the default).

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

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

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

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

Step 3 Click **Select Logs.**

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

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

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

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

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

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

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

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

Step 12 Exit the Cisco Unity Diagnostic tool.

To Reset the Unity Diagnostic Tool to Default Traces

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

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

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

Step 4 Exit the Cisco Unity Diagnostic tool.

Directory Messages Are Not Processed

If voice messages between Cisco Unity and the Octels are delivered successfully in both directions, chances are that directory messages will be also be delivered successfully. As Figure 4-5 and Figure 4-6 illustrate, the trouble spots are similar. However, if you do encounter a problem with directory messages, see the "CsBridgeConnector Traces" section on page 4-44 for information on enabling the traces on the Cisco Unity bridgehead server.

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

- Full Synchronization of Bridge Subscribers with Octel Node Directories, page 4-45
- Full Synchronization of Cisco Unity Subscribers with the Unity Node Directories, page 4-46

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

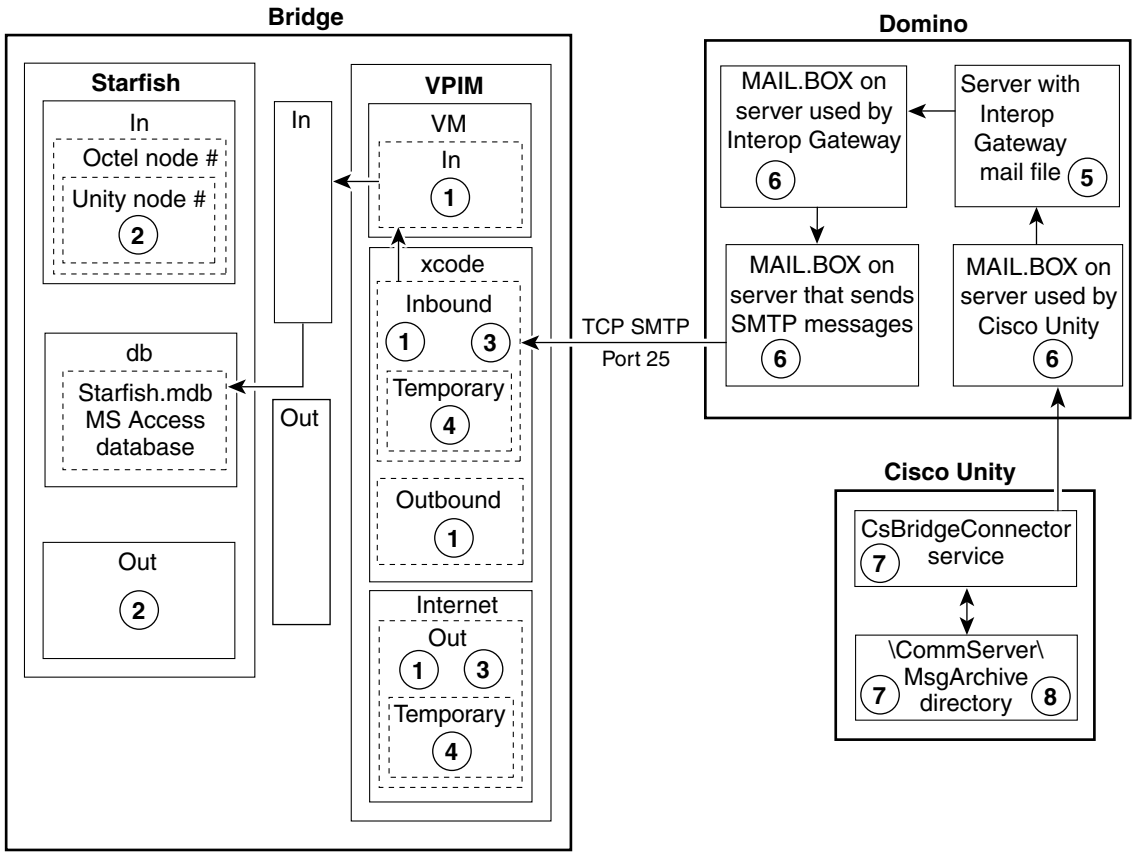
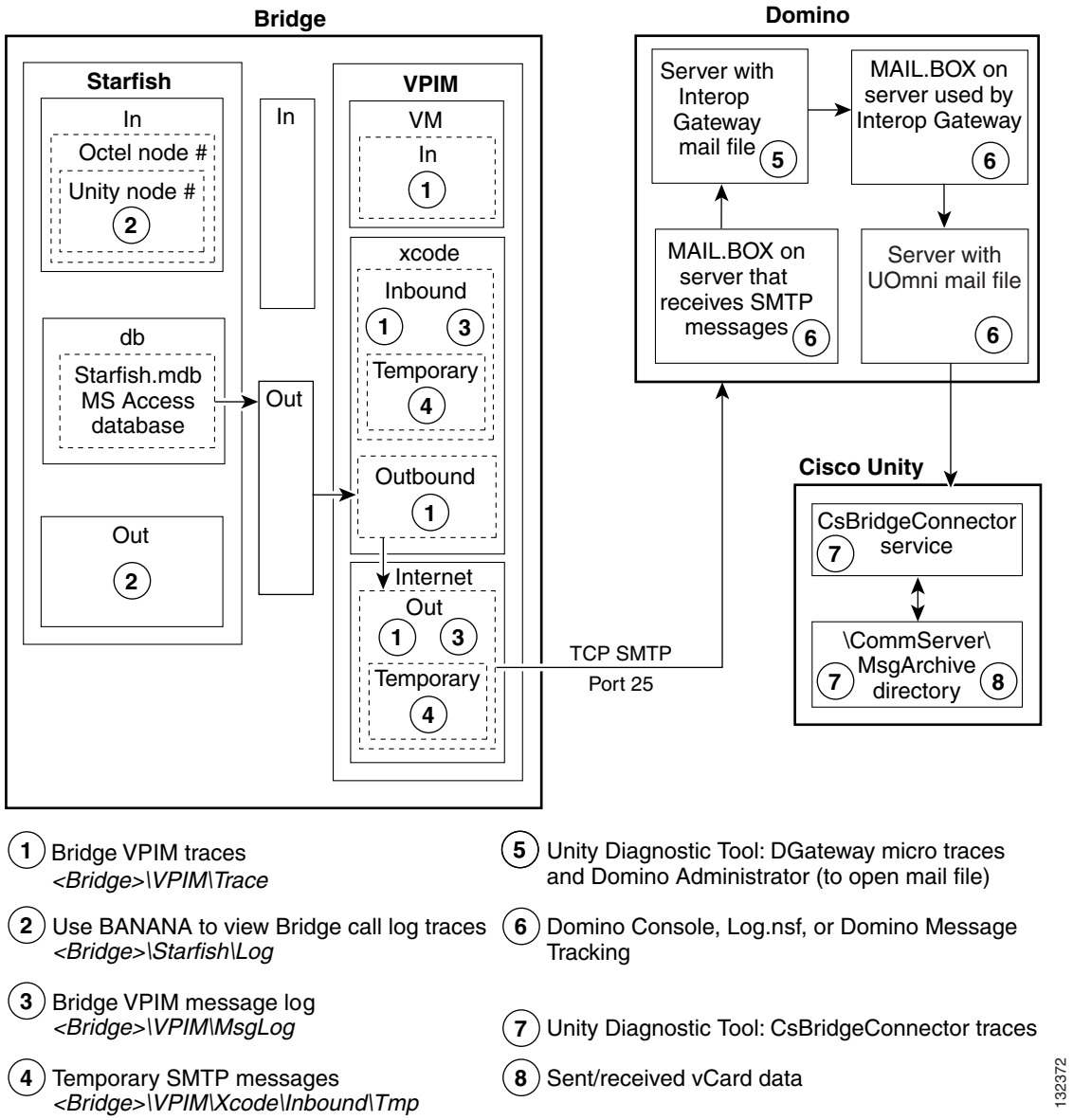


Figure 4-6 Troubleshooting Problems with Directory Messages from the Bridge to Cisco Unity



CsBridgeConnector Traces

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

To Enable CsBridgeConnector Traces

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Unity Diagnostic Tool**.

Step 2 On the Cisco Unity Diagnostic Tasks screen, click **Configure Macro Traces**. The Welcome to the Configure Macro Traces wizard displays.

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

Step 4 Expand **Bridge Directory Synchronization Traces**. Check the box next to the applicable macro trace(s):

- Basic Bridge delivery synchronization trace—Set this trace to verify that directory synchronization is working correctly within Cisco Unity.
- General Bridge delivery synchronization trace—Set this trace to narrow down directory synchronization problems to a specific Cisco Unity component.
- Extensive Bridge delivery synchronization trace—Set this trace to include additional Cisco Unity components and enable extensive logging.

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

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

Step 7 After the problem reoccurs, or sufficient time has passed to gather message data, in the tree in the left pane of the Unity Diagnostic tool, click **Processes > AvCsMgr**, and click the **Current** log file to view it.

The selected log file is formatted and displayed in the right pane.

Step 8 To export or save a copy of the log file, click **Action > Export List**.

Step 9 Name the file and save it to a location of your choice in .txt or .csv format.

Step 10 Disable all diagnostic traces that were activated in Step 4.

Full Synchronization of Bridge Subscribers with Octel Node Directories

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

To Synchronize Bridge Subscribers with Octel Node Directories

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

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Administration - Full synchronization of Bridge Subscribers with Octel Node Directories**.

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

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

Step 6 Click **Exit**.

Full Synchronization of Cisco Unity Subscribers with the Unity Node Directories

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

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

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

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

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

- To Trigger a Directory Synchronization of Cisco Unity Subscriber Information with the Unity Node Directories on the Bridge Server(s), page 4-46—This updates all Unity nodes on selected Bridge server(s).
- To Trigger a Directory Synchronization of Cisco Unity Subscriber Information with a Specific Unity Node Directory on the Bridge Server, page 4-46—This updates a specific Unity node on one Bridge server.

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

Step 1 On the Cisco Unity bridgehead server, in the Cisco Unity Administrator, go to the **Network > Bridge Options > Synchronization** page.

Step 2 Verify that each Bridge server to which directory information will be sent is configured with a Unity Node for each serial number listed in the Node ID table.

Step 3 In the Cisco Unity Bridge Servers table, check the check box next to each Bridge address to which Cisco Unity subscriber information should be sent.

Step 4 Click **Synchronize** to force a full synchronization of Cisco Unity subscribers with the subscriber directory on the Bridge. All Unity nodes on the selected Bridge server will be updated.

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

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

Step 1 On the Bridge server, open the Bridge Administrator.

Step 2 Click **Unity Nodes**.

Step 3 On the list of nodes, click the Unity node whose directory needs to be updated.

Step 4 Click **Edit**.

Step 5 Either print a copy of the page or write down the information that is on it.

Step 6 Click **Delete**, and then **OK** on the warning dialog box.

Step 7 Click **Add** to add back the node that you just deleted.

Step 8 Reenter the information from the deleted node (which you captured in Step 5), and click **Save**.

Directory information about all Cisco Unity subscribers associated with the same serial number as the Unity node will be sent to the Bridge.

CHAPTER 5

Advanced Troubleshooting Topics

This chapter contains advanced troubleshooting topics. In most cases, this information found in this chapter will not be needed for troubleshooting Bridge Networking problems. When you are troubleshooting a problem, always begin with the "Troubleshooting Bridge Networking" chapter.

See the following sections:

- Enabling and Interpreting Traces for the Brooktrout TR114 on the Bridge, page 5-1
- Using the Call Traces to Troubleshoot Why Messages Are Not Delivered from the Bridge to the Octels, page 5-14
- Using the Call Traces to Troubleshoot Why Messages Are Not Delivered from the Octel Node to the Bridge Server, page 5-19
- BANANA admin Call States, and Reasons for Communication Errors, page 5-21
- Bridge Compensates for Echoed Digits in Wakeup Packets, page 5-23

Enabling and Interpreting Traces for the Brooktrout TR114 on the Bridge

When experiencing analog communication problems between the Bridge and remote Octel nodes, the sflogs on the Bridge are most useful in determining the activity that is occurring on the analog calls. However, it is sometimes helpful to begin by determining what is occurring right at the TR114 voice board, as this can help pinpoint the exact source of the problem. This section describes how to enable and interpret traces of activity on the TR114 board.

Enabling Debug Traces for the Brooktrout TR114

To Enable Debug Traces for the Brooktrout TR114

Step 1 Browse to the directory **<Drive>:\<Path>\Starfish\Bin**, where <Drive> and <Path> denote the drive and the topmost directory where the Bridge software is installed.

Step 2 Open the file **btcall.cfg** in Notepad.

Step 3 Add the following line at the bottom of the file:

debug ./traceinfo.log

Step 4 Save the changes to btcall.cfg and close the file.

Step 5 Restart the Unity Bridge service from the Services Control Panel.

Brooktrout TR114 activity will now be logged to <BridgePath>\Starfish\Bin\Traceinfo.log. Be aware that each time the Unity Bridge service is restarted, the old traceinfo.log will be deleted and a fresh log begun.

If you need to restart the Unity Bridge service and want to save the traceinfo.log from the previous test, use the following procedure.

To Save the traceinfo.log from a Previous Test

Step 1 Stop the Unity Bridge service from the Services Control Panel.

Step 2 Rename **<BridgePath>\Starfish\Bin\Traceinfo.log** to a filename of your choice.

Step 3 Start the Unity Bridge service from the Services Control Panel.

Note On Bridge servers where message traffic is heavy, the traceinfo.log file can grow very large. There is no mechanism for limiting the size of traceinfo.log, and no cycling occurs. When you have finished troubleshooting, you should disable the tracing.

Disabling Debug Traces for the Brooktrout TR114

To Disable Debug Traces for the Brooktrout TR114

Step 1 Browse to the directory **<BridgePath>\Starfish\Bin**.

Step 2 Open the file **btcall.cfg** in Notepad.

Step 3 Remove the **debug ./traceinfo.log** line from the bottom of the file.

Step 4 Save the changes to btcall.cfg and close the file.

Step 5 Restart the Unity Bridge service from the Services Control Panel.

Interpreting Debug Traces for the Brooktrout TR114

Because the Brooktrout TR114 traceinfo.log is run on the same server as the sflog.*.log files, the time stamps will match up. This allows you to use these logs together to get a good picture of what is going on. See the description of the Call Tracing Level field in the “System Settings” section for information about enabling the sflog.*.log files.

Following is an excerpt from a traceinfo.log on a 4-port Bridge server for an outgoing analog message delivery from the Bridge (serial number 80100) to a remote Octel node (serial number 80200). Descriptions of the events are included, as well as the associated events from sflog.log. The excerpt displays the context of actions the board is taking based on requests from the Unity Bridge service (starfish.exe) and vice versa. In the following example traces, the sflog traces begin with the word

"SFLOG" followed by a number. Only the sflog.log events for line 3 (TR114 channel 2) are listed. The traceinfo.log events begin with the date and time followed by the TR114 channel on which the event occurred.

Table 5-1 Brooktrout and SFLOG Example Trace

Trace	Description
11/26 22:59:08.33 0 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:08.34 1 cmd: 0x26 DIS_RING_DET 0x0 **11/26 22:59:08.34 2 cmd: 0x26 DIS_RING_DET 0x0** 11/26 22:59:08.35 3 cmd: 0x26 DIS_RING_DET 0x0 **11/26 22:59:08.37 2 await ring** **11/26 22:59:08.37 2 cmd: 0x1f NUM_RINGS 0x1** **11/26 22:59:08.37 2 cmd: 0x27 ENA_RING_DET 0x0** 11/26 22:59:08.39 1 await ring 11/26 22:59:08.39 1 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:08.39 1 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:08.41 0 await ring 11/26 22:59:08.41 0 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:08.41 0 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:08.41 3 await ring 11/26 22:59:08.41 3 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:08.41 3 cmd: 0x27 ENA_RING_DET 0x0 **11/26 22:59:18.37 2 cmd: 0x26 DIS_RING_DET 0x0** 11/26 22:59:18.39 1 cmd: 0x26 DIS_RING_DET 0x0	All of the analog ports on the Bridge are in an idle state. They repeatedly cycle through their ring detect processes to monitor for incoming calls until they get one, or until an outgoing call is initiated by the Unity Bridge service (starfish.exe). The number immediately following the time stamp is the channel number on the TR114. Note that it is zero based, that is, channels 0–3 correspond to lines 1–4 on the Bridge server. The traces for channel 2 (which is Bridge line 3) are in bold.
SFLOG 1396 1700 2002/11/26-22:59:18.384 00000008 Line 3: Call Out Process Initiated for Node 80200 Window Type 0	The Bridge initiates the call out process for node 80200 normal messages (type 0). There is a message to deliver, and therefore a request is sent to the TR114 to make the call.
11/26 22:59:18.39 2 cmd: 0x24 ENABLE_TONE_DET 0x0 11/26 22:59:18.39 2 dialing ,20 11/26 22:59:18.39 2 cmd: 0x37 DIAL_STRING 0x0	These three events initiate an outgoing analog call on channel 2 (Bridge line 3). The dial string is ",20" where the comma is a one second pause and 20 is the phone number being dialed.
11/26 22:59:18.41 1 await ring 11/26 22:59:18.41 1 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:18.41 1 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:18.41 0 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:18.44 3 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:18.44 0 await ring 11/26 22:59:18.44 0 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:18.44 0 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:18.45 3 await ring 11/26 22:59:18.45 3 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:18.45 3 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:20.15 2 intr: 0xa ISTRDNE 0x0 11/26 22:59:20.15 2 cmd: 0x2b ENA_CALL_PROG 0x23	Call progress detection is initiated on the TR114. The TR114 waits for detection of ringback, busy or reorder tone, or detection of a human voice.

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
1/26 22:59:20.60 2 intr: 0x18 ILOW 0x40 11/26 22:59:20.89 2 intr: 0x19 IHI 0x3a 11/26 22:59:22.14 2 intr: 0x18 ILOW 0xfa 11/26 22:59:22.27 2 intr: 0x19 IHI 0x1a 11/26 22:59:22.77 2 intr: 0x18 ILOW 0x64 11/26 22:59:22.82 2 intr: 0x19 IHI 0xa 11/26 22:59:22.95 2 intr: 0x18 ILOW 0x1a 11/26 22:59:22.95 2 intr: 0x1b CALL_PROG 0x10 111/26 22:59:22.95 2 call progress: HUMAN	Voice detection has occurred. A connect event is sent to the Unity Bridge service.
11/26 22:59:22.95 2 cmd: 0x2a DIS_CALL_PROG 0x0 11/26 22:59:22.95 2 cmd: 0x24 ENABLE_TONE_DET 0x3 11/26 22:59:22.95 2 cmd: 0x24 ENABLE_TONE_DET 0x0 SFLOG 1396 1700 2002/11/26-22:59:22.960 00000100 Line 3: Call Status = Answer SFLOG 1396 1700 2002/11/26-22:59:22.960 00000100 Line 3: Playing BD	The Unity Bridge service acknowledges that the call has been answered and sends the tones “BD” to the Octel. DTMF tones are stored in.sph files in \Bridge\Starfish\Bin and played through the TR114 as audio files.
11/26 22:59:22.97 2 cmd: 0x5e SPEECH_PARAMS 0x0 11/26 22:59:22.99 2 cmd: 0x5c SPEECH_START 0x0	The TR114 receives the audio of “BD” and the associated parameters, and begins to play them to the Octel.
11/26 22:59:22.99 2 cmd-sync: 0x5d SPEECH_ALTER 0x8 11/26 22:59:23.02 2 intr: 0x2c ECHO_ADAPT 0xa 11/26 22:59:23.29 2 intr: 0x38 SPEECH_DONE 0x0	The TR114 completes playing the audio to the Octel. You will see only one pair of SPEECH_START/SPEECH_DONE events for each string of DTMF digits sent. Because the TR114 is simply playing recordings of DTMFs given to it by the Unity Bridge service, you will see the actual DTMF digits sent only in the sflogs.

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
11/26 22:59:23.29 2 cmd: 0x24 ENABLE_TONE_DET 0x3 11/26 22:59:24.46 2 intr: 0xb TONE_DETECT 0x8f 11/26 22:59:24.53 2 intr: 0xb TONE_DETECT 0xf 11/26 22:59:24.60 2 intr: 0xb TONE_DETECT 0x80 11/26 22:59:24.67 2 intr: 0xb TONE_DETECT 0x0 11/26 22:59:24.75 2 intr: 0xb TONE_DETECT 0x80 11/26 22:59:24.82 2 intr: 0xb TONE_DETECT 0x0 **Description of Tones Received** The first tone received is "C" (because f=C). This tone began at 22:59:24.46 (0x8f) and ended at 22:59:24.53 (0xf); thus it was 70 milliseconds in duration. The second tone received is "D" (because 0=D). This tone began at 22:59:24.60 (0x80) and ended at 22:59:24.67 (0x0); thus it was 70 milliseconds in duration. The interdigit time between the "C" and the first "D" was 70 milliseconds (22:59:24.60 – 22:59:24.53 = .07 seconds, or 70 milliseconds). The third tone received is "D" (because 0=D). This tone began at 22:59:24.75 (0x80) and ended at 22:59:24.82 (0x0); thus it was 70 milliseconds in duration. The interdigit time between the first "D" and the second "D" was 80 milliseconds (22:59:24.75 – 22:59:24.67 = .08 seconds, or 80 milliseconds).	The TR114 detects incoming DTMF digits from the Octel. There are two TONE_DETECT events for each tone detected, one when the beginning of the tone is detected and one when the end is detected. The event for detection of the beginning of a tone will look like "intr: 0xb TONE_DETECT 0x8c," where the "8" indicates the beginning of the tone and the "c" indicates what tone was detected. The end of the tone will look just the same, but will not include the "8" (for example, "intr: 0xb TONE_DETECT 0xc"). Note the "c" here does not represent the actual DTMF "C" tone. Use the following table to translate what the digit signifies: 1–9 = 1–9 a = 0 b = * c = # d = A e = B f = C 0 = D
SFLOG 1396 1700 2002/11/26-22:59:25.835 00000100 Line 3: Received CDD	The "CDD" detected by the TR114 is passed to the Unity Bridge service and reported as received in sflog.log.
SFLOG 1396 1700 2002/11/26-22:59:25.835 00000100 Line 3: Playing 12086D5082AC6AA897	The Unity Bridge services responds to the CDD packet by sending a request to the TR114 to play audio of the DTMF digit string "12086D5082AC6AA897."
11/26 22:59:25.82 2 cmd: 0x24 ENABLE_TONE_DET 0x0 11/26 22:59:25.82 2 cmd: 0x5e SPEECH_PARAMS 0x0 11/26 22:59:25.83 2 cmd: 0x5c SPEECH_START 0x0	The TR114 receives the audio of "12086D5082AC6AA897" and the associated parameters, and begins to play them to the Octel.
11/26 22:59:25.85 2 intr: 0x2c ECHO_ADAPT 0xa 11/26 22:59:25.94 2 cmd-sync: 0x5d SPEECH_ALTER 0x8 11/26 22:59:28.38 2 intr: 0x38 SPEECH_DONE 0x0	The TR114 completes playing the audio to the Octel.

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
11/26 22:59:28.38 2 cmd: 0x24 ENABLE_TONE_DET 0x3 11/26 22:59:28.42 1 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:28.43 1 await ring 11/26 22:59:28.43 1 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:28.43 1 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:28.45 0 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:28.46 0 await ring 11/26 22:59:28.46 0 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:28.46 0 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:28.46 3 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:28.47 3 await ring 11/26 22:59:28.47 3 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:28.47 3 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:29.56 2 intr: 0xb TONE_DETECT 0x81 11/26 22:59:29.63 2 intr: 0xb TONE_DETECT 0x1 11/26 22:59:29.70 2 intr: 0xb TONE_DETECT 0x83 11/26 22:59:29.77 2 intr: 0xb TONE_DETECT 0x3 11/26 22:59:29.85 2 intr: 0xb TONE_DETECT 0x87 11/26 22:59:29.92 2 intr: 0xb TONE_DETECT 0x7 11/26 22:59:29.99 2 intr: 0xb TONE_DETECT 0x80 11/26 22:59:30.06 2 intr: 0xb TONE_DETECT 0x0 11/26 22:59:30.13 2 intr: 0xb TONE_DETECT 0x87 11/26 22:59:30.19 2 intr: 0xb TONE_DETECT 0x7 11/26 22:59:30.26 2 intr: 0xb TONE_DETECT 0x80 11/26 22:59:30.33 2 intr: 0xb TONE_DETECT 0x0 11/26 22:59:30.40 2 intr: 0xb TONE_DETECT 0x85 11/26 22:59:30.47 2 intr: 0xb TONE_DETECT 0x5 11/26 22:59:30.54 2 intr: 0xb TONE_DETECT 0x8d 11/26 22:59:30.61 2 intr: 0xb TONE_DETECT 0xd 11/26 22:59:30.68 2 intr: 0xb TONE_DETECT 0x88 11/26 22:59:30.75 2 intr: 0xb TONE_DETECT 0x8 11/26 22:59:30.82 2 intr: 0xb TONE_DETECT 0x8c 11/26 22:59:30.89 2 intr: 0xb TONE_DETECT 0xc 11/26 22:59:30.97 2 intr: 0xb TONE_DETECT 0x87 11/26 22:59:31.04 2 intr: 0xb TONE_DETECT 0x7 11/26 22:59:31.09 2 intr: 0xb TONE_DETECT 0x8a 11/26 22:59:31.16 2 intr: 0xb TONE_DETECT 0xa 11/26 22:59:31.24 2 intr: 0xb TONE_DETECT 0x80 11/26 22:59:31.31 2 intr: 0xb TONE_DETECT 0x0 11/26 22:59:31.38 2 intr: 0xb TONE_DETECT 0x88 11/26 22:59:31.45 2 intr: 0xb TONE_DETECT 0x8	The TR114 detects incoming DTMF digits from the Octel. By using the conversion table provided earlier in this example, we can map the TONE_DETECT events to DTMF digits, as follows: 1 3 7 0 7 0 5 d 8 c 7 a 0 8 1 3 7 D 7 D 5 A 8 # 7 0 D 8 (The first line contains the TONE_DETECT events, and the second line contains the DTMF digits.)
SFLOG 1396 1700 2002/11/26-22:59:32.464 00000100 Line 3: Received 137D7D5A8#70D8 SFLOG 1396 1700 2002/11/26-22:59:32.464 00000100 Line 3: Protocol Level = 3	The “137D7D5A8#70D8” detected by the TR114 is passed to the Unity Bridge service and reported as received in sflog.log. From the received packet the Unity Bridge service can determine the analog Octel networking protocol level used by the Octel server.

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
SFLOG 1396 1700 2002/11/26-22:59:32.464 00000100 Line 3: Playing 2431#73258#51#4B	The Unity Bridge services responds to the received packet by sending a request to the TR114 to play audio of the DTMF digit string "2431#73258#51#4B."
11/26 22:59:32.45 2 cmd: 0x24 ENABLE_TONE_DET 0x0 11/26 22:59:32.45 2 cmd: 0x5e SPEECH_PARAMS 0x0 11/26 22:59:32.46 2 cmd: 0x5c SPEECH_START 0x0	The TR114 receives the audio of "2431#73258#51#4B" and the associated parameters, and begins to play them to the Octel.
11/26 22:59:32.49 2 intr: 0x2c ECHO_ADAPT 0xa 11/26 22:59:32.52 2 cmd-sync: 0x5d SPEECH_ALTER 0x8 11/26 22:59:34.74 2 intr: 0x38 SPEECH_DONE 0x0	The TR114 completes playing the audio to the Octel.
11/26 22:59:34.74 2 cmd: 0x24 ENABLE_TONE_DET 0x3 11/26 22:59:35.92 2 intr: 0xb TONE_DETECT 0x8a 11/26 22:59:35.99 2 intr: 0xb TONE_DETECT 0xa 11/26 22:59:36.06 2 intr: 0xb TONE_DETECT 0x86 11/26 22:59:36.13 2 intr: 0xb TONE_DETECT 0x6 11/26 22:59:36.20 2 intr: 0xb TONE_DETECT 0x89 11/26 22:59:36.27 2 intr: 0xb TONE_DETECT 0x9 11/26 22:59:36.35 2 intr: 0xb TONE_DETECT 0x87 11/26 22:59:36.42 2 intr: 0xb TONE_DETECT 0x7 11/26 22:59:36.49 2 intr: 0xb TONE_DETECT 0x8c 11/26 22:59:36.56 2 intr: 0xb TONE_DETECT 0xc 11/26 22:59:36.63 2 intr: 0xb TONE_DETECT 0x87 11/26 22:59:36.69 2 intr: 0xb TONE_DETECT 0x7 11/26 22:59:36.76 2 intr: 0xb TONE_DETECT 0x86 11/26 22:59:36.83 2 intr: 0xb TONE_DETECT 0x6 11/26 22:59:36.90 2 intr: 0xb TONE_DETECT 0x8a 11/26 22:59:36.97 2 intr: 0xb TONE_DETECT 0xa 11/26 22:59:37.04 2 intr: 0xb TONE_DETECT 0x85 11/26 22:59:37.11 2 intr: 0xb TONE_DETECT 0x5 11/26 22:59:37.18 2 intr: 0xb TONE_DETECT 0x88 11/26 22:59:37.25 2 intr: 0xb TONE_DETECT 0x8 11/26 22:59:37.32 2 intr: 0xb TONE_DETECT 0x80 11/26 22:59:37.39 2 intr: 0xb TONE_DETECT 0x0 11/26 22:59:37.47 2 intr: 0xb TONE_DETECT 0x85 11/26 22:59:37.54 2 intr: 0xb TONE_DETECT 0x5 11/26 22:59:37.61 2 intr: 0xb TONE_DETECT 0x88 11/26 22:59:37.66 2 intr: 0xb TONE_DETECT 0x8 11/26 22:59:37.74 2 intr: 0xb TONE_DETECT 0x8d 11/26 22:59:37.81 2 intr: 0xb TONE_DETECT 0xd 11/26 22:59:37.88 2 intr: 0xb TONE_DETECT 0x82 11/26 22:59:37.95 2 intr: 0xb TONE_DETECT 0x2 11/26 22:59:38.02 2 intr: 0xb TONE_DETECT 0x80 11/26 22:59:38.09 2 intr: 0xb TONE_DETECT 0x0	The TR114 detects incoming DTMF digits from the Octel. By using the conversion table provided earlier in this example, we can see that the TONE_DETECT events correspond to the following DTMF digits: 0 6 9 7 # 7 6 0 5 8 D 5 8 A 2 D

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
1/26 22:59:38.43 1 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:38.44 1 await ring 11/26 22:59:38.44 1 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:38.44 1 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:38.46 0 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:38.47 0 await ring 11/26 22:59:38.47 0 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:38.47 0 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:38.47 3 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:38.48 3 await ring 11/26 22:59:38.48 3 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:38.48 3 cmd: 0x27 ENA_RING_DET 0x0 SFLOG 1396 1700 2002/11/26-22:59:39.104 00000100 Line 3: Received 0697#76058D58A2D SFLOG 1396 1700 2002/11/26-22:59:39.104 00000008 Line 3: Call established from Serial # 80100 to Serial # 80200	The “0697#76058D58A2D” detected by the TR114 is passed to the Unity Bridge service and reported as received in sflog.log. From the received packet the Unity Bridge service is able to determine that Octel node #80200 has accepted our call and will allow us to proceed.
SFLOG 1396 1700 2002/11/26-22:59:39.114 00000100 Line 3: Playing 131A3C13#CAA7A*7AB72*C9D5A647*69D#1A	The Unity Bridge service responds to the received packet by sending a request to the TR114 to play audio of the DTMF digit string “131A3C13#CAA7A*7AB72*C9D5A647*69D#1A.”
11/26 22:59:39.10 2 cmd: 0x24 ENABLE_TONE_DET 0x0 11/26 22:59:39.10 2 cmd: 0x5e SPEECH_PARAMS 0x0 11/26 22:59:39.12 2 cmd: 0x5c SPEECH_START 0x0	The TR114 receives the audio of “131A3C13#CAA7A*7AB72*C9D5A647*69D#1A” and the associated parameters, and begins to play them to the Octel.
11/26 22:59:39.15 2 intr: 0x2c ECHO_ADAPT 0xa 11/26 22:59:41.09 2 cmd-sync: 0x5d SPEECH_ALTER 0x8 11/26 22:59:44.19 2 intr: 0x38 SPEECH_DONE 0x0	The TR114 finishes playing the audio to the Octel.
11/26 22:59:44.19 2 cmd: 0x24 ENABLE_TONE_DET 0x3 11/26 22:59:45.36 2 intr: 0xb TONE_DETECT 0x8a 11/26 22:59:45.43 2 intr: 0xb TONE_DETECT 0xa 11/26 22:59:45.51 2 intr: 0xb TONE_DETECT 0x82 11/26 22:59:45.58 2 intr: 0xb TONE_DETECT 0x2 11/26 22:59:45.65 2 intr: 0xb TONE_DETECT 0x84 11/26 22:59:45.72 2 intr: 0xb TONE_DETECT 0x4 11/26 22:59:45.79 2 intr: 0xb TONE_DETECT 0x83 11/26 22:59:45.86 2 intr: 0xb TONE_DETECT 0x3 11/26 22:59:45.92 2 intr: 0xb TONE_DETECT 0x80 11/26 22:59:45.99 2 intr: 0xb TONE_DETECT 0x0 11/26 22:59:46.06 2 intr: 0xb TONE_DETECT 0x81 11/26 22:59:46.13 2 intr: 0xb TONE_DETECT 0x1	The TR114 detects incoming DTMF digits from the Octel. By using the conversion table provided earlier in this example, we can see that TONE_DETECT events correspond to the following DTMF digits: 0 2 4 3 D 1
SFLOG 1396 1700 2002/11/26-22:59:47.145 00000100 Line 3: Received 0243D1	The “0243D1” detected by the TR114 is passed to the Unity Bridge service and reported as received in sflog.log.

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
SFLOG 1396 1700 2002/11/26-22:59:47.145 00000100 Line 3: Playing 67D59228#882313B*0AA*#C#1*DB4579B8D48D7D51A980	The Unity Bridge service responds to the received packet by sending a request to the TR114 to play audio of the DTMF digit string "67D59228#882313B*0AA*#C#1*DB4579B8D48D7D51A980."
11/26 22:59:47.13 2 cmd: 0x24 ENABLE_TONE_DET 0x0 11/26 22:59:47.13 2 cmd: 0x5e SPEECH_PARAMS 0x0 11/26 22:59:47.14 2 cmd: 0x5c SPEECH_START 0x0	The TR114 receives the audio of "67D59228#882313B*0AA*#C#1*DB4579B8D48D7D51A980" and the associated parameters, and begins to play them to the Octel.
11/26 22:59:47.17 2 intr: 0x2c ECHO_ADAPT 0xa 11/26 22:59:48.48 1 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:48.48 0 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:48.49 1 await ring 11/26 22:59:48.49 1 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:48.49 1 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:48.49 0 await ring 11/26 22:59:48.49 0 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:48.49 0 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:48.49 3 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:48.50 3 await ring 11/26 22:59:48.50 3 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:48.50 3 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:50.51 2 cmd-sync: 0x5d SPEECH_ALTER 0x8 11/26 22:59:53.61 2 intr: 0x38 SPEECH_DONE 0x0	The TR114 completes playing the audio to the Octel.
11/26 22:59:53.61 2 cmd: 0x24 ENABLE_TONE_DET 0x3 11/26 22:59:54.82 2 intr: 0xb TONE_DETECT 0x82 11/26 22:59:54.89 2 intr: 0xb TONE_DETECT 0x2 11/26 22:59:54.95 2 intr: 0xb TONE_DETECT 0x83 11/26 22:59:55.02 2 intr: 0xb TONE_DETECT 0x3 11/26 22:59:55.09 2 intr: 0xb TONE_DETECT 0x8e 11/26 22:59:55.16 2 intr: 0xb TONE_DETECT 0xe 11/26 22:59:55.23 2 intr: 0xb TONE_DETECT 0x8d 11/26 22:59:55.30 2 intr: 0xb TONE_DETECT 0xd 11/26 22:59:55.37 2 intr: 0xb TONE_DETECT 0x8f 11/26 22:59:55.44 2 intr: 0xb TONE_DETECT 0xf 11/26 22:59:55.51 2 intr: 0xb TONE_DETECT 0x8e 11/26 22:59:55.58 2 intr: 0xb TONE_DETECT 0xe	The TR114 detects incoming DTMF digits from the Octel. By using the conversion table provided earlier in this example, we can see that the TONE_DETECT events correspond to the following DTMF digits: 2 3 B A C B

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
SFLOG 1396 1700 2002/11/26-22:59:56.589 00000100 Line 3: Begin Mailbox Update SFLOG 1396 1700 2002/11/26-22:59:56.589 00000100 Line 3: End Mailbox Update SFLOG 1396 1700 2002/11/26-22:59:56.589 00000008 Line 3: Sending Message from mailbox 57100@JDC1 to mailbox 47100@jdc6a.ecsbu-lab-sea.cisco.com SFLOG 1396 1700 2002/11/26-22:59:56.589 00000008 Line 3: Playing Voice SFLOG 1396 1700 2002/11/26-22:59:56.589 00000100 Line 3: Playing c:\Bridge\Starfish\In\80200\80100\20021127065817606-443f73dd-da28-40ad-ae0a-26f2c388ff4f	The Unity Bridge service responds to the received packet by sending a request to the TR114 to play the actual voice message.

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
11/26 22:59:56.58 2 cmd: 0x5e SPEECH_PARAMS 0x0 11/26 22:59:56.59 2 play 1024 11/26 22:59:56.59 2 play 2048 11/26 22:59:56.59 2 play 3072 11/26 22:59:56.59 2 play 4096 11/26 22:59:56.59 2 play 5120 11/26 22:59:56.59 2 play 6144 11/26 22:59:56.59 2 play 7168 11/26 22:59:56.59 2 play 8192 11/26 22:59:56.59 2 cmd: 0x5c SPEECH_START 0x0 11/26 22:59:56.59 2 play 9216 11/26 22:59:56.60 2 play 10240 11/26 22:59:56.60 2 play 11264 11/26 22:59:56.60 2 play 12288 11/26 22:59:56.61 2 play 13312 11/26 22:59:56.61 2 play 14336 11/26 22:59:56.61 2 play 15360 11/26 22:59:56.62 2 play 16384 11/26 22:59:56.62 2 intr: 0x2c ECHO_ADAPT 0xa 11/26 22:59:56.63 2 play 17408 11/26 22:59:56.65 2 play 18432 11/26 22:59:56.68 2 play 19456 11/26 22:59:56.70 2 play 20480 11/26 22:59:56.73 2 play 21504 11/26 22:59:56.75 2 play 22528 11/26 22:59:56.78 2 play 23552 11/26 22:59:56.80 2 play 24576 11/26 22:59:56.83 2 play 25600 11/26 22:59:56.85 2 play 26624 11/26 22:59:56.94 2 play 27648 11/26 22:59:57.07 2 play 28672 11/26 22:59:57.20 2 play 29696 11/26 22:59:57.32 2 play 30720 11/26 22:59:57.45 2 play 31744 11/26 22:59:57.58 2 play 32768 11/26 22:59:57.71 2 play 33792 11/26 22:59:57.84 2 play 34816 11/26 22:59:57.96 2 play 35840 11/26 22:59:58.09 2 play 36864 11/26 22:59:58.22 2 play 37888 11/26 22:59:58.35 2 play 38912 11/26 22:59:58.48 2 play 39614 11/26 22:59:58.48 2 cmd-sync: 0x5d SPEECH_ALTER 0x8 11/26 22:59:58.49 1 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:58.49 0 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:58.50 1 await ring 11/26 22:59:58.50 1 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:58.50 1 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:58.50 0 await ring 11/26 22:59:58.50 0 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:58.50 0 cmd: 0x27 ENA_RING_DET 0x0 11/26 22:59:58.50 3 cmd: 0x26 DIS_RING_DET 0x0 11/26 22:59:58.51 3 await ring 11/26 22:59:58.51 3 cmd: 0x1f NUM_RINGS 0x1 11/26 22:59:58.51 3 cmd: 0x27 ENA_RING_DET 0x0 11/26 23:00:01.57 2 intr: 0x38 SPEECH_DONE 0x0	The TR114 completes playing the audio to the Octel.

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
SFLOG 1396 1700 2002/11/26-23:00:01.586 00000008 Line 3: Playing completed	The Unity Bridge service acknowledges that the playing of the voice message has finished.
SFLOG 1396 1700 2002/11/26-23:00:01.586 00000100 Line 3: Playing #	The Unity Bridge service sends a request to the TR114 to play the audio of the DTMF digit "#." Playing of this digit indicates to the Octel server the end of the voice message.
11/26 23:00:01.58 2 cmd: 0x24 ENABLE_TONE_DET 0x0 11/26 23:00:01.58 2 cmd: 0x5e SPEECH_PARAMS 0x0 11/26 23:00:01.59 2 cmd: 0x5c SPEECH_START 0x0	The TR114 receives the audio of "#" and the associated parameters, and begins to play it to the Octel.
11/26 23:00:01.59 2 cmd-sync: 0x5d SPEECH_ALTER 0x8 11/26 23:00:01.62 2 intr: 0x2c ECHO_ADAPT 0xa 11/26 23:00:01.75 2 intr: 0x38 SPEECH_DONE 0x0	The TR114 finishes playing the audio to the Octel.
11/26 23:00:01.75 2 cmd: 0x24 ENABLE_TONE_DET 0x3 11/26 23:00:02.93 2 intr: 0xb TONE_DETECT 0x88 11/26 23:00:03.00 2 intr: 0xb TONE_DETECT 0x8	The TR114 detects an incoming DTMF digit from the Octel. By using the conversion table provided earlier in this example, we can see that the TONE_DETECT event corresponds to DTMF digit "8."
SFLOG 1396 1700 2002/11/26-23:00:04.009 00000100 Line 3: Received 8	The "8" detected by the TR114 is passed to the Unity Bridge service and reported as received in sflog.log.
SFLOG 1396 1700 2002/11/26-23:00:04.009 00000100 Line 3: Playing 9	The Unity Bridge service responds to the received "8" by sending a request to the TR114 to play audio of the DTMF digit "9."
11/26 23:00:04.00 2 cmd: 0x24 ENABLE_TONE_DET 0x0 11/26 23:00:04.00 2 cmd: 0x5e SPEECH_PARAMS 0x0 11/26 23:00:04.01 2 cmd: 0x5c SPEECH_START 0x0	The TR114 receives the audio of "9" and the associated parameters, and begins to play it to the Octel.
11/26 23:00:04.01 2 cmd-sync: 0x5d SPEECH_ALTER 0x8 11/26 23:00:04.04 2 intr: 0x2c ECHO_ADAPT 0xa 11/26 23:00:04.17 2 intr: 0x38 SPEECH_DONE 0x0	The TR114 completes playing the audio to the Octel.
11/26 23:00:04.17 2 cmd: 0x24 ENABLE_TONE_DET 0x3 11/26 23:00:05.34 2 intr: 0xb TONE_DETECT 0x82 11/26 23:00:05.41 2 intr: 0xb TONE_DETECT 0x2 11/26 23:00:05.48 2 intr: 0xb TONE_DETECT 0x83 11/26 23:00:05.55 2 intr: 0xb TONE_DETECT 0x3 11/26 23:00:05.63 2 intr: 0xb TONE_DETECT 0x87 11/26 23:00:05.70 2 intr: 0xb TONE_DETECT 0x7 11/26 23:00:05.77 2 intr: 0xb TONE_DETECT 0x86 11/26 23:00:05.84 2 intr: 0xb TONE_DETECT 0x6 11/26 23:00:05.91 2 intr: 0xb TONE_DETECT 0x83 11/26 23:00:05.98 2 intr: 0xb TONE_DETECT 0x3 11/26 23:00:06.04 2 intr: 0xb TONE_DETECT 0x8d 11/26 23:00:06.11 2 intr: 0xb TONE_DETECT 0xd	The TR114 detects incoming DTMF digits from the Octel. By using the conversion table provided earlier in this example, we can see that the TONE_DETECT events correspond to the following DTMF digits: 2 3 7 6 3 A

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
SFLOG 1396 1700 2002/11/26-23:00:07.124 00000100 Line 3: Received 23763A SFLOG 1396 1700 2002/11/26-23:00:07.124 00000008 Line 3: Message Delivered SFLOG 1396 1700 2002/11/26-23:00:07.124 00000008 Line 3: Completed delivering Messages	The "23763A" detected by the TR114 is passed to the Unity Bridge service and reported as received in sflog.log. From the received packet, the Unity Bridge service is able to determine that Octel node #80200 has successfully received and processed the message. The Bridge has no more messages in the queue to deliver to this node.
SFLOG 1396 1700 2002/11/26-23:00:07.124 00000100 Line 3: Playing 045AC0BA9*84#D002A991C367C8ABDB0C2A4	The Unity Bridge service sends a request to the TR114 to play audio of the DTMF digit string "045AC0BA9*84#D002A991C367C8ABDB0C2A4."
11/26 23:00:07.11 2 cmd: 0x24 ENABLE_TONE_DET 0x0 11/26 23:00:07.11 2 cmd: 0x5e SPEECH_PARAMS 0x0 11/26 23:00:07.13 2 cmd: 0x5c SPEECH_START 0x0	The TR114 receives the audio of "045AC0BA9*84#D002A991C367C8ABDB0C2A4" and the associated parameters, and begins to play them to the Octel.
11/26 23:00:07.16 2 intr: 0x2c ECHO_ADAPT 0xa 11/26 23:00:08.51 1 cmd: 0x26 DIS_RING_DET 0x0 11/26 23:00:08.51 0 cmd: 0x26 DIS_RING_DET 0x0 11/26 23:00:08.52 1 await ring 11/26 23:00:08.52 1 cmd: 0x1f NUM_RINGS 0x1 11/26 23:00:08.52 1 cmd: 0x27 ENA_RING_DET 0x0 11/26 23:00:08.52 0 await ring 11/26 23:00:08.52 0 cmd: 0x1f NUM_RINGS 0x1 11/26 23:00:08.52 0 cmd: 0x27 ENA_RING_DET 0x0 11/26 23:00:08.52 3 cmd: 0x26 DIS_RING_DET 0x0 11/26 23:00:08.53 3 await ring 11/26 23:00:08.53 3 cmd: 0x1f NUM_RINGS 0x1 11/26 23:00:08.53 3 cmd: 0x27 ENA_RING_DET 0x0 11/26 23:00:09.10 2 cmd-sync: 0x5d SPEECH_ALTER 0x8 11/26 23:00:12.20 2 intr: 0x38 SPEECH_DONE 0x0	The TR114 finishes playing the audio to the Octel.
11/26 23:00:12.20 2 cmd: 0x24 ENABLE_TONE_DET 0x3 11/26 23:00:13.39 2 intr: 0xb TONE_DETECT 0x81 11/26 23:00:13.46 2 intr: 0xb TONE_DETECT 0x1 11/26 23:00:13.54 2 intr: 0xb TONE_DETECT 0x85 11/26 23:00:13.61 2 intr: 0xb TONE_DETECT 0x5 11/26 23:00:13.68 2 intr: 0xb TONE_DETECT 0x8e 11/26 23:00:13.75 2 intr: 0xb TONE_DETECT 0xe 11/26 23:00:13.82 2 intr: 0xb TONE_DETECT 0x8a 11/26 23:00:13.89 2 intr: 0xb TONE_DETECT 0xa 11/26 23:00:13.95 2 intr: 0xb TONE_DETECT 0x89 11/26 23:00:14.02 2 intr: 0xb TONE_DETECT 0x9 11/26 23:00:14.09 2 intr: 0xb TONE_DETECT 0x8e 11/26 23:00:14.16 2 intr: 0xb TONE_DETECT 0xe	The TR114 detects incoming DTMF digits from the Octel. By using the conversion table provided earlier in this example, we can see that the TONE_DETECT events correspond to the following DTMF digits: 1 5 B 0 9 B

Table 5-1 Brooktrout and SFLOG Example Trace (continued)

Trace	Description
SFLOG 1396 1700 2002/11/26-23:00:15.176 00000100 Line 3: Received 15B09B	The "15B09B" detected by the TR114 is passed to the Unity Bridge service and reported as received in sflog.log.
SFLOG 1396 1700 2002/11/26-23:00:16.918 00000008 Line 3: Call Out Completed.	The Unity Bridge service is done. It sends a request to the TR114 to hang up the call.

The TR114 begins the process of reinitializing the channel to be ready for the next incoming or outgoing call.

Using the Call Traces to Troubleshoot Why Messages Are Not Delivered from the Bridge to the Octels

We recommend that you use the Bridge Analog Network And Node Analyzer (BANANA) to troubleshoot analog problems between the Bridge and the Octels rather than using the call trace information in this section. We recommend use of BANANA, as it saves you from having to dig through the call traces to determine why messages were not delivered from the Bridge to the Octels.

However, in cases where it is necessary to evaluate the call traces rather than using BANANA, you will find in this section all of the details you need for using call traces to track down message delivery problems between the Bridge and the Octels.

- Are Calls Attempted?, page 5-14
- Are Dialouts Successful?, page 5-16
- Are Handshakes Successful?, page 5-17
- Are Any Messages Transmitted Successfully?, page 5-18

Are Calls Attempted?

To Determine Whether Calls Are Attempted by Viewing the Call Traces

Step 1 On the Bridge server, browse to the **Bridge\Starfish\Log** directory.

Step 2 Open the log file for the time period in question.

Step 3 Look for messages with the syntax **Line <Line number>: Call Out Process Initiated for Node <Node#> Window Type <WindowType>**, where:

- Line <Line number> is the line on which the call was attempted
- <Node#> is the destination Octel node serial number
- <WindowType> is 0, 1, or 2
  - 0=normal priority voice messages
  - 1=urgent priority voice messages
  - 2=administrative (text/voice name retrieval) calls

In Bridge 3.0(1) and later, these messages appear only when the Bridge is about to initiate a call to an Octel server.

Step 4 Look for the next line that has the same "Line <Line number>" notation you found in Step 3. The appearance of the "Line <Line number>" notation again, following the first appearance of the message, indicates whether the call is answered successfully.

Step 5 If lines similar to those described in Step 3 and Step 4 do appear in the log for the expected destination serial number and message type, an analog call is being attempted to the specified node. In this case, go to the "To Determine Whether Dialouts Are Successful by Viewing the Call Traces" procedure on page 5-16.

Step 6 If no lines similar to those described in Step 3 and Step 4 appear in the log, or if the only lines present in the log indicate "No Callout Activity was started," calls are not being attempted. In this case, continue with the following "Troubleshooting Why Calls Are Not Attempted" section.

Troubleshooting Why Calls Are Not Attempted

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

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

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

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

Are Dialouts Successful?

To Determine Whether Dialouts Are Successful by Viewing the Call Traces

Step 1 Look at the same **Call Out Process Initiated for Node <Node#> Window Type <WindowType>** lines in the sflog file that you opened in the "To Determine Whether Calls Are Attempted by Viewing the Call Traces" procedure on page 5-14. If the call is attempted, this line will be followed by another line indicating the status of the call. There are four possibilities:

- Call Status=Answer—The dialout was successful, and the call was successfully answered by the destination Octel node.
- Call Status=Ring No Answer—The dialout was successful, but the destination Octel node did not answer.
- Call Status=Busy—The dialout was successful, but the destination Octel node was busy.
- Call Status=Line Error—The dialout was not successful. The Bridge encountered an error with the analog port or line prior to successfully dialing the phone number.

Step 2 If the Call Status is "Answer," go to the "To Determine Whether Handshakes Are Successful by Viewing the Call Traces" procedure on page 5-17.

If the Call Status is not "Answer," continue with the following "Troubleshooting Why Dialouts Are Not Successful" section.

Troubleshooting Why Dialouts Are Not Successful

- Is the correct phone number defined?—In the Bridge Administrator, go to the Octel Node configuration page for each node. Confirm that the Phone Number, Extension, and Dial Sequence fields contain correct information.
- Are long distance calls blocked?—If the call to the Octel node is long distance, confirm that long distance calls are not blocked by the phone system on the lines the Bridge is using.
- Does Octel answer when you dial the Octel node manually?—Plug an analog phone into the lines going to the Bridge, and dial the Octel node manually.

Are Handshakes Successful?

To Determine Whether Handshakes Are Successful by Viewing the Call Traces

Step 1 In the sflog file that you opened in the "To Determine Whether Calls Are Attempted by Viewing the Call Traces" procedure on page 5-14, look for the status line **Call Status=Answer**. This indicates that the dialout was successful, and that the call was successfully answered by the destination Octel node.

Step 2 Look for the next event for this line, which should be **Playing BD**. "Playing BD" indicates that the Bridge has detected the prompt on the Octel system and is now playing the analog DTMF digits B and D to indicate to the Octel that this is an Octel analog networking call.

Step 3 Following the Playing BD line, look for a line that contains **Received CDD**. By transmitting the CDD DTMF string, the Octel system indicates that it recognizes this call as an Octel analog networking call and is ready to receive the next DTMF packet.

If instead you see a line that contains **Received CC**, this indicates that the Octel node is using the VOICENET protocol, which is not supported. The Octel servers must be running Octel analog networking.

Step 4 Look for the line **Call Established From Serial # <Unity/BridgeSerial#> to Serial # <OctelSerial#>**, which should appear after two more packets are exchanged in each direction. The presence of this line indicates that the handshake was successful.

Note It is not uncommon to occasionally see the Playing BD line two or three times before the Octel system responds with CDD.

Step 5 If the handshake was successful, go to the "To Determine Whether Any Messages Are Transmitted Successfully by Viewing the Call Traces" procedure on page 5-18.

If the handshake was not successful, continue with the following "Troubleshooting Why Handshakes Are Not Successful" section.

Troubleshooting Why Handshakes Are Not Successful

- Is the destination Octel node serial number correct?—In the Bridge Administrator, go to the applicable Octel Node configuration page. Confirm that the number in the Serial Number field matches the serial number for the destination Octel node.
- Is the serial number for the Unity node correct?—In the Bridge Administrator, go to the Unity Node configuration page. Confirm that the number in the Serial Number field matches the serial number entered in the Octel system. The serial number must be entered on each Octel node.
- Is the correct phone number defined?—In the Bridge Administrator, go to the Octel Node configuration page for each node. Confirm that the Phone Number, Extension, and Dial Sequence fields contain correct information. If the Bridge is not receiving a response to the handshake, a possible cause is that whoever or whatever answered is not an Octel server.

Are Any Messages Transmitted Successfully?

To Determine Whether Any Messages Are Transmitted Successfully by Viewing the Call Traces

Step 1 In the sflog file that you opened in the "To Determine Whether Calls Are Attempted by Viewing the Call Traces" procedure on page 5-14, look for **Message Delivered**. This line indicates that a message was successfully delivered to the Octel system.

There can be multiple messages delivered on the same call, so each Message Delivered line indicates the successful delivery of the message identified on the Sending Message line that precedes the Message Delivered line.

Following is an excerpt from an sflog of a successfully delivered message:

```
...
Line 11: Sending Message from mailbox 60032@NYUnityServer5 to mailbox
70044@BridgeServer1.paris.cisco.com
Line 11: Playing Voice
Line 11: Playing D:\Bridge\Starfish\In\80007\86364\935105e7-c584-4167-a0ce-d5b42def44fe
Line 11: Playing completed
Line 11: Playing #
Line 11: Received 8
Line 11: Playing 9
Line 11: Received 13D*C8
Line 11: Message Delivered
...
```

The excerpt shows that the message was successfully delivered to the Octel system. If the call abnormally terminates subsequent to these events, it will not affect the delivery of this particular message, and the delivery for this message will not be retried.

Step 2 If messages are transmitted successfully to the Octel node, but are not delivered to the Octel subscriber, troubleshoot the problem on the Octel node.

If messages are not transmitted successfully, continue with the following "Troubleshooting Why Messages Are Not Transmitted Successfully" section.

Troubleshooting Why Messages Are Not Transmitted Successfully

- Does the target mailbox ID of the message correspond to a valid user mailbox on the Octel system?—In the sflog file, confirm that the target mailbox ID on the Sending Message line corresponds to a valid mailbox number on the Octel node.
- Were there line problems?—In the sflog file, search for the phrase "Encountered communication problems with this node." This phrase can indicate poor line quality or DTMF protocol miscommunications. Confirm the quality of the line. Use an analog digit grabber to monitor the DTMF digit durations and inter-digit delays—they should be between 60ms and 120ms.
- Are the messages in the correct format?—In the sflog file, confirm that there is no line indicating the message was in an unsupported format. The Bridge can play messages sent from Cisco Unity formatted with either the G.711 or G.729a codec.

Using the Call Traces to Troubleshoot Why Messages Are Not Delivered from the Octel Node to the Bridge Server

We recommend that you use the Bridge Analog Network And Node Analyzer (BANANA) to troubleshoot analog problems between the Octels and the Bridge rather than using the call trace information in this section. We recommend use of BANANA, as it saves you from having to dig through the call traces to determine why messages were not delivered from the Bridge to the Octels.

However, in cases where it is necessary to evaluate the call traces rather than using BANANA, you will find in this section the information that you need for using call traces to track down message delivery problems between the Octels and the Bridge.

- The Windows Event Viewer on the Bridge server should be the first place to look when troubleshooting voice message flow from an Octel node to a Cisco Unity node. The Bridge services record errors and warnings to the Windows Event Viewer application log, and you can troubleshoot any errors or warnings you find in the Event logs.
- The call log traces can be used to obtain information about messages coming from Octel servers through the Bridge voice-fax card(s). The log records actions that the Bridge service attempts, notes whether those actions are completed successfully, and records the reasons for failed actions. Within the log directory are files named SFLOG.mmddtttt.LOG. Each file contains log entries for one hour of the day; the filename indicates which hour.
- Go to the Bridge\Starfish\Log directory and open the SFLOG.log that corresponds to the time the message was sent. Look for the following lines in the log file. The presence of these lines shows a successful transmission from the Octel node to the Bridge server.

  ```
  SFLOG 1888  664 2002/09/24-17:02:05.968 00000100
  Line 7: Received 252B605C794162D39B1C328D83CA153A79C4
  SFLOG 1888  664 2002/09/24-17:02:05.968 00000008
  Line 7: New Message from mailbox 10006 to mailbox 30022
  SFLOG 1888  664 2002/09/24-17:02:05.968 00000100
  Line 7: Playing 021#31
  SFLOG 1888  664 2002/09/24-17:02:06.890 00000008
  Line 7: Recording Voice
  SFLOG 1888  664 2002/09/24-17:02:06.890 00000100
  Line 7: Recording c:\Bridge\Starfish\Out\6c37c321-533e-45fc-bdf7-1676c6ed3046
  SFLOG 1888  664 2002/09/24-17:03:07.859 00000008
  Line 7: Recording completed
  SFLOG 1888  664 2002/09/24-17:03:08.859 00000100
  Line 7: Received #
  SFLOG 1888  664 2002/09/24-17:03:08.859 00000100
  Line 7: Playing 8
  SFLOG 1888  664 2002/09/24-17:03:11.296 00000100
  Line 7: Received 9
  SFLOG 1888  664 2002/09/24-17:03:11.296 00000100
  Line 7: Playing 0282C6
  SFLOG 1888  664 2002/09/24-17:03:12.203 00000008
  Line 7: Message Saved
  ```

  If you do not see the above lines in the log, troubleshoot any errors or discrepancies that may be displayed in the SFLOG. Verify that your phone lines are plugged in and that the Octel node and Cisco Unity node serial numbers and node IDs are configured correctly.

If the calling Octel server does not have the Cisco Unity node serial number defined in its node configuration, the Bridge hangs up immediately when it receives a call from the Octel node. In the following example, the SFLOGs show that the calling Octel sent an initial handshake packet of "CD" instead of "BD":

```
SFLOG 1732  704 2003/01/10-22:04:49.711 00000008
Line 1: Call Received.
SFLOG 1732  704 2003/01/10-22:04:50.713 00000100
Line 1: Playing 1.sph
SFLOG 1732  704 2003/01/10-22:04:56.531 00000100
Line 1: Received CD
SFLOG 1732  704 2003/01/10-22:04:57.533 00000100
Line 1: Received
SFLOG 1732  704 2003/01/10-22:04:58.083 00000008
Line 1: Incoming Call Completed
```

Additionally, the Bridge logs the following warning to the Windows Event Log:

```
Event Type: Warning
Event Source: Bridge
Event Category: None
Event ID: 108
Bridge received an incoming call that could not be processed. The calling server does not have
a Serial Number defined in its Bridge node profile.
Verify that all remote servers configured to communicate with Bridge have Serial Numbers for
all Bridge nodes.
```

Because the Bridge requires the Cisco Unity node serial number to be configured on the Octel server, you will have to define the serial number for the Cisco Unity node in the node profile on the Octel server. When the serial number for the Cisco Unity node is properly configured in the node profile on the Octel server, the Octel system will send the expected "BD" handshake packet which the Bridge will successfully respond to with "CDD," and the call will proceed as in the following example:

```
SFLOG  736  752 2002/12/31-21:41:45.017 00000008
Line 3: Call Received.
SFLOG  736  752 2002/12/31-21:41:46.019 00000100
Line 3: Playing 1.sph
SFLOG  736  752 2002/12/31-21:41:51.436 00000100
Line 3: Received
SFLOG  736  752 2002/12/31-21:41:51.436 00000100
Line 3: Playing 1.sph
SFLOG  736  752 2002/12/31-21:41:56.974 00000100
Line 3: Received BD
SFLOG  736  752 2002/12/31-21:41:56.974 00000100
Line 3: Playing CDD
SFLOG  736  752 2002/12/31-21:42:02.052 00000100
Line 3: Received 12##C#5D82AC6AA897
SFLOG  736  752 2002/12/31-21:42:02.062 00000100
Line 3: Protocol Level = 3
SFLOG  736  752 2002/12/31-21:42:02.062 00000100
Line 3: Playing 012444C54331CA
```

If the Message Was Received by the Bridge

- If the SFLOGs indicate that the handshake was successful, and that the Bridge received the message, a copy of the message should be saved to the Bridge\VPIM\Internet\Out and Bridge\VPIM\Internet\Out\Tmp directories.

Note The message will stay in the Bridge\VPIM\Internet\Out\Tmp directory only for the number of days that is set in the Retention Days for Temporary SMTP Messages setting. The message will stay in the Bridge\VPIM\Internet\Out directory until it is delivered to the Interop Gateway.

- Verify that the voice message appears in the Bridge\VPIM\Internet\Out\Tmp directory.

BANANA admin Call States, and Reasons for Communication Errors

When the Bridge receives or makes a call, the call goes through various states. If a call fails for some reason, BANANA admin displays the state the call was in when it failed. Table 5-2 lists the possible call state codes and text that may be displayed in BANANA admin. BANANA admin also displays a reason the call failed. Table 5-3 lists the reason codes and text for communication errors. If a call results in an error, BANANA admin assigns an error code by combining the call state and reason codes.

Table 5-2 Call State Code and Text Displayed in BANANA admin

Call State Code	Call State Text
0	Complete
1	Dialing
2	Wake-up
3	Wake-up Response
4	Line Sync
5	Line Sync Response
6	Session Header
7	Session Header Response
8	Message Header
9	Message Header Response
10	Additional Recipient Header
11	Additional Recipient Header Response
12	Text Name Confirmation
13	Audio Transmission
14	Audio Terminator
15	Fax Request
16	Fax Transmission
17	Save Request

Table 5-2 Call State Code and Text Displayed in BANANA admin (continued)

Call State Code	Call State Text
18	Save Response
19	Message Response
20	Admin Request
21	Admin Mailbox Response
22	Admin Response
23	Admin Recording Recd Confirmation
24	Text Name Response
25	Text Name Transmission
26	Recording
27	Recording Voice Name
28	Playing
29	Add Recipients
30	Call Out Process Initiated
31	Failure After Outbound Message Rejection
32	Request For Voice Name
998	Other
999	Unknown

Table 5-3 BANANA admin Reason Code and Reason Text for Communication Errors

Reason Code	Reason Text
0	Successful
1	Line Error
2	Line State Unknown
3	Busy
4	Ring No Answer
5	Expected Data Not Received
6	Received DTMF String Longer Than Expected
7	Received DTMF String Shorter Than Expected
8	Received Data Invalid
9	Silence Timeout
10	No End-of-Fax Received
11	Bridge Rejected Admin Name Push
12	Calling Ser# Not Configured as Octel Node
13	Target Unity Node Not Configured; or Invalid DTMFs
998	Other

Table 5-3 BANANA admin Reason Code and Reason Text for Communication Errors (continued)

Reason Code	Reason Text
999	Unknown

Bridge Compensates for Echoed Digits in Wakeup Packets

When viewing the starfish logs on the Unity Bridge server, or using BANANA to view call detail, the wakeup (BD) and wakeup response (CDD) packets contain additional B, C, and/or D digits however the call may proceed normally to completion or to some other point in the protocol.

Echoed digits that occasionally appear in the log do not indicate a problem. However, if echo is consistently a problem during transmissions and calls consistently fail later in the protocol despite the successful completion of the wakeup portion, the gateway settings and other environmental conditions should be investigated to resolve any underlying problems.

When an inbound call is received by the Bridge, the Bridge requires the first inbound DTMF sequence to be the Octel analog networking wakeup sequence of 'BD.' Exceptions to this are as follows:

1. If 'B' is received, without receiving the 'D' within the configured Inbound DTMF - Inter-Digit Timeout, the Bridge will return to a state waiting for 'BD.'
2. If 'BD' is any part of the sequence received, the entire sequence is accepted as the wakeup. In regular expression terms, the acceptable wakeup sequence would be represented as .*BD.*

Any sequence other than 1 and 2 above received while awaiting the wakeup sequence after answering an inbound call will be considered invalid and the call will end at this point. This includes a sequence of 'CD,' which is a valid wakeup sequence in the Octel analog networking protocol, but not supported by the Bridge (see CSCea35313).

When the Bridge places an outbound call, upon detection of a connected state, the Bridge sends the 'BD' wakeup sequence to the remote system. The Bridge requires the response from the remote system to be the Octel analog networking wakeup response of 'CDD.' Exceptions to this are as follows:

1. If 'CDD' is any part of the response sequence received, the entire sequence is accepted as the valid wakeup response. In regular expression terms, the acceptable wakeup sequence would be represented as .*CDD.*
2. If the response received begins with 'B,' but does not include 'CDD,' the Bridge will return to a state waiting for 'CDD.' This is to account for any echo conditions that may occur. The regular expression representation of sequences falling into this category is B.* (Note that anything matching the regular expression B.*CDD.* would fall into category a and be accepted immediately).

Any response sequence other than 1 and 2 above received while awaiting the wakeup response sequence after sending the 'BD' wakeup sequence will be considered invalid and the call will end at this point.

Uninstalling Bridge Networking Components

Overview

This chapter provides the uninstall information that you need in the following circumstances:

- In some organizations, Bridge Networking is used only for a period of time as subscribers are moved from Octel to Cisco Unity. When the transition is complete, and all subscribers are using Cisco Unity, the Bridge Networking option needs to be completely removed. See the "Completely Removing Bridge Networking" section on page 6-1.
- If you already have a Cisco Unity server configured as the bridgehead, and you want to make another server the bridgehead instead, see the "Making Another Cisco Unity Server the Bridgehead" section on page 6-2.
- If you want to move the Bridge software to another server, see the "Uninstalling the Bridge Software from the Bridge Server" section on page 6-5.

Completely Removing Bridge Networking

To completely remove the Bridge Networking option, do the following tasks:

1. Delete the existing Bridge delivery locations and Bridge subscribers. See the "To Delete the Bridge Delivery Locations and Bridge Subscribers" section on page 6-2.
2. Either disconnect the Bridge server from the network, or remove the Bridge software from the Bridge server. See the "To Uninstall the Bridge Software from the Bridge Server" procedure on page 6-2.

When designating the bridgehead server, you run ConfigMgr.exe on a Cisco Unity server. ConfigMgr.exe creates the UOmni_<Server Name> account and registers CsBridgeConnector as a service in order to enable automatic Bridge subscriber directory updates. The CsBridgeConnector service may still be running on the bridgehead server, and the UOmni_<Server Name> mailbox will still exist. The service and mailbox can be safely left as is after all Bridge data has been removed; we do not recommend that you disable the service or remove the mailbox. However, if you do decide to delete the UOmni mailbox, the CsBridgeConnector service will log errors to Event Viewer about not being able to find the UOmni mailbox. You can safely ignore the errors. Although you can stop the CsBridgeConnector service to prevent it from logging errors, every time that the Cisco Unity server is restarted, the CsBridgeConnector service will be started and will again log errors to Event Viewer about not being able to find the UOmni mailbox.

To Delete the Bridge Delivery Locations and Bridge Subscribers

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

Step 2 In the left pane, double-click **Global Subscriber Manager**.

Step 3 Expand the tree in the left pane so that the delivery location to be deleted is visible.

Step 4 Right-click the location and select **Delete This Location**. Click **Yes** on the warning dialog box.

All the Bridge subscribers associated with the delivery location are deleted automatically when the location is deleted. The corresponding Domino Person documents are also deleted.

Step 5 Repeat Step 4 as needed to delete all the Bridge locations.

Step 6 Close Global Subscriber Manager and Tools Depot.

To Uninstall the Bridge Software from the Bridge Server

Step 1 Wait until all outgoing analog messages on the Bridge have been delivered. To do so, verify that all subdirectories in the Bridge\Starfish\In directory are empty, and that no ports are in a Sending state on the Bridge Line Status page in the Bridge Administrator.

Step 2 Open the Services MMC on the Bridge Server, and stop the Unity Bridge service.

Incoming messages on calls that are in progress are allowed to finish transmission before the service is stopped. Calls in progress will not be allowed to begin transmission of new incoming messages after the Unity Bridge service shutdown has been requested. When all analog ports are idle and in a Down state on the Bridge Line Status page, the Unity Bridge service has stopped.

Step 3 Wait five minutes to allow processing to complete on any messages received just prior to Unity Bridge service shutdown.Verify that there are no messages queued in the Vpim\Internet\Out directory.

Step 4 Open the Services MMC on the Bridge Server, and stop the Digital Networking service.

Step 5 Open the Add/Remove Programs Control Panel, click **Unity Bridge**, and click **Remove** to uninstall the Cisco Unity Bridge software.

Step 6 Restart the Bridge server.

Making Another Cisco Unity Server the Bridgehead

If you already have a Cisco Unity server configured as the bridgehead, and you want to make another server the bridgehead instead, the following task list and procedures guide you through the process.

1. Gather information about the existing Bridge delivery locations. See the "To Obtain Information About Existing Delivery Locations" procedure on page 6-3.
2. Write down the Bridge options settings and the subscriber template settings that were used to create Bridge subscriber accounts. See the "To Gather Other Bridge-Related Information on the Existing Bridgehead" procedure on page 6-3.

3. If you want to manually recreate the Bridge subscriber accounts on the new bridgehead server instead of letting them be auto-created, save the existing Bridge subscriber information to a CSV file. See the "To Export Bridge Subscriber Data to a CSV File" section on page 6-3 and the "To Modify the CSV File for Use with the Cisco Unity Bulk Import Wizard" section on page 6-4.
4. Delete the existing Bridge delivery locations and Bridge subscriber accounts. "To Delete the Bridge Delivery Locations and Bridge Subscribers" section on page 6-4.
5. Delete the UOmni account. This is necessary because the UOmni account is associated with the existing bridgehead server. See the "To Delete the UOmni Person Document and Mail File" section on page 6-5.
6. Follow the instructions in the "Configuring the Cisco Unity Server Designated as the Bridgehead" section on page 2-9, making use of the information that you obtained from the old bridgehead server. (Note that if you have CSV files with delivery location and/or Bridge subscriber data, you use those CSV files with the Cisco Unity Bulk Import wizard instead of preparing new ones.)

To Obtain Information About Existing Delivery Locations

The Cisco Unity Bulk Import wizard allows you to export delivery location data to a CSV file.

Step 1 Disable virus-scanning and Cisco Security Agent services on the existing bridgehead server, if applicable.

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

Step 3 Follow the on-screen instructions to export the data to a CSV file.

To Gather Other Bridge-Related Information on the Existing Bridgehead

Step 1 Open the Cisco Unity Administrator on the existing bridgehead server.

Step 2 Go to the **Network > Bridge Options > Subscriber Creation Options** page, and either write down the information on the page, or take a screen shot of the page and save it to a file. (Press **Alt-PrtSc** to save a copy of the screen to the Windows clipboard. Open Microsoft Paint, paste the image, and save the file.).

Step 3 Go to the **Network > Bridge Options > Unknown Caller** page, and either write down the information on the page, or take a screen shot of the page and save it to a file.

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

Step 5 Click the **Find** icon.

Step 6 Enter the name of the template that is used for creating Bridge subscribers, and click **Find**.

Step 7 On the displayed list, double-click the template name.

Step 8 On each of the subscriber template pages, write down the settings that you changed from default values. If you are unsure which settings you changed, either write down all of the settings, or take a screen shot of the page and save it to a file.

To Export Bridge Subscriber Data to a CSV File

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 **Subscriber Information Dump**. The Subscriber Information Dump dialog box opens.

Step 3 In the Subscribers to Dump list, click **Bridge Subscribers Only**.

Step 4 Indicate the output file name and location.

Step 5 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 6 In the Data to Include in Output File list, check the **First Name**, **Last Name**, **Primary Extension**, and **Remote Address** check boxes. You can also check other check boxes in the list, as applicable.

Step 7 Click **Start**.

Step 8 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 9 Exit the Subscriber Information Dump and Tools Depot.

To Modify the CSV File for Use with the Cisco Unity Bulk Import Wizard

Step 1 Open the output CSV file in a text editor or spreadsheet application.

Step 2 Modify the column headers in the first row of the CSV file by changing the following headers:

First Name,Last Name,Primary Extension,RemoteAddress

to:

FIRST_NAME,LAST_NAME,DTMF_ACCESS_ID,REMOTE_ADDRESS

Step 3 If all Bridge subscribers will be associated with the same Bridge delivery location, skip to Step 4. (You do not need to include the DELIVERY_LOCATION column header because you will be prompted to specify a default delivery location when running Cisco Unity Bulk Import wizard.)

Otherwise, add the DELIVERY_LOCATION column header to the first row and enter the applicable delivery location Dial ID in each data row. If a row does not contain a value for DELIVERY_LOCATION, the default delivery location that the Cisco Unity Bulk Import wizard prompts for will be used.

Step 4 Change any other column headers as applicable. Refer to the Cisco Unity Bulk Import wizard Help for details.

Step 5 Save and close the CSV file.

To Delete the Bridge Delivery Locations and Bridge Subscribers

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

Step 2 In the left pane, double-click **Global Subscriber Manager**.

Step 3 Expand the tree in the left pane so that the delivery location to be deleted is visible.

Step 4 Right-click the location and select **Delete This Location**. Click **Yes** on the warning dialog box.

All the Bridge subscribers associated with the delivery location are deleted automatically when the location is deleted. The corresponding Domino Person documents are also deleted.

Step 5 Repeat Step 4 as needed to delete all the Bridge locations.

Step 6 Close Global Subscriber Manager and Tools Depot.

To Delete the UOmni Person Document and Mail File

Step 1 Open the Domino Administrator.

Step 2 Click the **People and Groups** tab.

Step 3 In the tree in the left pane, expand the **People** container.

Step 4 In the right pane, right-click **Omni, Unity** and click **Delete**.

Step 5 On the Delete Person dialog box, click **Delete the Mail Database on the Users' Home Server**.

Step 6 Click **OK**.

The Administration Process will create an Approve Mail File Deletion request. Refer to your Domino documentation for more information on approving mail file deletions via the Administration Process.

Step 7 Exist the Domino Administrator.

The CsBridgeConnector service on the old bridgehead server is going to log errors to Event Viewer about not being able to find the UOmni mail file. You can just ignore the errors. Alternatively, you can stop the CsBridgeConnector service. However, every time the Cisco Unity server is restarted, the CsBridgeConnector service will be started and will again log errors to Event Viewer about not being able to find the UOmni mail file.

Uninstalling the Bridge Software from the Bridge Server

If you are moving the Bridge software to another server, you should do so during off-hours while message traffic is light. Before uninstalling the Bridge software, you may want to back up the Bridge configuration files and restore them to the new Bridge server. See the "Backing Up and Restoring a Bridge Server" section on page 3-6 for more information.

If you are completely removing Bridge Networking, verify that you have already deleted the Bridge delivery locations and Bridge subscribers from Cisco Unity as described in the "Completely Removing Bridge Networking" section on page 6-1. This will prevent Cisco Unity subscribers from inadvertently sending messages to the Bridge server, which could result in undeliverable messages for which the sender would not receive an NDR.

To Uninstall the Bridge Software from the Bridge Server

Step 1 Wait until all outgoing analog messages on the Bridge have been delivered. To do so, verify that all subdirectories in the Bridge\Starfish\In directory are empty, and that no ports are in a Sending state on the Bridge Line Status page in the Bridge Administrator.

Step 2 Open the Services MMC on the Bridge Server, and stop the Unity Bridge service.

Incoming messages on calls that are in progress are allowed to finish transmission before the service is stopped. Calls in progress will not be allowed to begin transmission of new incoming messages after the Unity Bridge service shutdown has been requested. When all analog ports are idle and in a Down state on the Bridge Line Status page, the Unity Bridge service has stopped.

Step 3 Wait five minutes to allow processing to complete on any messages received just prior to Unity Bridge service shutdown.Verify that there are no messages queued in the Vpim\Internet\Out directory.

Step 4 Open the Services MMC on the Bridge Server, and stop the Digital Networking service.

Step 5 Open the Add/Remove Programs Control Panel, click **Unity Bridge**, and click **Remove** to uninstall the Cisco Unity Bridge software.

Step 6 Restart the Bridge server.

Reference: Bridge Settings on the Cisco Unity Server

When setting up Cisco Unity and the Bridge for networking, you enter information in both the Cisco Unity Administrator and in the Bridge Administrator. This chapter provides details about the Bridge Networking settings in the Cisco Unity Administrator. See the following sections for more information:

- Bridge Delivery Locations Profile Settings, page 7-1
- Bridge Delivery Locations Prefixes, page 7-4
- Bridge Delivery Locations Subscriber Creation Settings, page 7-5
- Bridge Options Subscriber Creation Settings, page 7-6
- Bridge Options Synchronization Settings, page 7-7
- Bridge Options Unknown Caller Settings, page 7-9

Also see the "Primary Location Settings" chapter.

Bridge Delivery Locations Profile Settings

Delivery locations are Cisco Unity objects that contain the addressing information that Cisco Unity needs to send messages to and receive messages from other voice messaging systems—which may or may not be Cisco Unity systems. You create a delivery location that corresponds to each remote messaging system with which the local Cisco Unity server communicates.

When creating a delivery location, you specify Bridge as the Destination Type. The Destination Type determines which fields are displayed on the delivery locations page.

Use the following tables to learn more about the profile settings for delivery locations.

Table 7-1 Profile Settings Applicable to All Types of Delivery Locations

Field	Considerations
Name	This displays the name of the delivery location. To change the name, enter a new name here, and then click the Save icon.

Table 7-1 Profile Settings Applicable to All Types of Delivery Locations (continued)

Field	Considerations
Dial ID	Enter the ID that identifies the location to Cisco Unity. Enter numbers only, up to a maximum of ten digits. The default minimum length is three digits. Although the minimum length for Dial IDs can be reduced by using the Advanced Settings Tool, one- and two-digit Dial IDs may conflict with private distribution list IDs during an address search. When a subscriber addresses a message by entering a one- or two-digit number, Cisco Unity first searches for a matching private distribution list. If a match is found, the search stops. Therefore, when a subscriber addresses a message by entering a location Dial ID (to narrow down the search scope to a particular location), if the number entered matches a private distribution list ID, the conversation offers only the private distribution list as a destination. If subscribers do not address messages to other locations by first entering a Dial ID, there is no conflict, and the minimum length for Dial IDs can be reduced to accommodate complex dial plans. When sending messages to a remote location, subscribers can dial a number that is made up of the Dial ID and the Remote mailbox number of the recipient. The following policies are recommended: • Establish a fixed length for Dial IDs and if possible, a fixed length for extensions. • Assign unique Dial IDs. Dial IDs should not be the same as other Dial IDs or extensions. • Assign Dial IDs that have at least three-digits. • Use a different numbering range for Dial IDs than for extensions. • If you use variable-length Dial IDs, the first digits of each ID should be unique with respect to other Dial IDs. • Even if the Dial ID will never be used by subscribers when they address messages, enter a number that does not conflict with extensions, such as 001 or 002.
Recorded Name	Record a name for the delivery location. The subscriber conversation plays this recorded name in a number of places. For example, assume that the setting Include Locations in Searches on the Network > Primary Location > Addressing Options page is enabled. When subscribers address a message by spelling the name, the recorded name for this delivery location is played in the message addressing search results along with subscriber names. (For example: “There are two matches. For Chris Newton, press 1. For New York, press 2.”) To record the name here, use the Media Master control bar. (Note that the Media Master is not available across a firewall that blocks DCOM communications.) Use the Options menu in the Media Master control bar to set recording and playback devices, if applicable, and to use other sound files.

Table 7-1 Profile Settings Applicable to All Types of Delivery Locations (continued)

Field	Considerations
Destination Type	*Display only.* Indicates the type of delivery location. The Destination Type is specified when the delivery location is created, and it cannot be changed. The Destination Type is one of the following: • AMIS—Indicates that the delivery location corresponds to an AMIS-compliant voice messaging system. Messages are sent by using the industry-standard Audio Messaging Interchange Specification analog (AMIS-a) protocol. • Bridge—Indicates that the delivery location corresponds to an Octel node in an Octel analog network. Messages are exchanged between Cisco Unity and the Octel system by using the Cisco Unity Bridge. Cisco Unity sends messages to the Bridge in Voice Profile for Internet Mail (VPIM) format with proprietary extensions. The Bridge converts the message format and sends it to the appropriate Octel server by using the Octel Analog Networking protocol. • VPIM—Indicates that the delivery location corresponds to a VPIM-compliant voice messaging system. Messages are sent by using the industry-standard VPIM protocol over the Internet or a private TCP/IP network.

Table 7-2 Profile Settings Specific to Bridge Delivery Locations

Field	Considerations
Bridge Server Full Computer Name	Enter the fully qualified domain name of the Bridge server used for messaging with the Octel node represented by this delivery location. This is the name displayed on the Bridge server in the Windows System Control Panel on the Network Identification tab in the Full Computer Name field. The name entered here must also match the name entered in the Bridge Server Full Computer Name field on the Digital Networking page in the Bridge Administrator.
Octel Node Serial Number	Enter the serial number of the Octel node that corresponds to this delivery location. This number must match the serial number of one of the nodes displayed on the Octel Nodes page in the Bridge Administrator. The number entered here must also match the serial number of a corresponding Octel node. The Octel Node Serial Number and the Remote Mailbox Length as a pair must be unique within the global directory. In the rare case that this is needed, you can create more than one Bridge delivery location with the same Octel Node Serial Number but with different Remote Mailbox Length values.

Table 7-2 Profile Settings Specific to Bridge Delivery Locations (continued)

Field	Considerations
Remote Mailbox Length	Enter the number of digits required for mailboxes as specified in Octel for the node that corresponds to this delivery location. You create at least one Bridge delivery location for each remote Octel node in the Octel analog network. 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. For example, assume that an Octel server with the serial number 45678 has been configured to allow mailboxes of length 4 and 5. When configuring the Cisco Unity bridgehead server, you create two Bridge delivery locations with the Octel Node Serial Number 45678; one delivery location has the Remote Mailbox Length set to 4, and the other has the Remote Mailbox Length set to 5. If you specify a prefix (or prefixes) for the location, then the value that you entered for the remote mailbox length is used to determine the recipient mailbox number. To determine the mailbox number when addressing a message, Cisco Unity starts at the end of the entered number, and keeps including digits until the number of digits equals the remote mailbox length.

Bridge Delivery Locations Prefixes

Use the following table to learn more about the delivery location prefixes page.

Table 7-3 Network > Delivery Locations > Prefixes Page

Field	Considerations
Prefixes Assigned to This Location	Enter a prefix or prefixes for the Octel node that corresponds to this delivery location. Prefixes are optional, but you may enter as many prefixes as required by your numbering plan. Enter numbers only, up to a maximum of 21 digits. The minimum length is 1 digit. Each prefix must be unique with respect to other prefixes within the global directory. When Octel subscribers send messages to subscribers on other nodes in the Octel analog network, they enter a network address as the message destination. A network address consists of a node prefix, which identifies the remote server, and the mailbox number of the recipient. In many cases, the prefix is the same as either the area code where the destination node is located, or the prefix(es) defined in the phone system dialing plan. This allows subscribers to use the same number when addressing a network message as they do when calling. In Cisco Unity, prefixes are optional, depending on your numbering plan. Prefixes are not needed when Cisco Unity subscribers can send messages to Octel subscribers by entering the dial ID of the location followed by the recipient mailbox number.
Assigned Location Prefixes	This displays prefixes that are in use for all delivery locations.

Bridge Delivery Locations Subscriber Creation Settings

Use the following table to learn more about the creation settings for auto-created Bridge subscribers associated with the delivery location.

Table 7-4 Network > Delivery Locations > Subscriber Creation Page

Field	Considerations
If the Octel Text Name Has No Comma	Indicate how Octel text names that do not contain commas should be parsed into first and last names for auto-created Bridge subscribers. Select one of the following: • Treat as FirstName LastName • Treat as LastName FirstName In Cisco Unity, the first and last names of subscribers are stored as distinct fields in the directory, which allows directory lookups to be configured by either the last or the first name. However, Octel subscriber names are stored as one single name. When the Bridge sends a request to create a new Bridge subscriber, the CsBridgeConnector service parses the single Octel text name by the rule you have selected here. For example, when Treat as FirstName LastName is selected, the Octel text name "Terry Campbell" is parsed such that "Terry" is the first name, and "Campbell" is the last name. When Treat as LastName FirstName is selected, the Octel text name "Bader Kelly" is parsed such that "Kelly" is the first name, and "Bader" is the last name. Default: Treat as LastName FirstName.
Mapping Octel Text Names to Cisco Unity Bridge Subscriber Names	Indicate how Octel text names should be mapped to the display names for auto-created Bridge subscribers. Select one of the following. • Map Octel Text Names Directly to Cisco Unity Bridge Subscriber Names: Click this option to have the display names for Bridge subscribers be the same as their corresponding Octel text names. • Custom Mapping: Click this option and enter a rule that defines how Octel text names are mapped to Bridge subscriber display names. Enter the tokens <FirstName>, <LastName>, or <TextName> in any combination along with any additional text. Always precede <FirstName>, <LastName>, or <TextName> with a space, comma, or semi-colon if not at the beginning of the rule, and always succeed one of these tokens with a space, comma or semi-colon unless it comes at the end of the rule. In other words, you must enter a space, comma, or semi-colon separator between tokens and additional text, except at the beginning or end of a rule. For example, assume that the Octel text name is "Bader, Kelly." – The rule <TextName> produces the display name Bader, Kelly. – The rule <FirstName> <LastName> produces the display name Kelly Bader. – The rule <TextName> (Voice mail) produces the display name Bader, Kelly (Voice mail). Unless hidden, Bridge subscriber display names are shown in the address books for the Cisco Personal Communications Assistant. To help prevent others from sending e-mail to Bridge subscribers, you may want to append a term such as "(Voice mail)" to the names of Bridge subscribers. Default: Map Octel Text Names Directly to Cisco Unity Bridge Subscriber Display Names.

Table 7-4 Network > Delivery Locations > Subscriber Creation Page (continued)

Field	Considerations
Include Location Dial ID in Primary Extension on Auto-Created Bridge Subscribers	Check the box to have the primary extension consist of the delivery location dial ID added to the beginning of the remote mailbox number when the CsBridgeConnector service creates Bridge subscribers.

Bridge Options Subscriber Creation Settings

Bridge options subscriber creation options are applied to all Bridge subscribers automatically created by Cisco Unity when it receives an Add User request from the Bridge.

Use the following table to learn more about Bridge subscriber creation options settings.

Table 7-5 Network > Bridge Options > Subscriber Creation Options Page

Field	Considerations
Subscriber Template	Select the template on which to base new Bridge subscriber accounts. The template affects most subscriber settings. By default, the predefined {Bridge Subscriber} Template will be used for auto-created Bridge subscribers, but you may select another template. By default, Bridge subscribers created by using the {Bridge Subscriber} Template are not added to the All Subscribers distribution list and are not listed in the Cisco Unity phone directory.
Allow Automatic Creation of Bridge Subscribers	Check the box to allow the CsBridgeConnector service to automatically create a Bridge subscriber and associated Person document when an Add-New-Subscriber request is received from the Bridge. When the box is unchecked, Add-New-Subscriber requests that do not match existing Bridge subscribers are discarded without processing. This setting supersedes the Allow Automatic Modification of Bridge Subscriber Names and Allow Automatic Modification of Bridge Subscriber Recorded Voice Name settings. If the Allow Automatic Creation of Bridge Subscribers box is checked, and an Add-New-Subscriber request is received that does not match a remote address of an existing Bridge Subscriber, then the Bridge Subscriber will be created based on the text name and voice name (if applicable) received in the request, regardless of the Modification settings below. Default: Check box not checked.
Allow Automatic Deletion of Bridge Subscribers	Check the box to allow the CsBridgeConnector service to automatically delete a Bridge subscriber and associated Person document when a Delete-Subscriber request is received from the Bridge. When the box is unchecked, Delete-Subscriber requests received from the Bridge are discarded without processing. Default: Check box not checked.

Table 7-5 Network > Bridge Options > Subscriber Creation Options Page (continued)

Field	Considerations
Allow Automatic Modification of Bridge Subscriber Names (First, Last, Display)	Check the box to allow the CsBridgeConnector service to automatically modify the first, last and display name for a Bridge subscriber and associated Person document when a Change-Text-Name request is received from the Bridge. Additionally, the CsBridgeConnector service will modify the first, last and display name for a Bridge subscriber and associated Person document when an Add-New-Subscriber request is received from the Bridge that matches an existing Bridge subscriber. When the box is unchecked, Change-Text-Name requests and Add-New-Subscriber requests that match existing Bridge subscribers are discarded without processing. Default: Check box not checked.
Allow Automatic Modification of Bridge Subscriber Recorded Voice Name	Check the box to allow the CsBridgeConnector service to automatically modify the recorded voice name for a Bridge subscriber when a Change-Spoken-Name request is received from the Bridge. Also allows the CsBridgeConnector service to automatically modify the recorded voice name for a Bridge subscriber when an Add-New-Subscriber request is received from the Bridge that matches an existing Bridge subscriber. When the box is unchecked, Add-New-Subscriber requests that match existing Bridge subscribers and Change-Spoken-Name requests and are discarded without processing. Default: Check box not checked.

Bridge Options Synchronization Settings

The Bridge synchronization options allow you to control the scope when synchronizing the subscriber directory on the Bridge with the subscriber directory on Cisco Unity. Additionally, this page provides an option for forcing a full synchronization.

Use the following table to learn more about Bridge synchronization options settings.

Table 7-6 Network > Bridge Options > Bridge Synchronization Options Page

Field	Considerations
Unity Node IDs	Displays a list of the serial numbers that have been defined on Cisco Unity subscribers. These are the serial numbers of nodes that the Cisco Unity bridgehead and Bridge servers represent in the Octel analog network.
Cisco Unity Bridge Servers: Select	Check the box next to each Bridge server address to which Cisco Unity subscriber information should be sent. Verify that the Bridge server(s) to which directory information will be sent is configured with a Unity Node for each serial number listed in the Unity Node ID table.

Table 7-6 Network > Bridge Options > Bridge Synchronization Options Page (continued)

Field	Considerations
Synchronize	Click this button to force a full synchronization of subscriber data on Cisco Unity with the subscriber directory on the selected Bridge server(s). For directory data about newly-created subscribers to be automatically sent to the Bridge, you first create the subscribers in Cisco Unity, and then create corresponding Unity Node(s) on the Bridge. If you do the reverse and create a Unity Node on the Bridge before creating any subscribers with the same serial number, you will have to force a synchronization. You can click Synchronize to force a full synchronization of the entire selected Bridge server, or you can delete and then add back the Unity Node on the Bridge server to force a synchronization of a specific Unity Node. During normal operation, Cisco Unity automatically synchronizes subscriber information with the Bridge on a regular basis. When a subscriber account is added, deleted, or modified, Cisco Unity sends the account information to the Bridge. The Bridge makes this information available to other Octel nodes when they make an administrative call to retrieve the voice and text names of Cisco Unity subscribers. You may want to force synchronization if the Cisco Unity server, the Bridge, or the network connection to the Bridge has been down for a long period of time, and if there have been numerous changes to subscriber information in Cisco Unity. Directory synchronization does not impact messaging. Subscribers can still send and receive messages when the directories are not synchronized. The time necessary for a full synchronization depends on many factors, such as the network connection to the Bridge, the size of the directory, whether subscribers have recorded voice names, and the codec used to record the voice names. (Voice name data is large in comparison with the other subscriber information that is sent to the Bridge.) To get an idea of how long full synchronization from Cisco Unity to the Bridge may take, here are a few examples obtained during testing: • 1000 subscribers with 5-second voice names recorded with the G.711 codec—approximately 5 hours • 1000 subscribers with no recorded voice names—approximately 3 minutes • 1000 subscribers with 2.5-second voice names recorded with the G.711 codec—approximately 2.5 hours • 1000 subscribers with 2.5-second voice names recorded with the G.729a codec—approximately 1 hour

Bridge Options Unknown Caller Settings

Table 7-7 Network > Bridge Options > Unknown Caller Page

Field	Considerations
Legacy Mailbox ID	Enter the mailbox number to be used for messages left for Bridge subscribers from unidentified callers. For messages to be delivered to an Octel node, Octel analog networking requires that the message sender has a mailbox number and a serial number. Enter any combination of digits from 0 to 9. Do not include any spaces. Typical mailbox numbers contain 3 to 10 digits (although a maximum of 64 digits is accepted).
Node ID	Select from the list or enter the serial number to be used for messages left for Bridge subscribers from unidentified callers. Choose a serial number from among those assigned to Unity Node(s) on the Bridge server(s). Enter any combination of digits from 0 to 9. Do not include any spaces. Typical serial numbers contain 4 or 5 digits (although a maximum of 64 digits is accepted).

Reference: Settings on the Bridge Server

When setting up Cisco Unity and the Bridge for networking, you enter information in both the Cisco Unity Administrator and the Bridge Administrator.

Accessing the Bridge for Administration

You can access the Bridge locally or remotely in Internet Explorer.

- To access the Bridge 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 from a remote server, in Internet Explorer, enter http://machinename, where machinename is the name of the Cisco Unity Bridge server.

This chapter provides details about the settings in the Bridge Administrator. See the following sections for more information:

- System Settings, page 8-1
- Digital Networking, page 8-6
- Unity Nodes, page 8-9
- Unity Node Configuration, page 8-10
- Octel Nodes, page 8-12
- Octel Node Configuration, page 8-12
- Directory List, page 8-14
- Directory Entry, page 8-15
- Line Status, page 8-16
- Queue Status, page 8-18

System Settings

The System Settings page in the Bridge Administrator allows you to configure how the Cisco Unity Bridge server handles message delivery and the exchange of NameNet information on a global basis for all remote Octel nodes. This page also includes settings that allow you to control how call tracing and call logs are configured for troubleshooting between the Bridge and the Octel analog network.

- To return to the stored system settings before you have saved them, click Reload.
- To save your system settings, click Save.

Use the following table to learn more about the System Settings page.

Table 8-1 System Settings

Field	Considerations
Attempts if Busy	Enter a number from 1 to 15 for the number of times that the server will call a busy line before it returns all the messages currently in the outbound queue as non-deliverable. The default value is 15. The counter for Attempts if Busy is on a per-node basis. The counter is reset to 0 when the Bridge connects to the node.
Attempts on No Answer	Enter a number from 1 to 15 for the number of times that the server will call a line that does not answer before it returns all the messages currently in the outbound queue as non-deliverable. The default value is 15. The counter for Attempts on No Answer is on a per-node basis. The counter is reset to 0 when the Bridge connects to the node.
Attempts on Bad Connection	Enter a number from 1 to 100 for the number of times that the server will call a line with a bad connection before it returns all the messages currently in the outbound queue as non-deliverable. The default value is 100. A bad connection is usually caused by an interruption on the line or poor line quality. However, a bad connection can also occur as a result of problems delivering one particular message. Messages to a particular Octel node are delivered in First In First Out (FIFO) order. When the number specified for Attempts On Bad Connection has been reached, all messages queued for delivery to that node are returned to the senders. Therefore, if you set a value between 3 and 5, this reduces the number of messages building up in the outgoing queue that would be returned when the message delivery problem to a node is caused by a single message. However, on busier systems where multiple calls may be delivering messages to the same node simultaneously, increasing the setting to a value between 6 and 10 is recommended. The counter for Attempts on Bad Connection is on a per-node basis. The counter is reset to 0 when the Bridge connects to the node.
Interval if Busy	Enter a number from 1 to 60 for the interval in minutes that the server waits between attempts to call a busy line. The default value is 1 minute. The interval is timed on a per-node basis and is reset when the Bridge connects to the node.
Interval if No Answer	Enter a number from 1 to 60 for the interval in minutes that the server waits between attempts to call a line that does not answer. The default value is 1 minute. The interval is timed on a per-node basis and is reset when the Bridge connects to the node.
Name Aging	Enter a number from 1 to 90 for the number of days that the server will retain a usage-based directory entry that has not been referenced before deleting the entry. Enter 0 to disable name aging. The default value is 30 days. Higher values for Name Aging keep entries in the Bridge directory longer and decrease the rate of automatic deletion and recreation of Bridge subscribers. When you enter 0 to disable name aging, it does not matter how long it has been since a directory entry has received a message from a Cisco Unity subscriber. With name aging disabled, the directory entry and its associated Bridge subscriber are not deleted automatically. Note that when Bridge subscribers are automatically created, the corresponding Domino Person documents are automatically created. Similarly, when Bridge subscribers are automatically deleted, the corresponding Domino Person documents are automatically deleted.

Table 8-1 System Settings (continued)

Field	Considerations
Name Retrieval Retries	Enter a number from 0 to 90 for the maximum number of retries that are made to retrieve the spoken name if it is not available initially. The default value is 0, which means no retry attempts will be made.
Name Retry Interval	Enter a number from 1 to 30 for the number of days between attempts to retrieve a spoken name. The default value is 1 day. Note that the Name Retry Interval expiration is the same for all directory entries, so that all retries are made on the same day. The Name Retrieval Retries and Name Retry Interval settings allow you to control how often the Bridge attempts to retrieve spoken names that were not yet recorded on the Octel system when the Bridge initially attempted to retrieve them. When a name is marked for retrieval (either through the usage based rules or when the name is added as a permanent directory entry), the Bridge attempts to retrieve the text and spoken name. If the Bridge fails to retrieve the spoken name, then each night at midnight, the Bridge determines whether the Name Retry Interval has expired. If so, the Bridge finds all directory entries that do not have spoken names. Each directory entry contains a name retrieval retry counter. For each directory entry that does not have a spoken name, the Bridge determines whether the retry counter has reached the maximum retry count specified in the Name Retrieval Retries setting. If so, the name is not scheduled for retry. If the counter has not reached the maximum retry count, an administrative call is scheduled for the node associated with the name. (The Bridge makes administrative calls according to the schedule for the node.) If the spoken name is not found, the retry counter for the directory entry increments. Name Retrieval Retries and Name Retry Interval settings are only relevant to scheduled retry attempts for name retrieval. In addition to scheduled attempts, each time an outgoing message to a remote Octel subscriber that does not have a recorded name in the Bridge database is processed, voice name retrieval for that Octel subscriber is retried by the Bridge at the next opportunity according to the Administrative schedule for that node. This occurs even when Name Retrieval Retries is set to 0. To reset the retry attempts for a particular Octel Node directory entry, run the MBUpload utility using the “C” (Change) option in each record.
Accept Remote Push	Check this check box to enable the Cisco Unity Bridge to accept requests from remote nodes to send the text and spoken name information for remote Octel subscriber mailboxes. By default, the Bridge will attempt to retrieve name information for remote Octel subscribers when needed. Some remote systems may also provide the capability to push name information to other nodes; in order to allow the Bridge to accept this information, this check box must be checked. When unchecked, the Bridge will reject all such requests from any remote node. This setting was added in Cisco Unity Bridge version 3.0(6). Default: unchecked.

Table 8-1 System Settings (continued)

Field	Considerations
Queued Call Threshold	Enter a number from 1 to 1000 for the threshold number of messages that must be in the outgoing message queue of a specific node for an additional port to be used for message delivery. As the number of messages in the queue increases, an additional port is added when the number of messages in the queue reaches a multiple of this parameter. The default value is 10. For example, if the value of this parameter is 10, one port will be used for message delivery if there are fewer than 10 messages in the queue. For 10–19 messages, two ports will be used. For 20–29 messages, three ports will be used, and so on. The total number of ports used is limited by the Max Ports Per Node parameter. This parameter is also used to determine when to disconnect a port used for outgoing messages to a specific node. As the number of messages in the queue decreases, a port is disconnected when the number of messages in the queue is below the next lower multiple of this parameter. When only two ports are in use, as the number of messages in the queue drops below half of this parameter, the second port is disconnected. For example, if the value of this parameter is 10, three ports will be used for message delivery if there are 20–29 messages in the queue. As the number of messages in the queue decreases, the third port is not disconnected until the number of messages in the queue drops to 10 or fewer. When the number of messages drops to 5 or fewer messages, the second port is disconnected so that only one port is used to transmit the remaining messages. Note that normal, urgent, and administrative messages to a specific node are in separate outgoing message queues. The Queued Call Threshold parameter is applied to each queue.
Max Ports Per Node	Enter a number from 1 to 24 for the maximum number of ports that are allowed to be used simultaneously to deliver messages to a particular node. The default value is 4. Note that normal, urgent, and administrative messages to a specific node are in separate outgoing message queues. The Max Ports Per Node parameter is applied to each queue.
Max Play Attempts Per Message *(available in Bridge version 3.0(5) and later)*	Enter a number from 1 to 15 for the number of times that the Bridge will play a message when the Octel does not send the expected response that indicates the message was successfully received. If the Bridge does not get the expected response from the Octel after playing the message the specified number of times, the Bridge stops trying to deliver the message, logs an error in Event Viewer, and returns an NDR to the sender. The default value is 5. The counter for Max Play Attempts Per Message is on a per-message basis. The counter is reset to 0 when the message is either successfully transmitted or returned as undeliverable. Note that when the counter for Max Play Attempts Per Message is incremented, the counter for Attempts on Bad Connection is also incremented. Therefore, you should set the number for Max Play Attempts Per Message to be less than the number set for Attempts on Bad Connection so that only the problematic message will be returned as undeliverable. (When the Attempts on Bad Connection threshold is reached, all messages queued for delivery to the node are returned to the senders.)

Table 8-1 System Settings (continued)

Field	Considerations
Max Retention Time – Normal *(available in Bridge version 3.0(5) and later)*	Enter a number from 1 to 48 for the number of hours that a normal priority message is queued on the Bridge for analog delivery before being returned to the sender as undeliverable. If the Bridge cannot send the message within the specified time period, the Bridge stops trying to deliver the message, logs an error in Event Viewer, and returns an NDR to the sender. The default value is 48 hours. However, you may want to lower this setting so that a problematic message is returned as undeliverable before the Attempts on Bad Connection threshold is reached (which results in all messages that are queued for delivery to the node being returned to the senders). By doing so, the Bridge can handle situations where a particular message is causing a transmission failure.
Max Retention Time – Urgent *(available in Bridge version 3.0(5) and later)*	Enter a number from 1 to 48 for the number of hours that an urgent message is queued on the Bridge for analog delivery before being returned to the sender as undeliverable. If the Bridge cannot send the message within the specified time period, the Bridge stops trying to deliver the message, logs an error in Event Viewer, and returns an NDR to the sender. The default value is 12. However, you may want to lower this setting so that a problematic message is returned as undeliverable before the Attempts on Bad Connection threshold is reached (which results in all messages that are queued for delivery to the node being returned to the senders). By doing so, the Bridge can handle situations in which a particular message is causing a transmission failure.
Inbound DTMF – First Digit Timeout *(available in Bridge version 3.0(3) and later)*	Enter a number from 10000 to 99000 for the maximum time to wait in milliseconds for the first digit of an analog protocol response from the remote system. The default is 30000 milliseconds.
Inbound DTMF – Inter-Digit Timeout *(available in Bridge version 3.0(3) and later)*	Enter a number from 1000 to 99000 for the maximum time to allow in milliseconds between digits of an analog protocol response from the remote system. The default is 2500 milliseconds.
Call Log Retention	Enter a number from 1 to 366 for the number of days that call and queue logs are to be retained. The default is 7 days. Call and queue log data is placed in a common log file. Files are stored on the Bridge server in the Drive:\Path\Starfish\Log directory, where Drive and Path denote the drive and the topmost directory where the Bridge software is installed. A separate file is used for each day. Files are named CallLog_YYYYMMDD.LOG where YYYY is the year, MM is the month and DD is the day. Call logs are used by the Bridge Traffic Analyzer for generating reports on Bridge activity. If you open the log files in a text editor, do not modify them. (If the files are modified, the Bridge Traffic Analyzer may not be able to interpret the data in the log files.)

Table 8-1 System Settings (continued)

Field	Considerations
Call Tracing Level	The Bridge service creates a trace log file that records actions related to calls placed or received through the analog voice-fax card(s). The log records actions that the service attempts, notes whether those actions are completed successfully, and logs the reasons that failed actions were not successful. It stores the log information in the directory Drive:\Path\Starfish\Log, where Drive and Path denote the drive and the topmost directory where the Bridge software is installed. Within the Log directory are the files SFLOG.mmddttttLOG. Each of these files contains log entries for one hour of the day; the title indicates which hour. The directory also contains the log file SFLOG.LOG, to which the Bridge server adds current entries, and which is then saved to the appropriate hour log. Log files that are older than 24 hours are overwritten. Choose the level of detail you want to see in the trace log by selecting one of the following options from the Tracing Level box. The default setting is None. • None—No Logging. • Basic—Records basic call information. • Verbose—Records detailed call information. • Debug—Records even more detailed call information.

Digital Networking

Digital Networking is the interface used to exchange messages with a Cisco Unity server. The Digital Networking Settings page in the Bridge Administrator provides settings that allow you to control how the Bridge uses SMTP to communicate with Cisco Unity, and how message tracing and message retention are configured for troubleshooting between the Bridge and Cisco Unity servers.

- To return to the stored networking settings before you have saved them, click Reload.
- To save your networking settings, click Save.

Use the following table to learn more about the Digital Networking page.

Table 8-2 Digital Networking Settings

Field	Considerations
ESMTP Server *Optional*	Optionally, enter the IP address or name of the server that accepts incoming SMTP messages from the Bridge. The value in the ESMTP Server field is used by the Bridge to establish an SMTP connection when sending messages. Depending on your network, the server could be: • A Domino server with the SMTP Listener task enabled • An ESMTP e-mail host that acts as a relay server When the Bridge sends SMTP messages, it addresses the messages by using the domain name that is entered on the Unity Nodes page in the Unity SMTP Mail Suffix field. For example, if "voice.mydomain.com" is entered in the Unity SMTP Mail Suffix field, messages will be addressed to: IMCEAOMNI-AvVoiceMessage@voice.mydomain.com (The extension of the recipient is in another field in the header of the SMTP message.) The domain name must be resolvable to an IP address so that the Bridge can establish a connection to the server that accepts incoming SMTP messages. Although you can enter an IP address in the ESMTP Server field to resolve the domain name, as a best practice, we recommend that you use Domain Name Service (DNS) for name resolution. If using DNS is not an option, then add an entry to the HOSTS file on the Bridge server to resolve the domain name to an IP address. If you enter an IP address in the ESMTP field, the Bridge always uses the address when establishing an SMTP connection. Because the IP address in the ESMTP Server field overrides DNS and the HOSTS file (which are standard mechanisms for name resolution), use it as a last resort. Note that a name can be entered in the ESMTP Server field to establish the SMTP connection. For example, assume that "RelayServer" is entered in the ESMTP Server field and that "voice.mydomain.com" is in the Unity SMTP Mail Suffix field on the Unity Nodes page. SMTP Messages are still addressed to "IMCEAOMNI-AvVoiceAddress@voice.mydomain.com" but the Bridge uses "RelayServer" when establishing a connection to the server that accepts incoming SMTP messages. In this example, the name "RelayServer" would need to be resolved to an IP address by using standard means such as DNS or the HOSTS file on the Bridge server.
Bridge Server Full Computer Name	Enter the fully qualified domain name of the Bridge server. This is the name displayed in the Windows System Control Panel on the Network Identification tab in the Full Computer Name field. The name that you enter here must match the name that is displayed in the Cisco Unity Administrator on the Primary Locations page in the Unity Bridge Server Address field.

Table 8-2 Digital Networking Settings (continued)

Field	Considerations
Tracing Level	The Bridge Digital Networking service creates a trace log file that records actions that it attempts, notes whether those actions are completed successfully, and logs the reasons why failed actions were not successful. It stores the log information in the directory Drive:\Path\VPIM\Trace, where Drive and Path denote the drive and the topmost directory where the Bridge software is installed. Within the Trace directory are the files VPIM.mmddttttLOG. Each of these files contains log entries for one hour of the day; the title indicates which hour. The <path>\VPIM\MsgLog folder contains the log file VpimMsg.log, to which the Bridge server adds current entries and then saves them to the appropriate hour log. Log files that are older than 24 hours are overwritten. Choose the level of detail you want to see in the trace log by selecting one of the following options from the Tracing Level box. The default setting is None. • None—No logging is done. • Entry—1 only. Logs service status information. • Error—1 through 3. Logs service error information. • Verbose—1 through 5. Logs internal function status information. • Debug—1 through 8. Logs internal debugging information. • Flow—1 through 10. Logs internal function flow information. • Intense—1 through 100 (all messages). Logs internal intense debugging information. **Caution** Set the tracing level to Verbose or lower under most circumstances. Tracing levels higher than Verbose can consume a large amount of hard disk space and slow down the server, and should be selected only if advised by your technical support representative.

Table 8-2 Digital Networking Settings (continued)

Field	Considerations
Retention Days for Temporary SMTP Messages	Enter the number of days that temporary SMTP messages should be kept before being discarded. The default value is 0 (zero). The Bridge server can be set to save inbound messages from Cisco Unity and outbound messages to Cisco Unity in SMTP e-mail format. • Inbound messages from Cisco Unity are stored in the VPIM\Xcode\Inbound\Tmp directory on the Bridge server. *Cisco Unity Bridge 3.0(5) and later:* The directory VPIM\Xcode\Inbound\Failed is also created, although it is not utilized at this time. • Outbound messages to Cisco Unity are stored in the VPIM\Internet\Out\Tmp directory on the Bridge server. *Cisco Unity Bridge 3.0(5) and later:* Messages that the Bridge could not deliver to Cisco Unity are stored in VPIM\Internet\Out\Failed. Outbound messages that the Bridge successfully delivered are still stored in VPIM\Internet\Out\Tmp. Note that when the Bridge saves a message to the Failed directory, it also logs a message in the Event Viewer Application log. The messages are saved for the specified number of days after they are received (in the case of inbound) or sent (in the case of outbound). This setting is useful for troubleshooting message delivery problems. By setting this parameter to a non-zero value, you can verify whether messages make it to the Bridge. Then you can open the messages in Notepad to examine the header fields on each message to look for misspelled addresses. You can also determine whether the outbound messages are larger than an e-mail host in your system can accept.
SMTP Port	The TCP/IP port number used by the Digital Networking Service for sending and receiving SMTP messages. The default value is 25, which is the standard SMTP port number. The use of the standard port number is recommended unless special circumstances require the use of a different port number. The SMTP servers with which the Bridge is communicating must use the same SMTP port number.
Enable Extended Absence Notifications	Check this check box to enable Cisco Unity subscribers to receive delivery receipts when the extended-absence greeting for an Octel subscriber is enabled and the mailbox is accepting messages. If unchecked, Cisco Unity subscribers will not receive notification that the extended-absence greeting is enabled if messages sent to the Octel subscriber mailbox are accepted. This setting was added in Cisco Unity Bridge version 3.0(6). Default: unchecked.

Unity Nodes

The Unity Nodes page in the Bridge Administrator displays information about the Unity node that has been defined. You create and configure a Unity node for each Octel server that has been migrated; the Bridge represents the migrated Octel server in the Octel analog network. You must set up the Cisco Unity server for networking with the Bridge before entering information on this page.

When there are multiple Bridge servers, the same set of Unity Nodes serial numbers must be configured on each Bridge server.

The following buttons are on the Unity Nodes page:

- Add Button—Click Add to create a new node.

- Edit Button—Select the node from the Node list, and click Edit to modify an existing node.
- Delete Button—Select the node from the Node list, and click Delete to delete an existing node from the list. Note that deleting the node here only deletes the node information from the Bridge.

Unity Node Configuration

After clicking Add or Edit from the Unity Nodes page, the Unity Node Configuration page in the Bridge Administrator is displayed. On this page, you enter information about the Unity node. You can also view the directory entries associated with this node.

Use the following table to learn more about the Unity Node Configuration page.

Table 8-3 Unity Node Configuration Settings

Field	Considerations
Serial Number	Enter the serial number of the node. Assign a unique serial number for the Unity node. Serial numbers of all nodes must be unique to identify each messaging server in the network. The Serial Number must match the number that is displayed in the Cisco Unity Administrator on the Primary Locations page in the Unity Bridge Node ID field. If the Bridge server and the associated Cisco Unity server replace an existing Octel Node, enter the Serial Number of the Octel Node that is being replaced. The Serial Number also needs to be entered on each Octel node if it is not already there. Note that after the configuration settings are saved, you cannot change the serial number when editing the node. To change the Serial Number, you have to delete the node, and add it again with the correct Serial Number.
Name	Enter a descriptive name for the node. You can enter up to 20 characters.
Unity Bridgehead Server Name	Enter the server name of the Cisco Unity server with which the Bridge communicates. (Enter the server name only, and not the fully qualified domain name.)

Table 8-3 Unity Node Configuration Settings

Field	Considerations
Unity SMTP Mail Suffix	Enter the Interop Gateway foreign domain name. The Bridge uses the name you enter here when it constructs the "to" address of the SMTP messages destined for Cisco Unity. The messages are addressed in the following format: • IMCEAOMNI-AvVoiceMessage@<Unity SMTP Mail Suffix> For voice messages sent from Octel subscribers to Cisco Unity subscribers. • IMCEAOMNI-AvVoiceAddress@<Unity SMTP Mail Suffix> For directory messages sent from the Bridge to the Cisco Unity bridgehead server. For example, if "voice.mydomain.com" is entered in the Unity SMTP Mail Suffix field, voice messages will be addressed to: IMCEAOMNI-AvVoiceMessage@voice.mydomain.com If you did not enter an address in the ESMTP Server field on the Digital Networking page, the Unity SMTP Mail Suffix is used by the Bridge when it establishes a network connection to the SMTP server that it sends the messages to. This means that the name in the Unity SMTP Mail Suffix field must be resolvable to an IP address. Two common ways to accomplish name resolution are through Domain Name System (DNS), or by using a HOSTS file. As a best practice, use DNS or the HOST file rather than entering an address in the ESMTP Server field. As a first choice for name resolution, we recommend that you add a host address resource (A) record and a mail exchange (MX) record in DNS by using the name in the Unity SMTP Mail Suffix field and the IP address of the server that handles incoming SMTP messages. If using DNS is not an option, then add an entry to the HOSTS file on the Bridge server with the name in the Unity SMTP Mail Suffix field and the IP address of the server that handles incoming SMTP messages.
Codec	Select the codec used to encode all voice messages sent from the Bridge to the Unity node. Note that this setting is independent of the format of the voice messages that the Bridge receives from the Unity node. The default setting is G.711. Voice messages sent from Cisco Unity to the Bridge can be recorded in the G.711 or the G.729a wave format. Therefore, you can configure each Cisco Unity server as needed to record voice messages by using either the default G.711 codec or the G.729a codec.
Save Button	Click Save to save the configuration settings.
Delete Button	Click Delete to delete this node. Note that deleting the node here only deletes the node information from the Bridge.
Directory Button	Click Directory to view the directory entries for this node. The Directory List page appears and displays the list of names associated with the node. This list is propagated from the Unity node to the Bridge server. To exit the Directory List and return to the Unity Node Configuration page, from the Configuration menu, click the node name. Unity node directory entries can be viewed but not edited on the Bridge.

Octel Nodes

The Octel Nodes page in the Bridge Administrator displays a list of Octel nodes that are currently defined. You should create and configure an Octel node to correspond to each Octel server in your network that you want Cisco Unity to communicate with. Additionally, in the Cisco Unity Administrator, you need to create a delivery location that corresponds to the Octel node that you create here.

The following buttons are on the Octel Nodes page:

- Add Button—Click Add to create a new node.
- Edit Button—Select the node from the Node list, and click Edit to modify an existing node.
- Delete Button—Select the node from the Node list, and click Delete to delete an existing node from the list.

Octel Node Configuration

After clicking Add or Edit from the Octel Nodes page, the Octel Node Configuration page in the Bridge Administrator is displayed. On this page, you enter information about the Octel node and the schedule for delivering messages to this node. Additionally, you can add or view directory entries that are associated with this node.

Use the following table to learn more about the Octel Node Configuration page.

Table 8-4 Octel Node Configuration Settings

Field	Considerations
Serial Number	Enter the unique serial number of the Octel node. Note that after the configuration settings are saved, you cannot change the serial number when editing the node. To change the Serial Number, you have to delete the node, and add it again with the correct Serial Number. The Serial Number must match the number that is displayed in the Cisco Unity Administrator in the Octel Node ID field on the Delivery Locations page that corresponds to this Octel Node. Additionally, the Serial Number must match the number of an Octel node.
Name	Enter a descriptive name for the remote node. You can enter up to 20 characters.
Phone Number	Enter the phone number that the server dials to send messages to the remote node. If the phone number of the remote node is in a different area code, include the area code. You can enter up to 14 digits. Note that the number dialed to reach the server consists of the Phone Number, Extension, and the Dial Sequence (see below). If a number longer than 14 digits is needed, the digits can be added to the Extension field or to the Dial Sequence.
Extension	Enter the extension number if it must be dialed to reach the remote node. You can enter up to 7 digits.

Table 8-4 Octel Node Configuration Settings

Field	Considerations
Dial Sequence	Enter the dial sequence that is required to call the remote node. At a minimum, the dial sequence should be set to "N" (phone number). You can enter up to 20 characters. The dial sequence can contain the following characters: • digits 0 to 9 • * and # (to correspond to the * and # keys on the phone) • P (for pause) • N (to insert the phone number) • X (to insert the extension number) For example, enter 9NPPPX.
Save Button	To save this node, modify the appropriate values and click Save.
Delete Button	Click Delete to delete this node.
Directory Button	Click Directory to view the directory for this node. The Directory List page appears and displays the list of names associated with the node. To add a name to the directory of this node, from the Directory List page, click Add. Enter the mailbox number and the name, and click Save. To exit the Directory List, from the Configuration menu, click the node name.

Message Delivery Windows

For each node on the network, you define schedules for delivering messages. The Cisco Unity Bridge server follows these schedules when placing calls to the Octel node to transmit messages addressed to mailboxes on that node. When defining schedules, consider the immediacy with which you want messages to be delivered. You may want to configure the Administration delivery window for late at night to save on toll charges.

By default, a message delivery window is defined for each message type. You can disable one or two message delivery windows, but you must leave at least one window enabled for message delivery to take place. You must enable an Administration window if you want to propagate names from the Octel node through the Bridge to your Cisco Unity servers.

The message type allows separate time windows and delivery intervals to be configured for different types of messages. By default, the three message types are enabled and configured with different intervals. Check the check box next to the message type that you want to enable and define the Begin, End, and Interval times to suit the schedule that you want the Bridge server to follow.

- Normal—Non-urgent messages from subscribers. Note that when Normal is the only type checked, Urgent and Administration messages are still delivered, but according to the Normal schedule.
- Urgent—Urgent messages from subscribers. Note that when Urgent is the only type checked, Administration messages are still delivered, but according to the Urgent schedule.
- Administration—Administrative messages only.

Use the following table to learn more about the Message Delivery Windows page.

Table 8-5 Octel Node Configuration—Message Delivery Windows Settings

Field	Considerations
Enabled	Check the check box next to the message type that you want to enable. Uncheck the check box(es) for the type(s) that you do not want to use.
Begin	Enter the time of day, in the format hh:mmAM or hh:mmPM, that you want to begin sending messages to the remote node. The time can be entered in 12-hour or 24-hour format.
End	Enter the time of day, in the format hh:mmAM or hh:mmPM, that you want to stop sending messages to the remote node. The time can be entered in 12-hour or 24-hour format.
Interval	Enter a number from 1 to 240 for the interval in minutes that the server waits before calling a node again. After a call to a node fails, the server attempts the call again after waiting the specified number of minutes.

Directory List

The Directory List in the Bridge Administrator allows the administrator to view the directory of names associated with the node. For Unity nodes, the entries can only be viewed, because mailbox propagation keeps the list maintained. In the case of Octel nodes, the administrator can add, view, or delete directory entries. Directory entries that are added by the administrator on the Bridge server are permanent. Permanent entries are not aged and must be manually deleted by the administrator.

The following are buttons on the Directory List page:

- Add Button—Click Add to add a directory entry.
- Delete Button—Click Delete to delete a directory entry.
- View Button—Click View to view a directory entry.

Adding a Name to an Octel Node Directory

You can add permanent subscriber names to an Octel node directory.

To Add a Name to an Octel Node Directory

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

Step 2 Select the Octel node you want to change, and click **Edit**.

Step 3 On the Octel Node page, click **Directory**.

Step 4 On the Directory List page, click **Add**.

Step 5 On the Directory Entry page, enter the subscriber mailbox number in the Mailbox Number box.

Step 6 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 7 Click **Save**.

The Bridge server makes an administrative call to the Octel node to obtain the recorded voice name and other user information.

Viewing a Name in an Octel Node Directory

You can view permanent subscriber names in an Octel node directory.

To View a Name in an Octel Node Directory

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

Step 2 Select the Octel node from the list, and click **Edit**.

Step 3 On the Octel Node page, click **Directory**.

Step 4 On the Directory List page, select a mailbox number from the Directory.

Step 5 Click **View**.

On the Directory Entry page, the subscriber mailbox number and name are visible. The Entry Type line indicates Permanent (created manually on the Bridge) or Usage-based (created by NameNet).

Step 6 To return to the Directory List page, from the Configuration menu, click **Node Directory**.

Deleting a Name in an Octel Node Directory

You should delete a subscriber name in an Octel node directory if the name is no longer being used.

To Delete a Name in an Octel Node Directory

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

Step 2 Select the Octel node from the list, and click **Edit**.

Step 3 On the Octel Node page, click **Directory**.

Step 4 On the Directory List page, select a mailbox number from the Directory.

Step 5 Click **Delete**.

A message displays the warning, “All details associated with this entry will be lost.”

Step 6 Click **OK** to confirm the deletion.

The Bridge will send Cisco Unity a “Delete User” request to delete the Bridge subscriber from Cisco Unity and to delete the associated Domino Person document.

Directory Entry

The Directory Entry page in the Bridge Administrator displays the subscriber mailbox number and name. For an Octel node directory entry that you add, the Entry Type line indicates Permanent.

To return to the Directory List page, click Node Directory from the Configuration menu.

Use the following table to learn more about the Directory Entry page.

Table 8-6 Directory Entry Settings

Field	Considerations
Mailbox Number	Displays the subscriber mailbox number.
Name	Displays the subscriber name.
Entry Type	Indicates whether the entry you view is Permanent or Usage-based. The Entry Type parameter displays when you view a current entry. Entries created by using this page are always Permanent.
Save Button	Click Save to save the new entry that you added. The Save button displays when you add a new entry to the directory.
Delete Button	Click Delete to delete the entry that you are viewing. The Delete button displays when you view an existing entry from the directory.

Line Status

The Line Status page in the Bridge Administrator allows you to monitor status information for the phone lines of the Cisco Unity Bridge server as it communicates with Octel servers. It also allows you to enable or disable specific phone lines on the Bridge server, and to specify whether each line is to be used for both incoming and outgoing calls or only for incoming calls. The Line Status page may be helpful when troubleshooting message flow between the Bridge server and Octel servers.

Use the following table to learn more about the Line Status page.

Table 8-7 Line Status Information

Field	Considerations
Line	Indicates the phone line for which status information is displayed.

Table 8-7 Line Status Information (continued)

Field	Considerations
Status	Indicates the status of a phone line, as follows: • Admin Receive—Receiving an administrative call to send names. • Admin Send—Placing an administrative call to retrieve names. • Calling—Beginning a network callout. • Disabled—Not initialized. • Down—Not yet ready. • Idle—On hook and available for a call. • Incoming Call—Beginning to receive an incoming call. • Receiving—Receiving messages. • Receiving Fax—Receiving fax data. • Receiving Voice—Receiving voice data. • Retired—The line is retired. Whenever a problem occurs that prevents the Bridge from initiating an outgoing analog call on a particular analog port—for example, line cord not plugged in or no dial tone from the phone system—if the same problem happens on the same line four times in succession, the Bridge will retire the line. • Sending—Sending messages. • Sending Fax—Sending fax data. • Sending Voice—Sending voice data. • Unknown—Unable to process a call because of an unknown condition.
Serial Number	Displays the Octel node with which the Bridge server communicates and the Unity node that is the source or destination of the message. An arrow points left (<--) or right (-->) between the two serial numbers to indicate the direction of message delivery. The serial numbers may or may not display, depending on the line status. When “Bridge” is displayed in the serial number field, this indicates that an administrative call is in progress.
Info	Indicates additional information about a phone line, depending on the line status.
Line Type	Displays whether the phone line is used for both outgoing and incoming calls (Action field set to All Calls) or only incoming calls (Action field set to Incoming Only).

Table 8-7 Line Status Information (continued)

Field	Considerations
Action	The Action box allows you to refresh the information on the Line Status page immediately or at preset intervals, and to enable or disable a specific phone line, as follows: • All Calls—Specifies that the phone line is to be used for both outgoing and incoming calls. In the blank box, enter the line number of the phone line that you want to change, and click Submit. The new line status will take effect immediately. This is the default setting for all phone lines. • Disable Line—Disables a specific phone line. In the blank box, enter the line number of the phone line that you want to disable, and click Submit. The Unity Bridge service must be stopped and restarted for Disable Line to take effect. • Enable Line—Enables a specific phone line. In the blank box, enter the line number of the phone line that you want to enable, and click Submit. The Unity Bridge service must be stopped and restarted for Enable Line to take effect. • Incoming Only—Specifies that the phone line is to be used for incoming calls only. In the blank box, enter the line number of the phone line that you want to change, and click Submit. The new line status will take effect immediately. • Refresh Interval—Sets the refresh interval and initiates automatic updates according to that interval. In the blank box, enter a number from 5 to 120 for the interval in seconds, and click Submit. Selecting another page from the Configuration menu automatically clears the Refresh Interval for the Line Status page. When you return to the Line Status page, the Refresh Interval action is stopped. • Refresh Now—Refreshes the information on the Line Status page immediately. Depending on which action you select, you can enter a line number or a time interval (in seconds) in the blank box next to the Action box.
Submit	Click Submit to process the action you select.

Queue Status

The Queue Status page in the Bridge Administrator allows you to monitor status information in the outbound message queue on the Cisco Unity Bridge server. The Queue Status page may be helpful when troubleshooting message flow between the Bridge server and Octel servers.

Use the following table to learn more about the Queue Status page.

Table 8-8 Queue Status Information

Field	Considerations
Serial Number	Lists the serial number of the Octel node for which status information is displayed.
Name	Lists the name of the Octel node for which status information is displayed.
Messages in Queue	Displays the number of normal and urgent messages that are in the queue for each Octel node.
Lines In Use	Displays the number of analog lines currently in use for sending messages to each Octel node.

Table 8-8 Queue Status Information (continued)

Field	Considerations
Action	The Action box allows you to refresh the information on the Queue Status page immediately or at preset intervals, as follows: • Refresh Interval—Sets the refresh interval and initiates automatic updates according to that interval. In the blank box, enter a number from 5 to 120 for the interval in seconds, and click Submit. Selecting another page from the Configuration menu automatically clears the Refresh Interval for the Queue Status page. When you return to the Queue Status page, the Refresh Interval action is stopped. • Refresh Now—Refreshes the information on the Queue Status page immediately. You can enter a time interval (in seconds) in the blank box next to the Action box.
Submit	Click Submit to process the action you select.

Primary Location Settings

Overview: Primary Location Settings

Each Cisco Unity server has a primary location, which is created during installation and which cannot be deleted. The primary location identifies the Cisco Unity server and contains the networking information needed to communicate with other locations, which can be Cisco Unity servers or other voice messaging systems. With the exception of public distribution lists, all subscribers and other Cisco Unity objects (such as call handlers) created on your Cisco Unity server are associated directly or indirectly with the primary location.

No matter which networking option Cisco Unity uses to send and receive voice messages, you need to customize the primary location of your Cisco Unity server.

See the following sections in this chapter for more information about the settings for the primary location:

- Primary Location Profile Settings, page 9-1—This section provides information about the settings that identify the Cisco Unity server to other Cisco Unity servers or to other voice messaging systems, and provides guidelines for assigning location Dial IDs.
- Primary Location Addressing Option Settings, page 9-5—This section provides information about the settings that allow you to select the scope of the search performed when a subscriber uses the phone to address a message by name or extension.

Primary Location Profile Settings

The primary location profile settings contain the network information needed to identify the Cisco Unity server to other Cisco Unity servers or to other messaging systems.

Assigning Dial IDs

The primary location profile settings contain a Dial ID, which Cisco Unity uses as an identifier for the location. You need to carefully plan the numbers that you choose as Dial IDs—for both the primary location and for any delivery locations—particularly when your organization has multiple Cisco Unity servers networked together. Without careful planning, it is possible to assign Dial IDs that have the effect of preventing Cisco Unity from finding a message recipient at another location.

In installations with multiple Cisco Unity servers networked together, be sure to consult with the administrators of the other Cisco Unity servers about the numbers that you can use for the Dial IDs of the primary location and for any delivery locations that you create. You need to verify that the Dial IDs on the local Cisco Unity server do not conflict with the Dial IDs and extensions used on other Cisco Unity servers.

Guidelines for Assigning Dial IDs and Extensions

The numbering plan for assigning Dial IDs and extensions can affect how easily Cisco Unity matches the number that a subscriber enters when addressing a message. The following guidelines are recommended:

- Establish a fixed length for Dial IDs, and if possible, a fixed length for extensions.
- Assign unique Dial IDs. A Dial ID must not be the same as any other Dial ID or any extension assigned to a subscriber, call handler, interview handler, or public distribution list. (Note that in installations with multiple Cisco Unity servers networked together, it is unfortunately possible to assign a non-unique Dial ID due to directory replication lag time.)
- Assign a numbering range for Dial IDs that extensions do not use. For example, you can assign Dial IDs with leading zeros—001, 002, and so on.
- If you use variable-length Dial IDs and extensions, the Dial IDs should be in a different numbering range than the range for extensions. For example, if there is a local extension 750123, do not assign a location the Dial ID of 750 if there is a possibility that this location will have the extension 123.
- If you use variable-length Dial IDs, the first digits of each ID should be unique with respect to other Dial IDs. For example, if you have a location with an ID of 750, do not assign another location the ID of 7503. In this example, during a blind addressing search, Cisco Unity would always match the blind address entered by the subscriber to location 750 and fail to find location 7503.

If you do not follow these guidelines, subscribers may encounter the following problems when addressing a message:

- A delay while Cisco Unity searches for a match
- Multiple matches for the number
- Failure to find the recipient at another location

Changing the Minimum Length of Primary Location Dial IDs

If necessary to accommodate the numbering plan for your organization, the minimum length for primary location Dial IDs can be reduced to one or two digits by changing a registry key, as described in the following "To Change the Minimum Length of a Location Dial ID" procedure. Note, however, that one- and two-digit Dial IDs may conflict with private distribution list IDs during an address search. When a subscriber addresses a message by entering a one- or two-digit number, Cisco Unity first searches for a matching private distribution list. If a match is found, the search stops. Therefore, when a subscriber addresses a message by entering a location Dial ID in order to narrow down the search scope to a particular location, if the number entered matches a private distribution list ID, the conversation offers only the private distribution list as a destination. If subscribers do not address messages to other locations by first entering a Dial ID, there is no conflict, and the minimum length for Dial IDs can be reduced to accommodate complex numbering plans.

Note For Cisco Unity failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated.

To Change the Minimum Length of a Location Dial ID

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 **Administration – Set the Minimum Extension Length for Locations**.

Step 4 In the New Value box, enter the number, and click **Set**.

Step 5 When prompted, click **OK**. You do not need to restart the Cisco Unity server to enable the registry change.

Step 6 Click **Exit**.

Use the following table to learn more about the primary location profile settings.

Table 9-1 Network > Primary Locations > Profile Page

Field	Considerations
Display Name	This displays the name of the primary location. To change the name, enter a new name here, and then click the Save icon.
Dial ID	Enter the ID that identifies the primary location. Enter numbers only, up to a maximum of 10 digits. The default minimum length is 3 digits. Although the minimum length for Dial IDs can be reduced by using the Advanced Settings Tool, one- and two-digit Dial IDs may conflict with private distribution list IDs during an address search. When a subscriber addresses a message by entering a one- or two-digit number, Cisco Unity first searches for a matching private distribution list. If a match is found, the search stops. Therefore, when a subscriber addresses a message by entering a location Dial ID to narrow down the search scope to a particular location, if the number entered matches a private distribution list ID, the conversation offers only the private distribution list as a destination. If subscribers do not address messages to other locations by first entering a Dial ID, there is no conflict and the minimum length for Dial IDs can be reduced to accommodate complex dial plans. The following policies are recommended: • Establish a fixed length for Dial IDs and if possible, a fixed length for extensions. • Assign unique Dial IDs. • If you use variable-length Dial IDs and extensions, the Dial IDs should be in a different numbering range than extensions. • If you use variable-length Dial IDs, the first digits of each ID should be unique with respect to other Dial IDs. (For example, do not create Dial IDs like 432 and 4325.) • Even if the Dial ID will never be used by subscribers when they address messages, enter a number that does not conflict with extensions, such as 001 or 002.

Table 9-1 Network > Primary Locations > Profile Page (continued)

Field	Considerations
Recorded Name	Record a name for the primary location. The recorded name for the location is played in the subscriber conversation in a number of places, including when: • Subscribers associated with a Cisco Unity server in a different dialing domain address a message to subscribers associated with this location. (For example, assuming that New York is the recorded name for this location: "There are two matches. For John Smith, at New York, press 1. For Mary Smith press 2.") • Subscribers associated with a Cisco Unity server in a different dialing domain listen to messages from subscribers associated with this location. (For example: "Message 1, a voice message, from John Smith at New York....") • The setting Include Locations in Searches on the Network > Primary Location > Addressing Options page is enabled on another primary location. When subscribers at the other location address a message, the recorded name for this primary location may be played in the message addressing search results along with subscriber names. (For example: "There are two matches. For Chris Newton, press 1. For New York, press 2.") To record the name here, use the Media Master control bar. (Note that the Media Master is not available across a firewall that blocks DCOM communications.) Use the Options menu in the Media Master control bar to set recording and playback devices, if applicable, and to use other sound files.

Table 9-1 Network > Primary Locations > Profile Page (continued)

Field	Considerations
Dialing Domain	Select from the list or enter the name of the dialing domain of which this location is a member. The list contains dialing domain names already configured on at least one other Cisco Unity server in the network that have replicated to the local server. Add the Cisco Unity server to a dialing domain when it is integrated with the same phone system or phone system network as other Cisco Unity servers that access the same directory. 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. A dialing domain provides a means to set the search scope for message addressing and for call transfers from the auto attendant and directory handler(s). You must add the Cisco Unity server to a dialing domain before you enable the following features: • Cross-server log in. • Cross-server transfers from the auto attendant and directory handler(s) • Live reply (“call the sender”) to another Cisco Unity subscriber on another networked Cisco Unity server. • Live reply to a user on another voice messaging system who has a corresponding AMIS, Bridge, or VPIM subscriber account on another networked Cisco Unity server. • Identified subscriber messaging for Cisco Unity subscribers on different networked Cisco Unity servers. • Identified subscriber messaging for AMIS, Bridge, and VPIM subscribers, even when your installation consists of only one Cisco Unity server. The default setting is None. Use the default when: • Your installation consists of only one Cisco Unity server, and the server is not configured for AMIS, Bridge, or VPIM Networking. • Your installation consists of two or more Cisco Unity servers, but each server is integrated with a separate phone system. There is no limit to the number of Cisco Unity servers that can be assigned to a single dialing domain, and there is no limit to the number of dialing domains. However, a Cisco Unity server can be a member of only one dialing domain.

Primary Location Addressing Option Settings

The primary location addressing options allow you to control the scope of the search that Cisco Unity performs when searching for a matching extension in the following cases:

- When a subscriber addresses a message by using the phone.
- When subscribers add members to private lists by using the phone or the Cisco Unity Assistant.
- When an administrator adds members to private distribution lists by using the Cisco Unity Administrator.

- When Cisco Unity looks up the recipient for an incoming AMIS message. Note that the search scope for incoming Bridge and VPIM messages is always global and is not controlled by the addressing settings.

You can set the scope to the local Cisco Unity server, to the dialing domain that the local Cisco Unity server is a member of, or to the entire global directory.

The addressing options also allow you to enable blind addressing searches for a matching delivery location Dial ID. You can set the blind addressing scope to those delivery locations created on the local Cisco Unity server, to delivery locations within the dialing domain, or to the entire directory.

Subscriber Addressing Options

Depending on how Cisco Unity is set up, subscribers can address messages to other subscribers by spelling the recipient name or entering a number. If desired, you can disable addressing by spelled name for all subscribers on each Cisco Unity server by unchecking the Enable Spelled Name Search in the Cisco Unity Administrator on the System > Configuration > Settings page.

If addressing by spelled name is enabled, subscribers spell the name or part of the name of the recipient by using the letters on the phone keypad. The Address Messages To Other Subscribers field in the Cisco Unity Administrator on the Subscribers > Subscriber Template > Conversation page, and on the Subscribers > Subscribers > Conversation page, allows you to set the default method of addressing. Subscribers can also set this option in the Cisco Unity Assistant. While addressing messages, subscribers can switch between spelling the name and entering a number by pressing # twice (##).

How Cisco Unity Searches for a Matching Name

When a subscriber addresses a message by spelling the recipient name, Cisco Unity searches for a match or partial matches among subscribers and public distribution lists. Only one search at the specified maximum scope level is performed. The scope of the search is dictated by the Subscriber Searches: Limit Searches To setting. For example, if searches are limited to the dialing domain, one search that includes both the local server and dialing domain is performed, and a list of matching names is reported back to the subscriber.

Public distribution lists, whether created on the local Cisco Unity server or not, are always considered local in scope for addressing purposes. Thus, if the scope is set to Local Server, subscribers can still address to a public distribution list created on another Cisco Unity server.

If the Include Locations in Searches setting is enabled, then primary locations from networked Cisco Unity servers and delivery locations are included in the search. If the subscriber selects a location from the list of names returned from the search, the conversation prompts the subscriber to spell the name of the recipient at that location. This allows subscribers to limit a search for a recipient to a specific location.

How Cisco Unity Searches for a Matching Number

When subscribers address a message by entering a number, the number can be:

- The ID of a private distribution list.
- The extension of a Cisco Unity subscriber or an external subscriber. (The external subscriber can be an AMIS, Bridge, Internet, or VPIM subscriber.)
- The alternate extension of a Cisco Unity subscriber or an external subscriber.
- The extension of a public distribution list.

- A location dial ID.
- A primary location dial ID from a networked Cisco Unity server and an extension of a Cisco Unity subscriber at that location.
- A delivery location dial ID and the extension of an external subscriber associated with the delivery location.
- A Bridge delivery location prefix and the remote mailbox of the recipient.
- A Bridge delivery location dial ID and the remote mailbox number of the recipient.

For example, a subscriber presses 3335678 on the phone to address a message. Table 9-2 shows some of the possible matches:

Table 9-2 Some of the Possible Matches for the Number 3335678

Number	Possible Match
3335678	Extension 3335678
3335678	Location dial ID 333, extension 5678
3335678	Location dial ID 3335, extension 678
3335678	Bridge delivery location prefix 3, remote mailbox number 335678
3335678	Bridge delivery location prefix 33, remote mailbox number 35678
3335678	Remote mailbox length of 4: Bridge delivery location prefix 333, remote mailbox number 5678
3335678	Remote mailbox length of 5: Bridge delivery location prefix 333, remote mailbox number 35678
3335678	Bridge delivery location dial ID 333, remote mailbox number 5678

To accommodate a variety of numbering plans, Cisco Unity searches for a match in stages, as the following sections describe:

1. Search for a Distribution List or Subscriber Extension on the Local Server, page 9-7
2. Search for a Subscriber Extension in the Dialing Domain and Then the Global Directory, page 9-8
3. Search for a Location Dial ID and Subscriber Extension at the Matching Location, page 9-8
4. Blind Addressing Search for a Bridge Delivery Location Prefix, page 9-9
5. Blind Addressing Search for a Delivery Location Dial ID, page 9-10

Search for a Distribution List or Subscriber Extension on the Local Server

Cisco Unity searches for a matching number by expanding the search scope in stages, starting with the local server, then expanding to search the dialing domain, and finally searching the global directory. The scope of the search is dictated by the setting Subscriber Searches: Limit Searches To. If a match is found at any scope level, the search stops and does not continue to the next scope level.

If the subscriber enters a one- or two-digit number, the Cisco Unity begins the search by looking for a match among the private distribution lists owned by the subscriber. If a match is found, the search stops, and the matched list is returned for confirmation.

If a match has not been found, or if the subscriber entered three or more digits, Cisco Unity searches for a matching subscriber extension on the local server. The search includes extensions for regular Cisco Unity subscribers and external subscribers. Both primary extensions and alternate extensions are searched. If a match is found, the search stops.

When a match is found to a subscriber extension, the subscriber will hear a confirmation (the conversation will play the recorded voice name and extension of the matched subscriber) depending on whether the conversation is configured to do so, and whether the recorded voice name exists. You can customize how the conversation confirms subscriber message addressing matches by using the Advanced Settings tool in Tools Depot to change the setting for Subscriber Addressing Confirm Match Mode.

If a match has not been found, Cisco Unity searches for a matching public distribution list extension. Public distribution lists, whether created on the local Cisco Unity server or not, are always considered local in scope for addressing purposes. Thus, if the scope is set to Local Server, subscribers can still address to a distribution list created on another Cisco Unity server. If a match is found, the search stops, and the matched list is returned for confirmation.

Search for a Subscriber Extension in the Dialing Domain and Then the Global Directory

If a match has not been found on the local server, and if allowed by the search scope setting, the search expands to subscriber extensions in the dialing domain (if it exists). If a match is found, the search stops, and the name is returned for confirmation. If a match still has not been found, and if allowed by the scope setting, the search expands to subscriber extensions in the global directory. The search at each scope level includes extensions and alternate extensions for regular Cisco Unity subscribers and external subscribers.

It is possible for duplicate extensions to exist in the global directory. If the entered number matches more than one extension, a list of matching names is reported back to the subscriber from which to choose. However, if there is a match on an extension in the dialing domain, the search stops. For example, assume that Kelly has extension 3047 and is associated with a Cisco Unity server in the dialing domain. Joe also has extension 3047, but he is associated with another networked Cisco Unity server that is outside of the dialing domain. When a subscriber on the local server enters 3047 to address a message, the match is for Kelly, who is in the dialing domain. After finding a match at the dialing domain scope, the search stops and does not continue to the global directory; thus, the extension for Joe is not found. To address messages to Joe, Kelly would need to enter the primary location dial ID of the Cisco Unity that Joe is associated with followed by his extension.

Search for a Location Dial ID and Subscriber Extension at the Matching Location

If a matching distribution list, location dial ID, or subscriber extension has not been found, the search continues.

Cisco Unity parses the number to find a matching location dial ID and a subscriber extension at that location. Cisco Unity searches for a match by expanding the search scope in stages, starting with the local server, then the dialing domain, and finally the global directory. The scope of the search is dictated by the setting Subscriber Searches: Limit Searches To. If a match is found at any scope level, the search stops and does not continue to the next scope level. When a match is found, the conversation will confirm the match, if configured to do so.

Assuming that the minimum length for dial IDs is set to the default (three digits), at each scope level Cisco Unity first searches for a location dial ID that matches the first three digits entered by the subscriber. If a match is found, Cisco Unity searches subscribers associated with the location for an extension that matches the remaining digits in the entered number. Cisco Unity continues the search by looking for a location with a dial ID that matches the first four digits entered by the subscriber. If a match is found, Cisco Unity searches subscribers associated with the location for an extension that matches the remaining digits in the number. The search for a matching location and extension continues in this manner. Note that the search is for the primary extension of the subscriber; alternate extensions are not included in the search.

For example, a subscriber addresses a message to 3335678. Cisco Unity searches for a location with the dial ID 333. If a match is found, Cisco Unity searches for a subscriber at that location who has extension 5678. Next (regardless of whether a match was found), Cisco Unity searches for a location with the dial ID 3335. If a match is found, Cisco Unity searches for a subscriber at that location who has extension 678.

At the local scope level, only the delivery locations created on the local server are included in the search. At the dialing domain level, primary locations from other networked Cisco Unity servers and delivery locations are included in the search, if they are in the dialing domain. At the global directory level, all locations are included in the search.

If a delivery location is matched, Cisco Unity searches for an external subscriber associated with the delivery location who has an extension that matches the remaining numbers. Note that extensions are searched, and not the remote mailbox numbers.

If you have changed the minimum number of digits in location dial IDs, Cisco Unity first searches for a matching dial ID according to the minimum that you set. For example, if you reduced the minimum length of a dial ID to one, Cisco Unity begins the search at each scope level by looking for a matching dial ID that matches the first digit entered by the subscriber. (Reducing the minimum dial ID length to one or two is not recommended because of the potential conflict with private distribution list IDs.)

Blind Addressing Search for a Bridge Delivery Location Prefix

If a match has not been found, Cisco Unity will continue with a blind addressing search if the setting Blind Addressing: Allowed Locations is set to something other than the default (which is None). The search starts on the local Cisco Unity server, and then expands to the dialing domain, and then to the global directory, as applicable. If a match is found at any scope level, the search stops and does not continue to the next scope level.

At each scope level Cisco Unity first searches for a Bridge delivery location prefix that matches the first digit entered by the subscriber. If a match is found, Cisco Unity searches among the Bridge subscribers associated with the location for a matching remote mailbox number. To determine the mailbox number, Cisco Unity starts at the end of the entered number, and keeps including digits until the number of digits equals the remote mailbox length defined for the location. Note that the search is for a matching remote mailbox number and not an extension. Cisco Unity continues the search by looking for a Bridge delivery location with a prefix that matches the first two digits entered by the subscriber. If a match is found, Cisco Unity searches among the Bridge subscribers associated with the location for a matching remote mailbox number. The search for a matching Bridge delivery location prefix and remote mailbox number continues in this manner and stops when the number of the remaining digits is one.

Because this is a blind addressing search, if a matching Bridge delivery prefix is found, the matched location will be returned for confirmation even if a matching Bridge subscriber is not found. For example, assume that there is a Bridge delivery location with the following settings:

Dial ID = 100
Prefix = 256
Remote Mailbox Length = 5
Recorded Name = “Paris”

A subscriber logs on to Cisco Unity and addresses a message to 2564321, where 64321 is the mailbox number of an Octel subscriber on a remote Octel node with which Cisco Unity communicates. When the search reaches the stage of looking for a Bridge delivery location prefix, Cisco Unity first searches for a Bridge delivery location with a prefix of 2, then searches for the prefix 25, and then searches for the prefix 256. Because the subscriber entered a prefix, Cisco Unity uses the remote mailbox length to determine the remote mailbox number from the entered number: 25**63452**. In this example, the last digit in the prefix overlaps with the first digit of the mailbox number. Assume that the search does not find a Bridge subscriber with a remote mailbox of 64321. The matched delivery location is returned for

confirmation, and the conversation plays “For extension 64321 at Paris, press #.” If the sending subscriber confirms the match, Cisco Unity addresses the message and sends it on its way to the Octel subscriber.

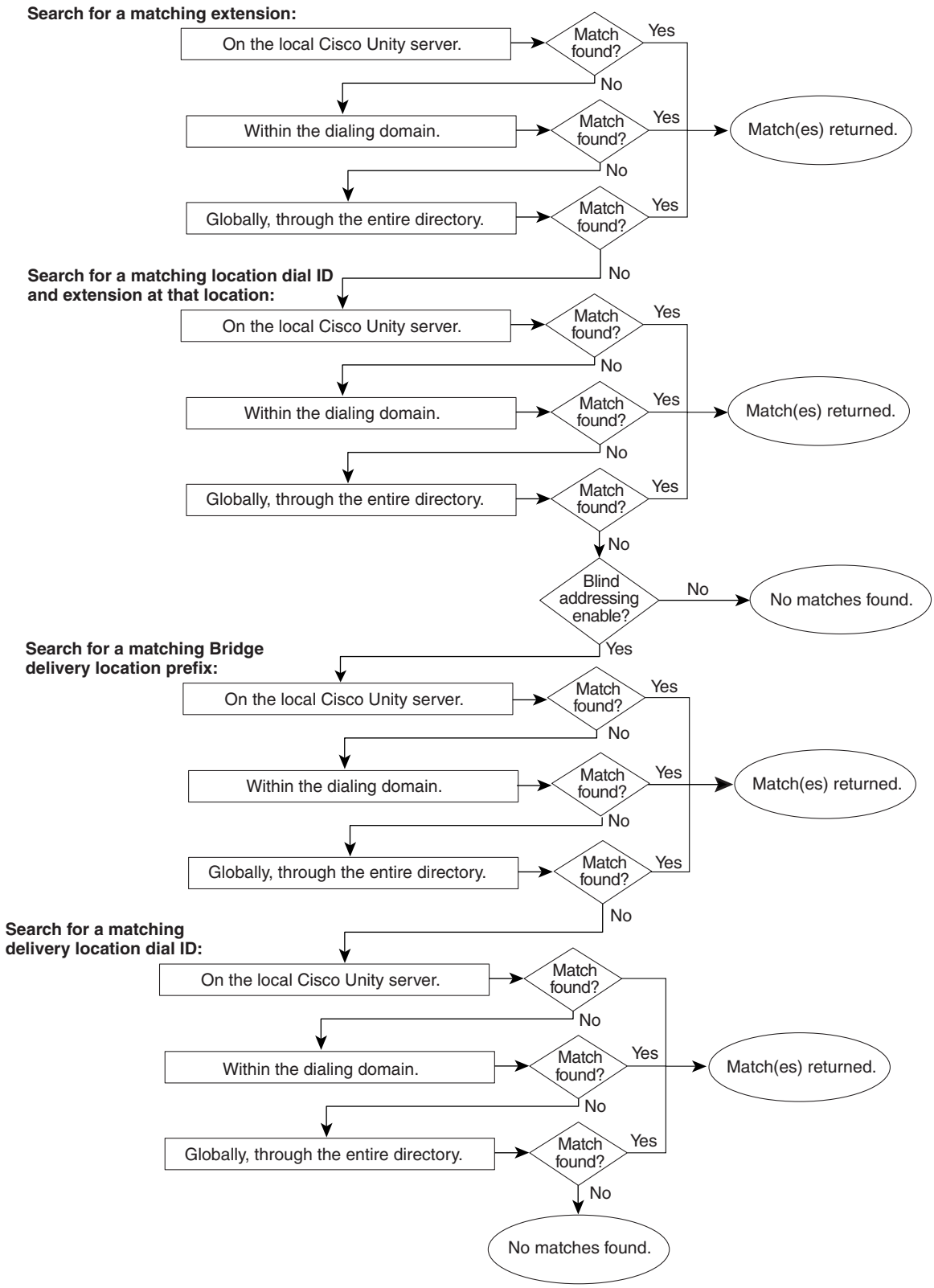
Blind Addressing Search for a Delivery Location Dial ID

If a match has not been found, Cisco Unity continues with the blind addressing search. The number is parsed to find a matching delivery location dial ID. The scope of the blind addressing search is determined by the setting Blind Addressing: Allowed Locations. The search starts on the local Cisco Unity server, and then expands to the dialing domain, and then to the global directory, as applicable.

Assuming that the minimum length for dial IDs is set to the default (three digits), at each scope level Cisco Unity first searches for a delivery location dial ID that matches the first three digits entered by the subscriber. Cisco Unity continues the search by looking for a delivery location with a dial ID that matches the first four digits entered by the subscriber. The search for a matching location continues in this manner. If the match is on a delivery location, the matched location is returned, along with the remaining digits entered as the mailbox for confirmation. If the match is on a Bridge delivery location, Cisco Unity searches among the Bridge subscribers associated with the location for a remote mailbox number that matches the remaining digits in the entered number. Note that because the match is on a location dial ID, the mailbox length is not used to construct the remote mailbox number; the remote mailbox number is presumed to be the remaining digits in the entered number. Because this is a blind addressing search, if a matching Bridge delivery dial ID is found, the matched location will be returned for confirmation.

Figure 9-1 illustrates the search that Cisco Unity performs when both the subscriber search and the blind addressing search (if enabled) are set to the global directory.

Figure 9-1 Subscriber Addressing Search for a Matching Number



Location Addressing Options Settings

When considering the address search scope settings for Cisco Unity servers in the network, keep in mind that Bridge Networking is based on a bridgehead topology. To ensure that Cisco Unity subscribers on any Cisco Unity server can address network messages to Octel subscribers, the address search scope on each server must encompass the bridgehead server because that is the server on which Bridge delivery locations and Bridge subscribers are created. Typically, you should set the address search scopes on all Cisco Unity servers to global scope. In circumstances where all Cisco Unity servers are configured to be in the same dialing domain, you can set the address search scope on all servers to the dialing domain, which in effect is the same as setting it to a global scope.

Use the following table to learn more about location addressing option settings.

Table 9-3 Network > Locations > Addressing Options Page

Field	Considerations
Subscriber Searches: Limit Searches To	Select the scope of the search that Cisco Unity performs when a subscriber addresses a message by using the phone, when members are being added to a public or private distribution list, and for incoming AMIS messages. • Local Server—Limits the search to subscribers created on the local Cisco Unity server. • Dialing Domain—If a match is not found while searching the local Cisco Unity server, the search expands to include subscribers created on other Cisco Unity servers that are in the same dialing domain as the local Cisco Unity server. • Global Directory—After searching the local Cisco Unity server and then the dialing domain (if there is one), the search expands to include every subscriber created on other Cisco Unity servers in the directory.

Table 9-3 Network > Locations > Addressing Options Page (continued)

Field	Considerations
Include Locations in Searches	Check this check box to have locations included in searches. This option is useful when the global directory is large and addressing a message by spelling the name results in many matches. For this setting to be helpful to subscribers, locations need to have recorded voice names. When checked, this setting allows subscribers to address a message in two steps. First subscribers select a particular location (by spelling the name or by entering the Dial ID). If Cisco Unity finds a matching location, the recorded voice name for the location is played (assuming one has been recorded). At this point, subscribers can spell the name of the recipient to limit the search to the specified location. Note that if the subscriber selected the location by entering the Dial ID, the subscriber needs to switch to spelling mode (by pressing # twice) to search for the subscriber. For example, assume there are two Cisco Unity servers configured for Digital Networking. Assume 100 is the Dial ID of the primary location for the Paris Cisco Unity server, and that a voice name ("the Paris sales office") for the location has been recorded. John, a subscriber on the local Cisco Unity server, wants to send a message to Kelly Bader at the Paris location, but he does not know the correct extension. • John logs on to Cisco Unity and presses 2 to send a message. • John enters 100# to select the Paris Cisco Unity server. • When the primary location 100 is found, the conversation plays, "For the Paris sales office, press #." • John presses # to confirm; the conversation plays, "Enter the extension followed by #." • John presses ##; the conversation plays, "Spell the name of a person or distribution list." • John enters 22337#. Cisco Unity searches for a matching subscriber name at location 100, and matches on Kelly Bader. The conversation plays, "For Kelly Bader at extension 3047, press #." • John presses # to confirm; the conversation plays, "Added. To add another name, press 1. To record the message, press #."
Blind Addressing: Allowed Locations	Select the scope of the blind addressing search for a matching delivery location that Cisco Unity performs when a subscriber addresses a message by using the phone. Select one of the following: • None—Do not allow blind addressing searches. • Local Server—Limits the search to delivery locations that were created on your Cisco Unity server. • Dialing Domain—If a match is not found while searching the local Cisco Unity server, the blind addressing search expands to include those delivery locations created on other Cisco Unity servers that are in the same dialing domain as the local Cisco Unity server. • Global Directory—After searching the local Cisco Unity server and then the dialing domain (if there is one), the search expands to include every delivery location created on other Cisco Unity servers in the global directory.

A

administrative calls Calls made by a node in an Octel analog network to populate its NameNet directory with the name, voice name, and extension of a subscriber on another node. Because the Cisco Unity Bridge can represent one or more nodes in the network, it places administrative calls to populate its NameNet directory. You can configure a schedule per Octel node on the Bridge server to control when it makes administrative calls to the node.

AMIS Audio Messaging Interchange Specification. An industry-standard protocol supported by Cisco Unity that provides an analog mechanism for transferring voice messages between different voice messaging systems.

AMIS Networking A Cisco Unity networking option. Allows messaging between Cisco Unity and other voice messaging systems that support the Audio Messaging Interchange Specification analog (AMIS-a) protocol. Cisco Unity and the other voice messaging systems maintain separate voice mail directories with no directory synchronization.

AMIS subscriber A representation in Cisco Unity of subscribers on an AMIS-compliant, remote messaging system. AMIS subscribers are created in Cisco Unity to enable Cisco Unity subscribers to find them in the directory and to send messages to them as they would to any other subscriber. AMIS subscribers are associated with a delivery location. They have corresponding Person documents that have "Other Internet Mail" set in the Mail System field, and they are listed in the Notes address book. Mailbox greetings and voice names can be individually recorded for each subscriber. Messages sent to an AMIS subscriber are sent via a Cisco Unity server that is designated as the AMIS bridgehead server to the applicable mailbox on the remote messaging system. AMIS subscribers do not have messages stored locally. Their messages are stored on the remote messaging system.

B

blind addressing One of the methods that Cisco Unity provides for addressing messages to remote messaging system users. Blind addressing allows addressing of messages without having the recipient mailbox number, text name, or recorded name in the directory.

Bridge Networking A Cisco Unity networking option. Allows messaging between Cisco Unity and Avaya Octel or Interchange systems on an Octel analog network by using the Cisco Unity Bridge. The Bridge, which acts as a networking gateway, must be installed on a separate and dedicated platform. Messaging between Cisco Unity and the Bridge is done by using SMTP over the Internet or any TCP/IP network. Messaging between the Octel servers and the Bridge is done by using the Octel analog networking protocol. Cisco Unity and the Octel systems maintain separate voice mail directories. However, the Bridge supports NameNet, which is an Octel Networking feature that allows for the propagation of text and voice names among nodes on the analog Octel network. NameNet allows subscribers to address messages to people at other nodes by spelling the recipient name, and to get voice name confirmation when addressing a message to someone on another node.

Bridge subscriber A representation in Cisco Unity of subscribers on an Avaya Octel messaging system. Bridge subscribers are created in Cisco Unity to enable Cisco Unity subscribers to find them in the directory and send messages as they would to any other subscriber. Bridge subscribers are associated with a delivery location. They have corresponding Person documents that have "Other Internet Mail" set in the Mail System field, and they are listed in the Notes address book. Mailbox greetings and voice names can be individually recorded for each Bridge subscriber. Messages sent to a Bridge subscriber are sent through the Cisco Unity Bridge server to the applicable mailbox on the Octel system. Bridge subscribers do not have messages stored locally. Their messages are stored on the Octel messaging system.

Bridge subscribers are automatically created when the Bridge creates usage-based directory entries for Octel users (in support of NameNet). You can also create Bridge subscribers manually in Cisco Unity or create permanent directory entries on the Bridge server, which results in the automatic creation of Bridge subscribers. Bridge subscribers that are automatically created are referred to "auto-created Bridge subscribers."

bridgehead server A Cisco Unity networking term. In installations with multiple Cisco Unity servers networked together, only one Cisco Unity server in the network needs to be configured for AMIS, Bridge, or VPIM networking— the server acts as the "bridgehead" server for the other Cisco Unity servers in the network.

D

delivery location A Cisco Unity object created on the local Cisco Unity server that corresponds to a remote voice messaging system. A delivery location contains the information that Cisco Unity needs for exchanging messages with the remote voice messaging system.

dialing domain A dialing domain is a collection of Cisco Unity servers that access the same directory and that are integrated with the same phone system or phone system network. (Note this includes Cisco Unity servers configured for dual integrations.) A dialing domain is a grouping scheme that allows Cisco Unity to handle call transfers from one Cisco Unity server to another. Within the dialing domain, subscriber extensions in Cisco Unity must be unique just as the phone extensions in the phone system must be unique. (Typically, a subscriber extension and phone extension are the same number.) With a networked phone system, subscribers dial a phone extension without having to dial a trunk access code or prefix when calling someone who is at another location in the phone network. In the same way, when grouped in a dialing domain, subscribers associated with one Cisco Unity server enter a subscriber extension when sending messages to subscribers associated with another Cisco Unity server.

Digital Networking A Cisco Unity networking option. Allows messaging among multiple Cisco Unity servers connected to a single, global directory. That is, the Domino servers used by the Cisco Unity servers are in the same Domino domain. Message routing is done by the Domino router. In Cisco Unity 4.0(5) and later, if the Domino servers are in different Domino domains, the Cisco Unity servers can be configured to monitor the same set of Domino address books.

directory The data store used by Cisco Unity, which contains information about subscribers, distribution lists, and locations. Cisco Unity stores data in the directory (typically, names.nsf) on the Domino server that was specified in the Message Store Configuration wizard during set-up.

Almost all of the information about subscriber accounts and other Cisco Unity objects is stored in a SQL database on the Cisco Unity server, rather than in the directory. However, a minimal amount of information about subscribers, distribution lists, and locations is also still stored in the directory, primarily to support Unified Messaging and networking.

directory messages Messages that contain directory information (name, voice name, and extension) about a subscriber. In Bridge Networking, directory messages are sent between the Cisco Unity bridgehead server and the Bridge. Additionally, the Bridge participates in NameNet, and therefore it makes administrative calls to, and receives calls from, Octel nodes on the Octel analog network to share directory information.

E

extension address Also referred to as a remote address. The destination address created by Cisco Unity when sending a message to a recipient on another voice messaging system or a remote Cisco Unity server. The extension address is in the format:
<Type>:<DeliveryLocationDialID>_<RemoteMailboxNumber>@<ForeignDomain>
where type can be AMIS, OMNI, or VPIM. The Interop Gateway parses the extension address to determine the routing path for the message.

external subscriber A Cisco Unity term for AMIS, Bridge, and VPIM subscribers, who do not retrieve their voice messages on the local Domino network. Instead, messages for the external subscribers are sent to a remote voice messaging system.

H

home Cisco Unity server When Cisco Unity servers are networked via Digital Networking, the home Cisco Unity server is the Cisco Unity server on which a subscriber account was created.

I

identified subscriber messaging (ISM) ISM affects what subscribers hear when they call other subscribers from their primary or alternate extensions and are forwarded to the greetings of the subscribers they call. If they then leave a message, ISM affects what the called subscriber hears and can do when listening to the message. When ISM is enabled, Cisco Unity recognizes that the calling extension is associated with a subscriber and accordingly plays the internal greeting of the called subscriber. Additionally, when the called subscriber later listens to the message, Cisco Unity plays the recorded voice name of the subscriber who left the message and allows the called subscriber to record a reply.

Internet subscriber Internet subscribers are Cisco Unity subscribers who do not have mailboxes on the local Domino network. Instead, messages for Internet subscribers are sent to an e-mail address that you specify when you create the Internet subscriber account. Internet subscribers are created in Cisco Unity to enable Cisco Unity subscribers to find them in the directory and send messages as they would to any other subscriber. Internet subscribers have corresponding Person documents in the Domino directory. Mailbox greetings and voice names can be individually recorded for each Internet subscriber. Messages sent to an Internet subscriber are sent via SMTP over the Internet or any TCP/IP network.

Interop Gateway The Interop Gateway for Domino is a Cisco Unity service that enables messaging between Cisco Unity and other voice messaging systems. When configuring AMIS, Bridge, or VPIM Networking, you run the Interop Gateway Configuration wizard and specify a Domino Foreign domain name (for example, “voicemail.domain.com”) and mail file that AMIS, Bridge, and VPIM messages will be routed through. The Interop Gateway monitors the Foreign domain mail file for messages, and re-addresses and reformats the messages as needed.

IP Internet Protocol. Network layer for the TCP/IP protocol suite. Internet Protocol (version 4) is a connection-less, best effort packet switching protocol.

L

location A Cisco Unity object that contains the addressing information that Cisco Unity needs to exchange messages with other voice messaging systems (which may or may not be Cisco Unity systems). See also delivery location and primary location.

M

MIME Multipurpose Internet Mail Extensions. An industry-standard specification for formatting non-ASCII messages so that they can be sent over the Internet. Many e-mail clients now support MIME, which enables them to send and receive graphics, audio, and video files via the Internet mail system. In addition, MIME supports messages in character sets other than ASCII.

N

NameNet An Avaya Octel networking feature supported by Bridge Networking that allows for the propagation of text and voice names among nodes on the analog Octel network. NameNet allows subscribers to address messages to people at other nodes by spelling the recipient name, and to get voice name confirmation when addressing a message to someone on another node.

network address An Avaya Octel networking term for the numeric address that an Octel subscriber enters as the message destination when addressing a message to an Octel subscriber on a network node. The network address consists of a node prefix that identifies the remote server to which the message is addressed, and additional digits that identify the recipient mailbox on the remote server.

networked subscriber A subscriber who is associated with a Cisco Unity server that is Digitally Networked with the local Cisco Unity server.

networking In Cisco Unity, “networking” is the general term for messaging between Cisco Unity servers, and between Cisco Unity and other voice messaging systems.The term networking has a broad definition and encompasses the following ideas:

Subscribers associated with one Cisco Unity server can use the phone to send voice messages to:

- Subscribers associated with another Cisco Unity server.
- Individuals with access to a computer connected to the Internet.
- Individuals who use a voice messaging system other than Cisco Unity.

Unidentified callers can find any subscriber in the directory and leave a voice message. Depending on the phone system and network configuration, unidentified callers who reach the Cisco Unity automated attendant or directory assistance can be transferred to any subscriber phone, even to the phone of a subscriber who is not associated with the local server.

Cisco Unity offers the following networking options: Digital Networking, AMIS Networking, Bridge Networking, and VPIM Networking.

node In Octel analog networking, a node is a voice messaging server on the network that is identified by a serial number. A Cisco Unity Bridge server can be configured to represent one or more nodes in the Octel network.

In AMIS Networking, Cisco Unity and the other voice messaging systems that it communicates with are called nodes. Each node is assigned a unique ID, referred to as a Node ID.

numbering plan In Cisco Unity, the method of assigning primary and alternate extension numbers. Typically, the Cisco Unity primary extension for a subscriber is the same as the subscriber extension on the phone system—the Cisco Unity numbering plan is usually the same as the phone system dial plan. In this way, when subscribers call Cisco Unity, log on as a subscriber, and send a message to a subscriber, the number that they enter when addressing the message is the same as when they call the subscriber directly.

P

pilot number The phone number used to access a Cisco Unity server. For example, subscribers dial a pilot number when logging on to Cisco Unity. The phone system that Cisco Unity is integrated with dials a pilot number when transferring callers to a greeting. Other voice messaging systems dial a pilot number when sending messages to Cisco Unity via AMIS.

primary location Each Cisco Unity server is associated with one location, referred to as the default or primary location, which is created during installation and which cannot be deleted. With the exception of public distribution lists, all subscribers and other Cisco Unity objects (such as call handlers) created on your Cisco Unity server are associated with the primary location.

Each primary location contains the addressing information that Cisco Unity needs to route messages between Cisco Unity servers. Because Cisco Unity stores location and subscriber addressing information in the directory, the addressing information replicates to other Cisco Unity servers on the network.

R

remote address See extension address.

S

SMTP Simple Mail Transfer Protocol. An industry-standard Internet protocol providing e-mail services. It is a TCP/IP protocol that defines the message format and method for sending messages from one host to another. SMTP was originally designed only for ASCII text, but MIME and other encoding methods enable program and multimedia files to be attached to e-mail messages. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another.

T

TCP/IP Transmission Control Protocol/Internet Protocol. A communications protocol developed to network dissimilar systems. This is an Internet protocol that has become the global standard for communications. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent. Every client and server in a TCP/IP network requires an IP address that is either permanently assigned or dynamically assigned at startup.

U

UAmis account Outgoing AMIS messages are placed in a special Domino mail file named UAmis_<Server name>. The AMIS schedule and AMIS delivery options in the Cisco Unity Administrator allow you to control when outgoing AMIS messages will be sent.

UOmni account Administrative messages from the Bridge to create, modify, or delete Bridge subscribers are placed in a special Domino mail file named UOmni_<Servername>. The Bridge Connector (a Cisco Unity component that runs as a Windows 2000 service called CsBridgeConnector) monitors the UOmni mail file. When it receives a message, it parses the data and sends a request to the Cisco Unity database component to make the necessary change (creation, modification, or deletion) to the Bridge subscriber account.

V

vCard A standard format for an electronic business card that includes fields for the phone number, text name, and e-mail address of the message sender. Cisco Unity allows you to specify whether the voice name and vCard of the sender will be sent with outgoing messages to a VPIM-compliant voice mail system.

VPIM Voice Profile for Internet Mail. An industry-standard Internet messaging protocol to allow disparate voice messaging systems to exchange voice messages over the Internet or any TCP/IP network. VPIM is based on the SMTP and MIME protocols.

VPIM Networking A Cisco Unity networking option. Allows messaging between Cisco Unity and other voice messaging systems that support the Voice Profile for Internet Mail (VPIM) version 2 protocol. Messages are exchanged by using SMTP over the Internet or any TCP/IP network. Cisco Unity and the other voice messaging systems maintain separate voice mail directories.

VPIM subscriber VPIM subscribers are a representation in Cisco Unity of subscribers on a remote voice messaging system. VPIM subscribers are associated with a delivery location. They have corresponding Person documents that have “Other Internet Mail” set in the Mail System field, and they are listed in the Notes address book. Cisco Unity subscribers address messages to VPIM subscribers just like they do to regular subscribers, but the messages are sent via VPIM to the applicable mailbox on the remote voice messaging system. VPIM subscribers can be included in Cisco Unity public distribution lists, and outside callers can leave them messages (if they are listed in the Cisco Unity phone directory).

A

accounts, UOmni 1-12

adding

- Bridge subscribers, with Bulk Import wizard 2-32
- Bridge subscribers, with the Bridge Administrator 2-33
- Bridge subscribers, with the Cisco Unity Administrator 2-33
- Bridge subscribers, with the Cisco Unity Bridge Mailbox Import tool 2-34
- delivery locations with Bulk Import wizard 2-13

addressing

- Bridge subscribers 1-18
- message options 1-16
- messages, blind 1-17

automated attendant, setting search scope 2-37

B

backing up Bridge server 3-6

BANANA

- about 2-22
- getting started 3-4
- installing 2-23
- test calls 2-24

blind addressing 1-17

Bridge Administrator

- accessing 8-1
- adding password protection 2-18

bridgehead server 1-6

Bridge Mailbox Import tool 2-34

Bridge server

- backing up 3-6
- configuring 2-16
- directory list 8-14
- line status 8-16
- message delivery windows 8-13
- Octel nodes 8-12
- offline backup 3-7
- online backup 3-6
- queue status 8-18
- restoring 3-7
- system settings 8-1
- Unity nodes 8-9

Bridge settings

- delivery location prefix 7-4
- delivery location profile 7-1
- delivery location subscriber creation 7-5
- options 2-10
- subscriber creation options 7-6
- synchronization options 7-7

Bridge subscribers

- appearance in Notes address book 1-24
- automatic creation, modification, and deletion, disabling 1-23
- call transfer settings 1-27
- creating subscriber accounts 2-27
- creation options settings 7-6
- deleting 1-22
- directory entries 1-11
- identified subscriber messaging 2-36
- limitations 1-18
- live reply 1-22
- overview 1-18

Bridge subscribers, licenses 1-18

Bridge Traffic Analyzer 3-5

Brooktrout traces 5-1

Bulk Import wizard
creating locations 2-12
errors, correcting 2-32
modifying existing delivery locations 2-14
overview 2-30

C

callers, identifying 1-21
call transfer settings for Bridge subscribers 1-27
codecs, supported by the Bridge 1-26
ConfigMgr.exe, using to install and configure components 2-9
CSV files
correcting delivery location import errors 2-13
correcting import errors 2-32
creating delivery locations 2-12
preparing for import 2-30

D

deleting
Bridge subscribers 1-22
UOmni mail file 1-12
delivery locations
correcting import errors 2-13
creating 2-11
creating, final tasks 2-25
creating CSV files 2-12
creating via Cisco Unity Administrator 2-11
creating with Bulk Import wizard 2-13
mailbox length 1-8
modifying existing 2-14
prefix 1-8
designating the bridgehead server 2-9
dial IDs
assigning 9-1
changing minimum length 9-2
guidelines for assigning 9-2
directories, synchronizing 1-12, 4-42
directory entries, correspondence to Bridge subscribers 1-11
directory information sharing 1-10
directory lookups, Asian and European names 1-28
directory messages, troubleshooting 4-42
disaster recovery 3-7
distribution lists 1-28
DNS 2-6

E

extension addresses 1-20
extensions
Bridge subscribers 1-19
guidelines for assigning 9-2

F

failover and directory synchronization 1-13
Foreign domain
changing name 3-9
name 1-15

G

glossary A-1

H

HOSTS file 2-6

I

identified subscriber messaging
about 1-21
about extending to include Bridge subscribers 2-36
enabling 2-38
extending to include Bridge subscribers 2-38

inbound search scope 1-29
Interop Gateway
about 1-15
changing Foreign domain name 3-9
configuring 2-7
moving the mail file 3-11
verifying the configuration 2-8

L

licenses, Bridge subscribers 1-18
live reply, Bridge subscribers 1-22
locations
addressing options settings, reference 9-12
Bridge 1-8
Bridge delivery location profile settings 7-1
delivery, creating 2-11
delivery, creating, final tasks 2-25
primary, addressing options settings, about 9-5
primary, customizing 2-37
primary, profile settings 9-3
primary, profile settings, about 9-1
settings overview 9-1

M

mailbox ID, adding to subscriber accounts 2-14
mailbox length 1-8
mail file, UOmni 1-12
maintenance 3-1
Max Ports per Node setting 3-2
message delivery window settings, adjusting 2-23
messages
address format 1-17
addressing options 1-16
delayed 1-29
handling limitations 1-16
leaving versus sending 1-21
messaging protocols 1-4

N

NameNet emulation 1-10
name resolution 2-6
network settings
Bridge subscriber creation options 7-6
Bridge synchronization options 7-7
delivery locations profile 7-1
location addressing options settings, reference 9-12
primary location addressing options, about 9-5
primary location profile settings, about 9-1
primary location profile settings, reference 9-3
notable behavior 1-26

O

Octel analog network, testing 2-22
Octel nodes, representation in Cisco Unity 1-8
options settings
bridgehead server 2-10
Bridge subscriber creation 7-6
Bridge synchronization 7-7

P

password, Bridge Administrator 2-18
permissions required for identified subscriber messaging 2-38
Person documents and connection to Bridge subscribers 1-18
ports, controlling 3-1
prefixes 1-8
primary locations
addressing options settings, about 9-5
addressing options settings, reference 9-12
customizing 2-37
profile settings, about 9-1

profile settings, reference 9-3
settings overview 9-1
profile settings, Bridge delivery locations 7-1

Q

Queued Call Threshold setting 3-2

R

reference
settings on the Bridge server 8-1
settings on the Cisco Unity server 7-1
relay server 2-4
remote addresses 1-20
removing
Bridge Networking completely 6-1
Bridge software 6-5
resolving names and IP addresses 2-6
restoring Bridge server 3-7

S

search scopes
automated attendant, setting 2-37
how Cisco Unity searches for names 9-6
how Cisco Unity searches for numbers 9-6
inbound Bridge messages 1-29
serial number, adding to subscriber accounts 2-14
setup task list 2-2
subscribers
addressing options 9-6
appearance in Notes address book 1-24
automatic creation, modification, and deletion, disabling 1-23
Bridge 1-18
call transfer settings 1-27
creating accounts 2-27
creation options 2-10
creation options settings 7-6
deleting 1-22
directory entries 1-11
experience with Bridge subscribers 1-21
limitations 1-18
overview 1-18
synchronizing
Bridge subscribers with Octel node directories 4-45
Cisco Unity subscribers with Unity node directories 4-46
options 2-10

T

testing
Octel analog network 2-22
setup 2-24
troubleshooting
advanced 5-1
Brooktrout card 5-1
configuration problems 4-1
directory messages between Cisco Unity and the Bridge 4-42
directory synchronization tools 4-6
messages from Cisco Unity to Octel 4-7
messages from Octel to Cisco Unity 4-24
tools 4-4

U

uninstalling Bridge software 6-5
UOmni mail file 1-12
utilities
BANANA 2-23
ConfigMgr.exe 2-9

W

wizard, Bulk Import 2-30