Networking Guide for Cisco Unity (With Microsoft Exchange)

Release 5.x
September, 2007

Americas 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: 408 527-0883

Text Part Number: OL-13844-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Networking Guide for Cisco Unity Release 5.x (With Microsoft Exchange)
© 2007 Cisco Systems, Inc. All rights reserved.

C O N T E N T S

Preface

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

Purpose

The *Networking Guide for Cisco Unity* introduces you to the various networking options available in Cisco Unity, and explains how to set them up.

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

Audience

The *Networking Guide for Cisco Unity* is intended for system administrators and others responsible for setting up and managing Cisco Unity. If you are administering the Cisco Unity server, you need a working knowledge of Windows and of the message store (Domino or Exchange) in which voice messages are stored. If you are setting up Cisco Unity to communicate with other voice messaging systems, you need a working knowledge of those voice messaging systems.

Document Conventions

This guide uses the following conventions:

Table 1   Networking Guide for Cisco Unity Conventions

Convention	Descriptions
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.)

Table 1   Networking Guide for Cisco Unity Conventions (continued)

Convention	Descriptions
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter ping <IP address>.)
- (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 *Networking Guide for Cisco Unity* 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, see the *Documentation Guide for Cisco Unity*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmaps_list.html.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance, contact us by sending e-mail to export@cisco.com.

Networking in Cisco Unity

Overview: Networking in Cisco Unity

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 that 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 phone 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.

See the following sections:

- Networking Options, page 1-1
- Message Addressing Options, page 1-2
- Locations and External Subscribers, page 1-3

Networking Options

The main goal of networking in Cisco Unity is to deliver messages from a Cisco Unity server to a target, and to deliver messages from the target to Cisco Unity. The networking options available in Cisco Unity are defined according to a combination of the message transport mechanism and the target, as shown in Table 1-1.

Table 1-1   Networking Options

Networking Option	Description
Digital Networking	Allows messaging among multiple Cisco Unity servers connected to a single, global directory. That is, the Exchange partner servers must be in the same Active Directory forest. Message routing is done by Exchange.

Table 1-1   Networking Options (continued)

Networking Option	Description
Internet Subscribers	Allows messaging with individuals over the Internet or any TCP/IP network by using SMTP. The recipient receives the message as an e-mail with a WAV attachment. Internet subscribers can have local extensions, recorded voice names, and greetings, and be listed in the directory, but they do not have mailboxes in the local Exchange network. Messages are addressed to Internet subscribers as they are to regular subscribers, but the messages are sent to the e-mail address that you specify when creating the Internet subscriber account.
Trusted Internet Subscribers	Trusted Internet subscribers are Internet subscribers that are trusted with decrypted secure messages. Trusted Internet subscribers must be associated with a Trusted Internet Location. Secure messages to Trusted Internet subscribers are decrypted by the Cisco Unity Voice Connector for Microsoft Exchange before they are sent by the Exchange server. (Messages to regular Internet subscribers are sent directly by the Exchange server and cannot be decrypted and therefore cannot be played by the recipient.)
AMIS	Allows messaging with other voice messaging systems that support the Audio Messaging Interchange Specification analog (AMIS-a) protocol. In essence, the sending voice messaging system calls the receiving voice messaging system, there is an exchange of DTMF tones as defined by the protocol, the sending system plays the message, and the receiving system records it.
Bridge	Allows messaging between Cisco Unity and an Octel system on an Octel analog network by using the Cisco Unity Bridge. The Cisco Unity Bridge acts as a networking gateway between Cisco Unity and the Octel system, and allows the systems to exchange voice and fax messages. Messaging between Cisco Unity and the Bridge is done over the Internet or any TCP/IP network by using SMTP. Messaging between the Octel servers and the Bridge is done by using the Octel analog networking protocol. The Bridge must be installed on a separate and dedicated platform.
VPIM	Allows messaging with other voice messaging systems that support the Voice Profile for Internet Mail (VPIM) protocol. VPIM allows different voice messaging systems to exchange voice, text, and fax messages over the Internet or any TCP/IP network. VPIM is based on SMTP and the Multi-Purpose Internet Mail Extension (MIME) protocol. VPIM Networking can be used for messaging between Cisco Unity servers that access different directories, between Cisco Unity and Cisco Unity Express, and between Cisco Unity with Exchange and Cisco Unity with Domino systems.

Message Addressing Options

With AMIS, Bridge, and VPIM Networking, you can set up different addressing options, as follows:

- **Blind Addressing**—With blind addressing, Cisco Unity has the information it needs to send messages to the remote voice messaging system, even though the recipient mailbox number, text name, and recorded name are not in the directory.

- **"External" Subscribers**—You create AMIS, Bridge, and/or VPIM subscribers on the local Cisco Unity server to correspond to subscribers on the remote voice messaging system. These external subscribers (also referred to as "proxy users" or "remote subscribers") can have local extensions, recorded voice names, and greetings, and can be listed in the directory. However, they do not have mailboxes in the local Exchange network. Messages are addressed to an external subscriber as they are to a regular subscriber, but the messages are sent to the applicable mailbox on the remote voice messaging system. External subscribers have corresponding Active Directory contacts.

- **A Combination**—The various ways of sending and receiving messages, as detailed in Table 1-1, are not mutually exclusive. For example, if the Cisco Unity servers in your organization are set up to access a global directory (and thus can make use of the Digital Networking option), you can still add Internet subscriber accounts for contractors working at home. In addition, if you are migrating users from an existing voice messaging system to Cisco Unity in stages, you can add AMIS, Bridge, or VPIM connectivity to the mix. Figure 1-1 depicts a configuration that uses a mix of the various networking options.

Figure 1-1   Networking in Cisco Unity
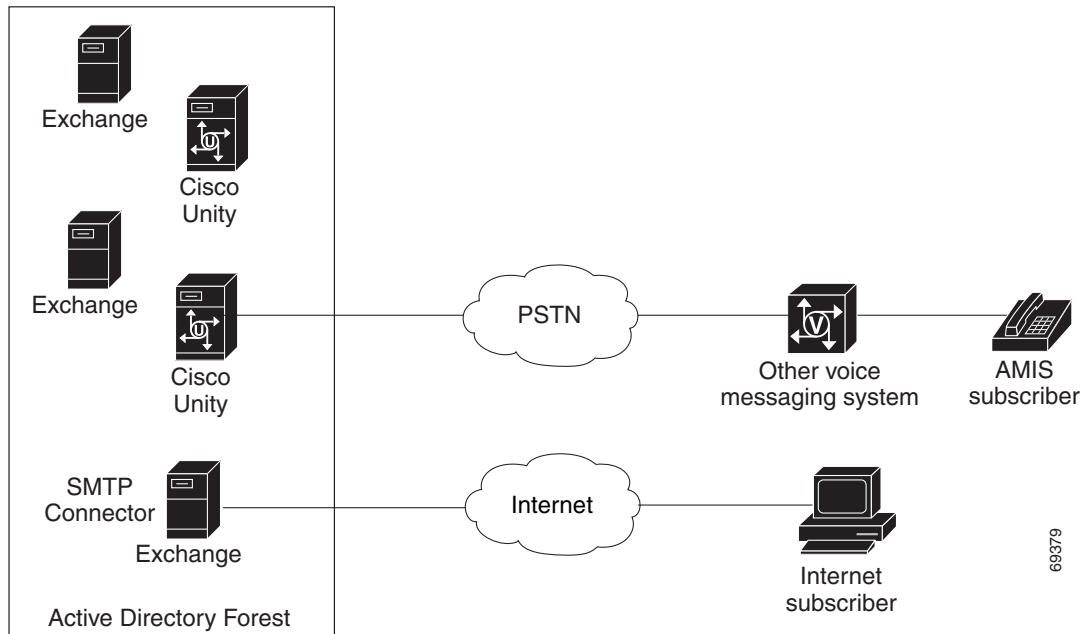
Locations and External Subscribers

Regardless of which networking option you choose, the setup process is similar.

For each networking option, you customize the settings for the primary location. Each Cisco Unity server has a default or primary location, which is created during installation and which cannot be deleted. The primary location contains information that identifies the Cisco Unity server to other messaging systems, which may or may not be Cisco Unity systems. See the "Overview: Primary Location Settings" section on page 9-1 for more information.

To set up AMIS, Bridge, or VPIM Networking, you create delivery locations. A delivery location contains the network information that Cisco Unity needs to send messages to other messaging servers, which may or may not be Cisco Unity servers. You create a delivery location for each voice messaging server with which the local Cisco Unity server will communicate.

Note   Trusted Internet Locations are a special type of delivery location. They do not contain information about other messaging servers, but rather serve as a delivery location for Trusted Internet subscribers that are trusted with decrypted secure messages. Based on the configuration settings of the Trusted Internet

Location, messages are decrypted by the Voice Connector before they are sent by Exchange over the Internet or any TCP/IP network via SMTP. (Messages to regular Internet subscribers are sent directly by the Exchange server and cannot be decrypted and therefore cannot be played by the recipient.)

Optionally, you can also create "external" subscribers (that is, AMIS, Bridge, and/or VPIM subscribers). The messages for external subscribers are stored externally to the Cisco Unity voice message store. When creating an external subscriber, you specify a delivery location that the external subscriber is associated with so that Cisco Unity has the information it needs to send messages to them.

Voice Connector

The Cisco Unity Voice Connector for Exchange is a Cisco Unity networking component that enables messaging between Cisco Unity servers and other voice messaging systems.

The Voice Connector for Exchange 2000 can be used when your network consists only of Exchange 2000 or Exchange 2003 servers, or a mixture of Exchange 2000, Exchange 2003, and Exchange 2007 servers.

> ⚠ **Caution**   The Voice Connector for Exchange 2000 can be installed on an Exchange 2000 server or an Exchange 2003 server, but it cannot be installed on an Exchange 2007 server.

The Voice Connector performs the following functions:

- AMIS Networking—The Voice Connector routes voice messages to the applicable UAmis_<Servername> mailbox for outgoing analog delivery. Incoming AMIS voice messages received by the Cisco Unity AMIS bridgehead are routed to the Voice Connector for processing.

- Bridge Networking—The Voice Connector performs the message conversion and address translation that allows Cisco Unity to exchange messages with the Bridge server.

- VPIM Networking—The Voice Connector performs the message conversion and address translation that allows Cisco Unity to exchange messages with other Cisco Unity servers or other voice messaging systems by using the VPIM protocol. VPIM Networking also provides messaging between:

    - Cisco Unity servers that access separate directories
    - Cisco Unity with Domino systems and Cisco Unity with Exchange systems
    - Cisco Unity and Cisco Unity Express

Note that the Voice Connector is not needed with Digital Networking because the Cisco Unity servers access the same directory.

The Voice Connector ships with Cisco Unity and is available on the Cisco Unity Voice Connector for Exchange Software Download page, at
http://www.cisco.com/cgi-bin/tablebuild.pl/unity-voice-connector.

Active Directory Schema Extensions

A small subset of Cisco Unity data is stored in Active Directory. Therefore, before installing Cisco Unity, the Active Directory schema must be extended. In addition to the schema extensions required before installing Cisco Unity, the Active Directory schema must be extended before setting up the following:

- Bridge Networking
- VPIM Networking

The schema extensions needed to support Digital Networking and AMIS Networking are part of the general set of schema extensions for Cisco Unity.

For detailed information about the data that is stored in the directory, see the following white papers: *Cisco Unity Data and Active Directory (Cisco Unity 5.x and Later with Microsoft Exchange)* and *Active Directory Capacity Planning (Cisco Unity Version 5.x and Later with Microsoft Exchange)*. Both white papers are available at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html).

Comparison of AMIS, Bridge, and VPIM Networking

AMIS, Bridge, and VPIM Networking can be used for networking Cisco Unity with other voice messaging systems. However, there are several differences among these networking options, as described in the following sections:

- Interoperability
- General Connectivity Costs
- Supported Voice Gateways
- International Availability
- Blind Addressing
- Addressing by Name or by Extension
- Spoken Name Confirmation
- Audio Formats Supported
- Delivery Receipt/Read Receipt
- Directory Information Sharing
- Distribution Lists
- Mailbox ID Translation
- Fax Messaging
- Message Transport Time Considerations
- Private Messages
- Secure Messages
- Simultaneous Analog Sessions for Message Delivery to or from Remote Voice Mail Systems
- Urgent Messages
- System Broadcast Messages

Table 1-2   Interoperability

AMIS	Bridge	VPIM
For the most up-to-date list of supported voice messaging systems, see the applicable *Supported Hardware and Software, and Support Policies for Cisco Unity*, at http://www.cisco.com/en/US/ products/sw/voicesw/ps2237/ prod_installation_guides_list.html.	For the most up-to-date list of supported voice messaging systems, see the applicable *System Requirements, and Supported Hardware and Software for Cisco Unity Bridge*, at http://www.cisco.com/en/US/products/ sw/voicesw/ps2237/prod_installation_ guides_list.html.	For the most up-to-date list of supported voice messaging systems, see the applicable *Supported Hardware and Software, and Support Policies for Cisco Unity*, at http://www.cisco.com/en/US/products/ sw/voicesw/ps2237/prod_installation_ guides_list.html.

Table 1-3   General Connectivity Costs[1]

AMIS	Bridge	VPIM
License for the Cisco Unity server that functions as an AMIS bridgehead. Analog ports on the Cisco Unity server. Connectivity can be made in one of two ways: by using voice cards, or through supported voice gateways. (See Table 1-4.) Analog lines for message delivery. Applicable long distance charges if the Cisco Unity bridgehead server and the remote voice messaging system are physically located in different areas.	License for the Bridge server. (Note that a license is no longer required on the Cisco Unity bridgehead server.) A separate server for the Bridge software. Each server supports up to 24 ports. Voice cards for the Bridge server. Analog lines for message delivery between Bridge and Octel nodes. Applicable long distance charges if the Bridge server and the Octel system are physically located in different areas. SMTP network bandwidth for message delivery between the Bridge and Cisco Unity.	License for the Cisco Unity server that functions as a VPIM bridgehead. SMTP network bandwidth for message delivery.

1. Note that the costs shown in this table are associated with Cisco Unity. There may be additional connectivity costs associated with enabling AMIS, Octel Analog Networking, or VPIM for the voice messaging system with which Cisco Unity exchanges messages.

Table 1-4   Supported Voice Gateways

AMIS	Bridge	VPIM
For the most up-to-date list of supported voice gateways, see the applicable *Supported Hardware and Software, and Support Policies for Cisco Unity*, at http://www.cisco.com/en/US/ products/sw/voicesw/ps2237/prod_ installation_guides_list.html.	For the most up-to-date list of supported voice gateways, see the applicable *System Requirements, and Supported Hardware and Software for Cisco Unity Bridge*, at http://www.cisco.com/en/US/products/ sw/voicesw/ps2237/prod_installation_ guides_list.html.	N/A.

Table 1-5   International Availability

AMIS	Bridge	VPIM
All countries in which Cisco Unity is sold.	For a list of countries for which there is a voice-fax card approved for use, see the "Supported Voice-Fax Cards" section in the *System Requirements, and Supported Hardware and Software for Cisco Unity Bridge*, at http://www.cisco.com/en/US/products/ sw/voicesw/ps2237/prod_installation_ guides_list.html. Some deployments may service users in countries that are not on the "Supported Voice-Fax Cards for the Cisco Unity Bridge Server" list, but only when the Bridge server itself is located in one of the countries listed. The Bridge server is supported only when using the English-language version of Windows. The locale must be set to English (United States), and the language settings must be set only to Western Europe and United States. (Choosing additional language settings is not supported.) The Bridge software is not localized in any language other than English.	All countries in which Cisco Unity is sold.

Table 1-6   Blind Addressing

AMIS	Bridge	VPIM
Available through the Cisco Unity Telephone User Interface (TUI), Cisco Unity ViewMail for Microsoft Outlook, and the Cisco Unity Inbox.	Available through the Cisco Unity TUI, ViewMail, and the Cisco Unity Inbox.	Available through the Cisco Unity TUI, ViewMail, and the Cisco Unity Inbox.

Table 1-7   Addressing by Name or by Extension

AMIS	Bridge	VPIM
Available through the Cisco Unity TUI, ViewMail, and the Cisco Unity Inbox when AMIS subscribers exist in the Cisco Unity directory.	Available through the Cisco Unity TUI, ViewMail, and the Cisco Unity Inbox when Bridge subscribers exist in the Cisco Unity directory.	Available through the Cisco Unity TUI, ViewMail, and the Cisco Unity Inbox when VPIM subscribers exist in the Cisco Unity directory.

Table 1-8   Spoken Name Confirmation

AMIS	Bridge	VPIM
Available when a recorded voice name exists for the AMIS subscriber. Voice names for AMIS subscribers must be recorded individually in the Cisco Unity Administrator. Voice names for AMIS subscribers can be imported by using the Cisco Unity Bulk Import utility.	Available when a recorded voice name exists for the Bridge subscriber. Voice names for Bridge subscribers can be recorded individually in the Cisco Unity Administrator. However, because the Bridge supports directory information sharing, the text and recorded voice names of Octel subscribers are retrieved on a usage basis, and Bridge subscribers can be automatically created in the Cisco Unity directory with the retrieved text and voice names. Similarly, the text and voice names of Cisco Unity subscribers are retrieved by the Octel servers on a usage basis, and directory entries are automatically created on the Octel servers with the retrieved text and voice names. Voice names for Bridge subscribers can be imported by using the Cisco Unity Bulk Import utility.	Cisco Unity includes support for the automatic creation of VPIM subscribers. Therefore, the text and recorded voice names of senders on remote VPIM systems can be derived from incoming VPIM messages, and VPIM subscribers can be automatically created in the Cisco Unity directory with the derived text and voice names. Available when a recorded voice name exists for the VPIM subscriber. Voice names for VPIM subscribers can be recorded individually in the Cisco Unity Administrator. Voice names for VPIM subscribers can be imported by using the Cisco Unity Bulk Import utility.

Table 1-9   Audio Formats Supported[1]

AMIS	Bridge	VPIM
The AMIS protocol is not dependent on audio format. Any codec supported for use with Cisco Unity can be used.	Octel Analog Networking is not dependent on audio format. The Cisco Unity servers must use either the G.711 or the G.729a codec in order to communicate with the Cisco Unity Bridge servers.	The VPIM Version 3 Specification includes support for the following audio formats: G.711, G.726, and GSM 6.10. Any codec supported for use with Cisco Unity can be used. Outbound VPIM messages can be converted to G.726 or sent in the format in which they were recorded. Incoming VPIM messages can be converted to G.711, G.729a, or GSM 6.10, or remain in the format in which they were sent.

1. For a list of audio formats supported by Cisco Unity, see the *Audio Codecs and Cisco Unity* white paper, at
    http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

Table 1-10   ***Delivery Receipt/Read Receipt***

AMIS	Bridge	VPIM
The AMIS protocol does not support this functionality. A request for a delivery or read receipt may be allowed on either Cisco Unity or the remote AMIS voice mail system when addressing, but the request will not result in a receipt.	Requests for a delivery or read receipt generated by Cisco Unity are returned from the Octel system as delivery receipts. The receipt is sent to the sender after the message is delivered to the Octel node, regardless of when the Octel system places the message in the subscriber mailbox or when the message is actually read.	Requests for a delivery or read receipt generated by either Cisco Unity or the remote VPIM system are honored, although both are treated as requests for delivery receipts.

Table 1-11   ***Directory Information Sharing***

AMIS	Bridge	VPIM
The AMIS protocol does not provide any mechanism for sharing or synchronizing directory information. If the remote AMIS system is configured to send the recorded voice name in messages, Cisco Unity will play it as part of the message.	Avaya Octel analog networking includes the NameNet feature, which provides a mechanism to propagate text and voice names among nodes on the Octel analog network, based on message activity or by administrator request. The Cisco Unity Bridge participates in NameNet. The Bridge retrieves Octel subscriber names and voice names from other Octel nodes, and stores the data in a directory on the Bridge server. The Bridge also maintains a directory of Cisco Unity subscribers, and sends Cisco Unity names and voice names to the Octel nodes upon request. The Bridge synchronizes Octel subscriber information with Cisco Unity. By default, Cisco Unity allows the automatic creation, modification, and deletion of Bridge subscribers based on the information sent by the Bridge. Cisco Unity synchronizes Cisco Unity subscriber information with the Bridge. 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.	Although the VPIM specification does not define a mechanism for directory information sharing or synchronization, some VPIM-compliant voice mail systems may process vCards or header information in VPIM messages and update their directories based on message activity. Cisco Unity can be configured to include the recorded voice name and/or vCard of the sender in messages to the remote VPIM systems. The delivery location settings for a remote voice messaging system can be configured to allow automatic creation, modification, and deletion of VPIM subscribers for that location, based on vCard or header information received in incoming voice messages from that location. If the remote VPIM system is configured to send the recorded voice name and/or vCard in messages, Cisco Unity will make them available as part of the message.

Table 1-12   Distribution Lists

AMIS	Bridge	VPIM
The AMIS protocol does not support delivery to a distribution list on the recipient voice messaging system. Outbound messages from Cisco Unity to the AMIS system must be addressed to a mailbox ID on the remote system. (However, an administrator on the remote system may be able to configure a mailbox ID to forward messages to a distribution list.) Outbound messages from Cisco Unity can be addressed to a Cisco Unity public or private distribution list that includes AMIS subscribers. Private distribution lists can include blind addresses. Incoming AMIS messages are delivered to subscriber mailboxes only, and cannot be delivered to Cisco Unity public distribution lists. (However, you may be able to set up a Cisco Unity subscriber account whose sole purpose is to forward messages to a Cisco Unity public distribution list. See your Microsoft Exchange and Outlook documentation for more information.)	Octel Analog Networking does not support delivery to a distribution list on the recipient voice messaging system. Outbound messages from Cisco Unity to the Octel system must be addressed to a mailbox ID on the remote system. (However, an administrator on the remote system may be able to configure a mailbox ID to forward messages to a distribution list.) Outbound messages from Cisco Unity can be addressed to a Cisco Unity public or private distribution list that includes Bridge subscribers. Private distribution lists can include blind addresses. Incoming Bridge messages are delivered to subscriber mailboxes only, and cannot be delivered to Cisco Unity public distribution lists. (However, you may be able to set up a Cisco Unity subscriber account whose sole purpose is to forward messages to a Cisco Unity public distribution list. See your Microsoft Exchange and Outlook documentation for more information.)	The VPIM specification does not include support for message delivery to a distribution list on the recipient voice messaging system. Outbound messages from Cisco Unity to the VPIM system must be addressed to a mailbox ID on the remote system. (However, an administrator on the remote system may be able to configure a mailbox ID to forward messages to a distribution list.) Outbound messages from Cisco Unity can be addressed to a Cisco Unity public or private distribution list that includes VPIM subscribers. Private distribution lists can include blind addresses. Incoming VPIM messages are delivered to subscriber mailboxes only, and cannot be delivered to Cisco Unity public distribution lists. (However, you may be able to set up a Cisco Unity subscriber account whose sole purpose is to forward messages to a Cisco Unity public distribution list. See your Microsoft Exchange and Outlook documentation for more information.)

Table 1-13   Mailbox ID Translation

AMIS	Bridge	VPIM
Not available.	Prefixes can be defined so that Cisco Unity subscribers can address messages to Octel subscribers by entering a network address consistent with phone network dial plans. All Cisco Unity subscribers are mapped to a configurable mailbox and serial number value for use when communicating with Octel servers. This allows any Cisco Unity subscriber to represent mailbox X at node serial number Y within the Octel network, independent of the Cisco Unity numbering plan.	Additional digits can be automatically added to the beginning of the mailbox numbers that are associated with the Cisco Unity sender and remote recipient on messages that are sent from Cisco Unity subscribers. The same digits can be removed from the beginning of the remote sender and Cisco Unity mailbox numbers for delivery to Cisco Unity subscribers.

Table 1-14   Fax Messaging

AMIS	Bridge	VPIM
The AMIS protocol does not support this functionality.	Supported.	Supported; however, VPIM supports only the TIFF-F message format.

Table 1-15   Message Transport Time Considerations

AMIS	Bridge	VPIM
Analog delivery of the message from the sending system to the receiving system is the most significant contribution to transport time. The minimum analog delivery time can be calculated by multiplying the actual recording length of the message by the number of recipients of the message. The AMIS protocol requires a separate analog transmission of the message for each recipient. For example, a five-minute message with 10 recipients would require a minimum of 50 minutes for the analog transmission.	Analog delivery of the message from the sending system to the receiving system is the most significant contribution to transport time. The minimum analog delivery time is the actual recording length of the message. Octel Analog Networking allows a single analog transmission of a message addressed to multiple recipients, which the receiving node will deliver to all intended recipients. For example, a five-minute message with 10 recipients would require a minimum of 5 minutes for the analog transmission.	Exchange routing time and SMTP delivery time to a remote VPIM system are the only considerations. For example, a five-minute message with 10 recipients would likely take less than one minute to transmit.

Table 1-16   Private Messages

AMIS	Bridge	VPIM
The AMIS protocol does not support this functionality. Messages marked private when they are sent are not marked private when the recipient retrieves them.	Supported. Messages marked private when they are sent are marked private when the recipient retrieves them.	Supported. Messages marked private when they are sent are marked private when the recipient retrieves them.

Table 1-17   Secure Messages

AMIS	Bridge	VPIM
Incoming messages cannot be encrypted before being delivered to the local recipient. With default settings: Outgoing secure messages are undeliverable and will generate an NDR. When configured: Outgoing secure messages are decrypted by the Voice Connector and the message is no longer secure.	With default settings: Incoming messages will not be encrypted before being delivered to the local recipient. Outgoing secure messages are undeliverable and will generate an NDR. When configured: Incoming messages are encrypted before being delivered to the local recipient. Outgoing secure messages are decrypted by the Voice Connector and the message is no longer secure.	With default settings: Incoming messages will not be encrypted before being delivered to the local recipient. Outgoing secure messages are undeliverable and will generate an NDR. When configured: Incoming messages are encrypted before being delivered to the local recipient. Outgoing secure messages are decrypted by the Voice Connector and can be re-encrypted if the receiving server is Cisco Unity with Exchange and if secure messaging is configured. During transport outside the Cisco Unity system, messages are not encrypted.

Table 1-18   Simultaneous Analog Sessions for Message Delivery to or from Remote Voice Mail Systems

AMIS	Bridge	VPIM
Supported. Limited to the voice mail port availability on the AMIS bridgehead server. Ports available to place outgoing AMIS calls can be configured in the Cisco Unity Administrator (but not per AMIS destination).	Supported. Limited to Bridge server analog port availability. Maximum number of ports to deliver simultaneously to any single node, and the threshold to initiate and disconnect additional calls, can be configured per Bridge server.	N/A.

Table 1-19   *Urgent Messages*

AMIS	Bridge	VPIM
The AMIS protocol does not support this functionality. Messages marked urgent when they are sent are not marked urgent when the recipient retrieves them.	Supported. Messages marked urgent when they are sent are marked urgent when the recipient retrieves them.	Supported. Messages marked urgent when they are sent are marked urgent when the recipient retrieves them.

Table 1-20   *System Broadcast Messages*

AMIS	Bridge	VPIM
Not available.	Regular voice messages can be sent to a bulletin mailbox on an Octel Aria system or to a System Distribution List (SDL) on an Octel Serenade system. Similarly, system broadcast messages can be sent to a bulletin mailbox or SDL. Both types of message will be transmitted in the same way by the Cisco Unity Bridge and treated identically when delivered to the bulletin mailbox or SDL.	System broadcast messages can be sent between Cisco Unity with Exchange servers that do not share the same directory, or between Cisco Unity with Exchange and Cisco Unity Express servers, using VPIM. Other types of remote messaging systems will treat the system broadcast message in the same way they would treat a regular voice message.

Road Map to the Networking Documentation: Where to Go from Here

If your installation includes multiple Cisco Unity servers networked together and accessing a common directory, much of the information that you need is included in the "Digital Networking" chapter. Start with "Digital Networking" even if you will also be using other networking options.

If you plan to use AMIS to communicate with another voice messaging system, see the "AMIS Networking" chapter.

If you plan to use VPIM to communicate with another voice messaging system, see the "VPIM Networking" chapter.

If you plan to use the Bridge to communicate with Octel systems on an Octel analog network, see the *Networking Guide for Cisco Unity Bridge*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Regardless of which networking option you choose, you need to customize the settings for the primary location. See the "Primary Location Settings" chapter.

Digital Networking

Overview: Digital Networking

Each Cisco Unity server has a maximum number of subscribers that it can serve. When the voice messaging needs of your organizations require more than one Cisco Unity server, the servers can be networked together such that they access a single, global directory, while at the same time, each Cisco Unity installation in the network continues to serve only those subscribers that were created on the server. Digital Networking is the Cisco Unity feature that allows subscribers who are associated with one Cisco Unity server to exchange messages with subscribers who are associated with other Cisco Unity servers. With Digital Networking, subscribers can use the phone to log on to Cisco Unity and send voice messages to subscribers who are associated with other Cisco Unity servers ("To send a message, press 2"). After listening to messages, subscribers can reply to messages that were sent from subscribers on other Cisco Unity servers.

When the networked Cisco Unity servers are integrated with the same phone system, the servers can be grouped into a dialing domain and configured such that:

- Calls are transferred from the automated attendant or directory assistance to subscribers who are not associated with the local server.

- Identified subscriber messaging (ISM) works for networked subscribers: subscribers who call and leave messages for subscribers on other Cisco Unity servers in the dialing domain are identified as subscribers.

Subscribers use the same Cisco Unity tools for messaging with subscribers on other networked Cisco Unity servers that they use for messaging with subscribers on the same server. If your organization also has the FaxMail and Text to Speech e-mail features, subscribers can use the phone to forward fax and e-mail messages to any subscriber in the organization.

Although Cisco Unity stores information about subscribers (and other Cisco Unity objects such as call handlers) in a SQL Server database on the Cisco Unity server, a small subset of information about subscribers, distribution lists, and locations is also stored in Active Directory to enable Digital Networking. When subscriber and location data from other Cisco Unity servers replicates in Active Directory, Cisco Unity detects the data and updates the SQL Server database. Because of directory replication, each Cisco Unity server has the information that it needs to address voice messages to subscribers who are associated with the other Cisco Unity servers.

Requirements for Setting Up Digital Networking

The key to Digital Networking is that all of the Cisco Unity servers access a common directory. To use Digital Networking, the Cisco Unity servers must be in the same Active Directory forest.

Note that Cisco Unity servers that are licensed for Unified Messaging (UM) and Cisco Unity servers that are licensed for Voice Messaging (VM) can use Digital Networking to exchange messages. There are no licensing issues associated with VM and UM existing in the same Exchange organization or Active Directory forest, as long as the VM subscribers access voice and fax messages only over the phone interface or with the separately licensed Cisco Personal Communications Assistant (PCA).

For specific information about requirements and support, see the *Cisco Unity Networking Options Requirements* document, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Licenses and License Pooling

Digital Networking is enabled on every Cisco Unity server. There are no additional licenses that you need to obtain to set up Digital Networking.

Though you do not need a license for Digital Networking, you may want to add a licensed feature called license pooling. License pooling allows Cisco Unity servers that are set up for Digital Networking to pool licenses for subscribers and for the Cisco Unity Inbox. With license pooling, if total utilization across all of the Cisco Unity servers does not exceed total licenses for the feature, the Cisco Unity server is in compliance with licensing restrictions. For example: two Cisco Unity servers each have 500 licenses for subscribers; with license pooling, one of the servers can use 501 or more licenses as long as the total used by both servers does not exceed 1,000.

For all licensed features other than subscriber licenses, licensing is on a per-machine basis. Licensing information is stored with the primary location for each Cisco Unity server. Because location data is stored in the directory, each Cisco Unity server has the information that it needs to keep track of license usage in the pool.

For more information about license pooling and obtaining licenses for Cisco Unity features, see the applicable *Licensing for Cisco Unity* white paper, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

In This Chapter

In this chapter, you will find procedures for setting up and upgrading Digital Networking, followed by detailed discussions of the concepts and terminology you need to understand. See the following sections:

- Setting Up Digital Networking, page 2-3—This section describes the prerequisites for setting up Digital Networking, and provides a task list containing a high-level view of all of the tasks that you need to complete for the setup, and the order in which they should be completed.

- Procedures for Setting Up Cisco Unity to Use Digital Networking, page 2-4—This section contains all of the procedures necessary to set up Cisco Unity for Digital Networking.

- Digital Networking Concepts and Definitions, page 2-14—This section explains Digital Networking concepts in detail. If you are unfamiliar with Digital Networking, we recommend that you read this section prior to completing the setup procedures.

- Notable Behavior, page 2-24—This section contains information about notable behavior related to Digital Networking.

Related Documentation

- *Accessing Voice Mail in Multiple Unity Server Environments*, at http://www.cisco.com/warp/public/788/AVVID/one_message_button_two_unity_servers.html.

- The *Cisco Unity Data and Active Directory (Cisco Unity 5.x and Later with Microsoft Exchange)* white paper, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

- The *Active Directory Capacity Planning (Cisco Unity Version 5.x and Later with Microsoft Exchange)* white paper, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

Setting Up Digital Networking

Prerequisites

- Cisco Unity is already installed on the servers, according to the requirements and instructions in the Cisco Unity installation guide.

- Cisco Unity meets the requirements as described in the "Requirements for Setting Up Digital Networking" section on page 2-1.

Task List: Setting Up Digital Networking

Use this task list to set up Digital Networking on each Cisco Unity server. The cross-references take you to detailed procedures. If a system is using failover, do the tasks only on the primary server unless a task requires changing the registry, which must be done on both the primary and secondary servers. (The instructions will note this.)

1. Optionally, obtain and enable a license file for license pooling. See the "Enabling License Pooling (Optional)" section on page 2-4.

2. Customize the primary location. See the "Customizing the Primary Location" section on page 2-6.

3. Set the addressing, directory handler, and automated attendant search scopes. See the "Setting the Addressing, Directory Handler, and Automated Attendant Search Scopes" section on page 2-6. The Automated Attendant search option must be set to search the dialing domain in order for identified subscriber messaging to work.

4. Optionally, enable identified subscriber messaging (ISM). See the "Setting Up Identified Subscriber Messaging Between Networked Cisco Unity Subscribers (Optional)" section on page 2-8.

5. Modify the All Subscribers public distribution list. See the "Modifying the All Subscribers Public Distribution List" section on page 2-10.

6. Optionally, add alternate extensions to each subscriber account. For instructions, see the "Setting Up Alternate Extensions" section in the "Setting Up Features That Are Controlled by Subscriber or Subscriber Template Settings" chapter of the *System Administration Guide for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

7. Optionally, set up system broadcast messaging in order to send system broadcasts to all subscribers in the directory. See the "Setting Up System Broadcast Messaging for Sending to All Subscribers in the Directory (Optional)" section on page 2-10.

8. Optionally, change the default search scope in the Cisco Personal Communications Assistant to the global directory. See the "Changing the Default Search Scope for the Cisco PCA (Optional)" section on page 2-11.

9. Optionally, enable live reply between subscribers on different Cisco Unity servers. See the "Enabling Live Reply Between Cisco Unity Servers in the Same Dialing Domain (Optional)" section on page 2-11.

10. Test the Digital Networking setup. See the "Testing the Digital Networking Setup" section on page 2-12.

11. For Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) integrations only: Optionally, enable the cross-server features. See the "Cross-Server Logon, Transfers, and Live Reply" chapter for details.

Procedures for Setting Up Cisco Unity to Use Digital Networking

This section contains all of the procedures necessary to set up each Cisco Unity server for Digital Networking. Consult the "Task List: Setting Up Digital Networking" section on page 2-3 for information on the order in which the procedures must be completed.

Enabling License Pooling (Optional)

For each Cisco Unity server, you can choose whether it will participate in the license pool. To place a Cisco Unity server in the pool, obtain a license file with license pooling enabled, and then install the license file on the Cisco Unity server. If a license file on a Cisco Unity server does not have the license pooling feature enabled, the server does not participate in the pool, and compliance for licenses on that server is measured on a per-machine basis.

You obtain the license file by completing registration information on Cisco.com. Shortly after registration, Cisco e-mails the license file. The e-mail from Cisco contains instructions on how to save and store the files.

> **Note**   If the system is using failover, you install the license files only on the primary server.

The following information is required during registration:

- The MAC address (physical address) for the network interface card (NIC) in the Cisco Unity computer.

- The product authorization key (PAK) that appears on the sticker located on the front of the sleeve for Cisco Unity DVD 1 or CD 1.

Do the following procedures in the order listed.

To Get the MAC Address of the Cisco Unity Computer

Step 1   On the Cisco Unity server, do one of the following:

- If the server contains a dual NIC that has been configured for fault tolerance, run the NIC-configuration utility provided by the manufacturer, and write down the MAC address (excluding hyphens) that is shared by the two NICs. Then skip the rest of this procedure.

- If the server does not contain a dual NIC or if the server contains a dual NIC that is not configured for fault tolerance, on the Windows Start menu, click **Programs > Accessories > Command Prompt**.

Step 2   In the Command Prompt window, enter **ipconfig /all**, and press **Enter**.

Step 3   Write down the value of Physical Address, excluding the hyphens, or save it to a file that you can access during online registration. (For example, if the physical address is 00-A1-B2-C3-D4-E5, record 00A1B2C3D4E5.)

If the server contains more than one NIC, one value will appear for each NIC. Write down the value for the NIC that you will use to connect the Cisco Unity server to the network.

Step 4   Close the Command Prompt window.

To Register and Obtain the License Files

Step 1   Browse to the registration website at http://www.cisco.com/go/license (URL is case sensitive).

You must be a registered user on Cisco.com to obtain license files.

Step 2   Enter the PAK or software serial number, and click **Submit**.

Step 3   Follow the on-screen prompts.

Step 4   Shortly after registration, you will receive an e-mail with the Cisco Unity license files.

If license files are lost, it can take up to one business day to get another copy.

If you do not receive the license files within 1 hour or to get another copy of a license file, call the Cisco Technical Assistance Center (TAC) and ask for the Licensing Team:

In the U.S.	800 553-2447
Outside the U.S.	For your local Cisco TAC phone number, see the Cisco Worldwide Contacts page at http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Or open a service request by using the TAC Service Request Tool at http://tools.cisco.com/ServiceRequestTool/create/DefineProblem.do.

You will need to provide information to verify Cisco Unity ownership—for example, the purchase order number or the PAK (which appears on the sticker located on the front of the sleeve for Cisco Unity DVD 1 or CD 1).

To View the License Pooling Information

Step 1   On a Cisco Unity server that has a license file with license pooling enabled, double-click the **Cisco Unity Tools Depot** icon on the desktop.

Step 2   In the left pane of the Tools Depot window, expand **Administration Tools**.

Step 3   Double-click **License Info Viewer**.

Step 4   Under Cisco Unity Licensing, expand **License Pool**.

Step 5   Under License Pool, click **Subscriber Mailboxes**, **Maximum Unified Messaging Subscribers**, or **Cisco Unity Inbox Subscribers**.

Step 6   In the right pane, the names of the networked servers that share the subscriber license appear.

Customizing the Primary Location

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, do one of the following:

- If this server is not integrated with the same phone system as other networked Cisco Unity servers, click **None**.

- If this server is integrated with the same phone system as other networked Cisco Unity servers, 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   If you will be setting up for VPIM Networking, enter the SMTP Domain Name.

Step 7   Click **Save**.

For additional information about primary location settings, see the "Primary Locations Profile Page" section in the "Network Settings" chapter of the *Interface Reference Guide for the Cisco Unity Administrator*, available at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Setting the Addressing, Directory Handler, and Automated Attendant Search Scopes

Do the procedures in the following sections to set up the search scopes:

- Setting the Addressing Search Scope, page 2-6
- Setting the Directory Handler Search Scope, page 2-7
- Setting the Automated Attendant Search Scope, page 2-7

Setting the Addressing Search Scope

For detailed information about the addressing search options, see the "Primary Location Addressing Option Settings" section on page 9-3.

To Set the Addressing Search Scope

Step 1 In the Cisco Unity Administrator, go to the **Network > Primary Location > Addressing Options** page and set the addressing options as follows:

- To allow subscribers that are created on the local Cisco Unity server to address messages to subscribers on other Cisco Unity servers that access the same directory, select **Dialing Domain** or **Global Directory**, as applicable.

- If you are using blind addressing to a Cisco Unity server in a separate directory, or to another voice messaging system, set the Blind Addressing Allowed Locations setting to something other than None, as applicable.

Step 2 If you want subscribers to be able to do a spell-by-name search that is limited to a specific location, check the **Include Locations in Searches** check box.

Step 3 Click the **Save** icon.

Setting the Directory Handler Search Scope

To Set the Directory Handler Search Scope

Step 1 In the Cisco Unity Administrator, go to the **Call Management > Directory Handlers > Profile** page. If you are using only the default directory handler, skip to Step 3.

Step 2 Click the **Find** icon to find and view the directory handler that you want to change.

Step 3 Go to the Search Options page, and click **Dialing Domain**.

Step 4 Click the **Save** icon.

Step 5 Repeat Step 2 through Step 4 for each directory handler that you want to change.

Setting the Automated Attendant Search Scope

By default, callers who reach the opening greeting for your organization can be transferred only to subscribers who are associated with the local Cisco Unity server. If you want to set up the automated attendant so that callers can be transferred to subscribers who are associated with other Cisco Unity servers in the same dialing domain, change a registry setting as described in the following procedure.

The automated attendant search scope must be set to search the dialing domain in order for the following features to work:

- Identified subscriber messaging between Cisco Unity servers in the dialing domain

- Cross-server transfers from the automated attendant of one Cisco Unity server to another Cisco Unity server in the dialing domain

Note If the system is configured for failover, the registry changes must be made on both the primary and secondary Cisco Unity servers.

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**.

Setting Up Identified Subscriber Messaging Between Networked Cisco Unity Subscribers (Optional)

Enabling identified subscriber messaging (ISM) between networked Cisco Unity subscribers requires the following:

- The Cisco Unity servers must be connected to the same phone system or phone system network as described in the "Dialing Domains" section on page 2-15.

- The servers must be configured to be in the same dialing domain, as described in the "Customizing the Primary Location" section on page 2-6.

- 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 2-7.

- The applicable permissions must be set, as described in the "Setting Permissions on Active Directory Containers Used for Importing Subscribers" section on page 2-8.

- Identified subscriber messaging on each server must be enabled in the Cisco Unity Administrator as described in the "Enabling Identified Subscriber Messaging on Each Cisco Unity Server" section on page 2-9.

Setting Permissions on Active Directory Containers Used for Importing Subscribers

In Permissions wizard, on the Choose Active Directory Containers for Import page, you choose the Active Directory containers from which you want to import users, contacts, and groups to make them Cisco Unity subscribers and public distribution lists. Note the following:

- You must choose a container for the domain that includes the Cisco Unity server.

- If you will be importing users from the same container for every Cisco Unity server, choose that container. For example, if CiscoUnityServer1 and CiscoUnityServer2 will both be importing users from Container1 only, choose Container1.

- If, for all of the Cisco Unity servers combined, you will be importing users from two or more containers, the Cisco Unity message store services account on each Cisco Unity server must be granted SendAs permission on every container from which users will be imported on every Cisco Unity server in the forest. For example, if CiscoUnityServer1 will import users from

Container1 and Container2, and if CiscoUnityServer2 will import users from Container3 and Container4, the Cisco Unity message store services account for each Cisco Unity server must have SendAs permission for all four containers.

Although you can use different message store services accounts on each Cisco Unity server and set the SendAs permissions by using Active Directory Users and Computers, the easiest way to set the needed permissions is when you run Permissions wizard on each Cisco Unity server. Make note of the following:

- Use the same message store services account on each Cisco Unity server.
- Specify all of the import containers that will be used by all of the Cisco Unity servers.

Note that all of the Cisco Unity servers can use the same installation, directory services, and message store services accounts.

To Set the Applicable Permissions

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, expand **Administration Tools**.

Step 3   Double-click **Permissions Wizard**.

Step 4   Do the following:

- Choose the same Active Directory account for the Cisco Unity message store services account:
  - Click **Next** without changing any options until you arrive at the Choose the Cisco Unity Message Store Services Account page.
  - Choose the same Active Directory account for the Cisco Unity message store services account on every Cisco Unity server.
- Choose the applicable containers:
  - Click **Next** without changing any options until you arrive at the Choose Active Directory Containers for Import page.
  - Choose all of the containers from which users will be imported for every Cisco Unity server in the forest.

Step 5   Click **Next** without changing any options until you complete the wizard.

Step 6   Repeat Step 1 through Step 5 on each Cisco Unity in the forest.

Enabling Identified Subscriber Messaging on Each Cisco Unity Server

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 on Each Cisco Unity Server

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

Step 2   In the Identified Subscriber Messaging section, uncheck the **Disable Identified Subscriber Messaging** 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.

Modifying the All Subscribers Public Distribution List

By default, the predefined All Subscribers public distribution list on each Cisco Unity server has the same recorded voice name and extension. If you do not modify the recorded voice name and extension, subscribers will hear a confusing list of choices when they address messages to an All Subscribers distribution list, and errors will be logged to the Windows Event Viewer on the Cisco Unity server.

To Modify the All Subscribers Public Distribution List

Step 1   In the Cisco Unity Administrator, go to the **Public Distribution List > Profile** page.

Step 2   Click the **Find** icon.

Step 3   In the Find By list, indicate how to find the distribution list, and then click **Find**.

Step 4   In the Name list, click **All Subscribers -<Server Name>** to display the profile settings for the list.

Step 5   Record a unique voice name for the list.

Step 6   Assign a unique extension to the list.

Step 7   Optionally, change the display name of the list to match the recorded voice name. By default, the Cisco Unity server name is appended to the display name, so the display name is unique in the directory.

Step 8   Click the **Save** icon.

Setting Up System Broadcast Messaging for Sending to All Subscribers in the Directory (Optional)

System broadcast messages are recorded announcements that are sent to everyone in an organization (or to particular location(s) within an organization). When each server has been configured for Digital Networking, a system broadcast message can be sent to all subscribers on all Cisco Unity servers that share the same directory. Alternatively, a system broadcast message can be sent to all subscribers on one or more specific Cisco Unity servers that access the same subscriber directory, by addressing the message to the delivery location Dial ID of the desired server.

System broadcast messages do not light message waiting indicators (MWIs) on subscriber phones, nor do they cause distinctive dial tones to notify subscribers of a new message when they pick up their desk phone receiver. System broadcast messages also do not trigger message notifications for alternative devices, such as a pager or another phone.

To allow one or more Cisco Unity subscriber(s) to send system broadcast messages to subscribers on multiple Cisco Unity servers, you first set up and offer the subscriber(s) access to the Cisco Unity Broadcast Message Administrator. For information on setting up the Cisco Unity Broadcast Message Administrator, see the "Sending System Broadcast Messages" section in the "Cisco Unity Conversation" chapter of the *System Administration Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Note that individual subscribers can be granted permissions to send system broadcast messages either on the local Cisco Unity server only, or to subscribers on multiple servers.

In organizations where there are multiple Cisco Unity or Cisco Unity Express servers that access different directories, the VPIM Networking option must be used in order to include subscribers on those servers in the distribution of a system broadcast message. For information on setting up system broadcast messages to be distributed to VPIM locations, see the "Networked System Broadcast Messages" section on page 8-7.

Changing the Default Search Scope for the Cisco PCA (Optional)

By default, the search scope for the Cisco Personal Communications Assistant (PCA) address book is set to local directory. As a possible convenience to subscribers in your organization, you may want to change the default search scope to global directory instead. When the default search scope is set to the global directory, subscribers can search for subscribers at different locations without having to change the search scope themselves. In addition, subscribers will not need to keep track of which Cisco Unity subscribers are listed in the local directory and which are listed in the global directory.

Regardless of the default search scope that you specify here, subscribers can still switch between the local and global directory as they use the Cisco PCA Address Book in the Cisco Unity Inbox and Cisco Unity Assistant.

Use the following procedure to set the global directory as the default search scope for the Cisco PCA Address Book. The change affects all subscribers that are associated with the Cisco Unity server.

To Set the Default Search Scope to the Global Directory for the Cisco PCA Address Book

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 Inbox and Assistant—Set Default Address Book Search Scope**.

Step 4   In the New Value list, click **1**, and then click **Set** so that the Address Book searches for subscribers within the global directory by default.

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

Step 6   Click **Exit**.

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

Enabling Live Reply Between Cisco Unity Servers in the Same Dialing Domain (Optional)

Live reply allows subscribers who listen to their messages by phone to reply to a message from a subscriber by calling the subscriber. For live reply to work:

- Subscribers must belong to a class of service in which live reply is enabled. Live reply is enabled on the Subscribers > Class of Service > Messages page in the Cisco Unity Administrator, by checking the Subscribers Can Reply to Messages from Subscribers by Calling Them check box.

- Transfer numbers must be configured for each Cisco Unity subscriber.

- Cisco Unity must identify the sender of the message as a subscriber. This happens either when the sender logs in to his or her mailbox to send the message, or when identified subscriber messaging is enabled and the sender calls the recipient from a recognized subscriber phone number and is forwarded to Cisco Unity. (To set up identified subscriber messaging, see the "Setting Up Identified Subscriber Messaging Between Networked Cisco Unity Subscribers (Optional)" section on page 2-8.)

By default, live reply is restricted to subscribers on the same Cisco Unity server. Do the following procedure to enable live reply via release to phone system transfer between subscribers on different Cisco Unity servers in the same dialing domain.

To Enable Live Reply Between Cisco Unity Servers in the Same Dialing Domain

Step 1   Verify that the addressing search scope has been set to the dialing domain as described in the "Setting the Addressing, Directory Handler, and Automated Attendant Search Scopes" section on page 2-6.

Step 2   In the Cisco Unity Administrator, go to the **Network > Dialing Domain Options** page. (If the link is not active, that means that the Cisco Unity server has not been configured to be in a dialing domain.)

Step 3   In the Live Reply section, check the **Subscribers Can Call Back a Cisco Unity Subscriber on a Different Cisco Unity Server** check box.

Step 4   Leave the **Release Calls to the Phone System** button selected (this is the default).

> ⚠️
> **Caution**   Do not select the **Cross-Server Live Reply: Pass Control to the Called Subscriber's Cisco Unity Server** option unless you have read the restrictions and requirements that are explained in the "Cross-Server Logon, Transfers, and Live Reply" chapter.

Step 5   Click the **Save** icon.

Testing the Digital Networking Setup

Each Cisco Unity server stores the primary location data and a subset of the data about subscriber accounts and distribution lists in the directory. The time that it takes for data from other Cisco Unity servers to be reflected on the local server depends on your Active Directory network configuration and replication schedule. You need to wait for the Cisco Unity data to replicate to the other servers before testing the Digital Networking setup.

To test the Digital Networking setup, create test subscriber accounts or use existing subscriber accounts on each Cisco Unity server. When setting up subscriber accounts in the Cisco Unity Administrator to be used in the tests, be sure to:

- Record voice names.
- Record and enable internal greetings.
- Check the List in Phone Directory check box on the Subscriber Profile page.
- Check the Before Playing Each Message, Play the Sender's Name check box on the Subscriber Conversation page.

Do the following tests to make sure Digital Networking is functioning properly:

- To Verify Messaging Between Subscribers on Different Cisco Unity Servers, page 2-13

To Verify Messaging Between Subscribers on Different Cisco Unity Servers

Verify that messaging between subscribers on different Cisco Unity servers works in both directions (for example, from server A to server B and from server B to server A).

Step 1   Log on to a Cisco Unity server as a subscriber.

Step 2   Press **2** to record and send messages to subscribers who are associated with other Cisco Unity server(s).

Step 3   Log on to the applicable Cisco Unity server as the recipient subscriber to verify that the message was received.

Step 4   Repeat Step 1 through Step 3 in the opposite direction.

To Verify Call Transfers from the Automated Attendant to Subscribers on Other Cisco Unity Servers

If the automated attendant search scope is set to search the dialing domain, verify that outside callers are transferred to subscribers who are associated with other Cisco Unity servers.

Step 1   From a non-subscriber phone, call the Cisco Unity server that has been configured to handle outside callers, and enter the extension of a subscriber who is associated with another Cisco Unity server.

Step 2   Verify that you reach the correct subscriber phone.

To Verify Call Transfers from a Directory Handler to Subscribers on Other Cisco Unity Servers

If the directory handler search scope is set to search the dialing domain, verify that outside callers can find subscribers who are associated with other Cisco Unity servers in the phone directory.

Step 1   From a non-subscriber phone, call the Cisco Unity server that has been configured to handle outside callers, and transfer to a directory handler.

Step 2   Verify that you can find a subscriber who is associated with another Cisco Unity server in the phone directory, and that the directory handler transfers the call to the correct subscriber phone.

To Verify Identified Subscriber Messaging Between Networked Subscribers

Do this test if the Cisco Unity servers have been configured for identified subscriber messaging between networked subscribers.

Step 1   Verify that Cisco Unity plays an internal greeting for subscribers who leave messages, by doing the following sub-steps:

    a.   From a subscriber phone, call a subscriber who is associated with another Cisco Unity server, and allow the call to be forwarded to voice mail.

    b.   Verify that the internal greeting plays.

    c.   Leave a test message.

Step 2   Verify that subscribers are identified when the recipient listens to a message, by doing the following sub-steps:

    a.   Log on to the applicable Cisco Unity server as the recipient subscriber and listen to the test message that you recorded in Step 1.

    b.   Verify that the subscriber conversation announces who the message is from by playing the recorded voice name of the sending subscriber.

    c.   After listening to the message, verify that the subscriber conversation allows you to reply to the message.

To Verify Live Reply Between Subscribers on Different Cisco Unity Servers in the Dialing Domain

Do this test if the Cisco Unity servers have been configured for live reply (via release to phone system transfer) between subscribers on different Cisco Unity servers in the same dialing domain.

Step 1   From a subscriber phone, call a subscriber who is associated with another Cisco Unity server, and allow the call to be forwarded to voice mail.

Step 2   Leave a message.

Step 3   Log on to the applicable Cisco Unity server as the recipient subscriber and listen to the test message that you recorded in Step 2.

Step 4   After listening to the message, verify that the subscriber conversation allows you to live reply to the message by pressing 4-4 (or by pressing 8-8 if Optional Conversation 1 is used).

Step 5   Verify that the live reply call is correctly transferred to the phone of the subscriber who left the message.

Digital Networking Concepts and Definitions

The following sections explain Digital Networking concepts in detail:

- Distribution Lists, page 2-22
- System Broadcast Messages, page 2-23

Locations and Digital Networking

Central to how Digital Networking works is a Cisco Unity object called a 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) that are 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.

The primary location also contains a Dial ID, which Cisco Unity uses as an identifier for the location. Carefully plan the numbers that you choose as Dial IDs for the primary location (and for any delivery locations that you create). Without careful planning, it is possible to inadvertently assign Dial IDs that will cause problems in locating message recipients at another location. See the "Assigning Dial IDs" section on page 9-2 and the "Location Addressing Options" section on page 9-8 for more information.

Dialing Domains

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. (This includes Cisco Unity servers that are 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 on the phone network. In the same way, when grouped in a dialing domain, subscribers who are associated with one Cisco Unity server enter a subscriber extension when sending messages to subscribers who are associated with another Cisco Unity server.

To be in a dialing domain, all of the Cisco Unity servers must access the same directory; a dialing domain cannot span directories. Dialing domains are not related to Exchange routing groups or Active Directory sites.

To group the Cisco Unity servers in a dialing domain, you enter information on the primary location page of each Cisco Unity server, as described in the "Customizing the Primary Location" section on page 2-6.

The following sections describe the functionality that can be provided when the Cisco Unity servers are in the same dialing domain:

- Release to Switch Transfers from the Automated Attendant or a Directory Handler to Subscribers on Other Cisco Unity Servers, page 2-16
- Identified Subscriber Messaging with Networked Cisco Unity Subscribers, page 2-16
- Addressing Search Scopes, page 2-17
- Addressing Options for Subscribers in a Dialing Domain, page 2-17
- Dialing Domains Shield Against Overlapping Numbering Plans, page 2-17

Release to Switch Transfers from the Automated Attendant or a Directory Handler to Subscribers on Other Cisco Unity Servers

By default, when a caller enters the extension of a subscriber from the automated attendant (for example, from the opening greeting), or a caller spells the name of a subscriber from a directory handler, Cisco Unity searches only the local server for a matching subscriber. For calls to be transferred from the automated attendant or a directory handler on one Cisco Unity server to a subscriber on another Cisco Unity server, the servers must be configured to be in the same dialing domain.

To enable this functionality, you set search scopes so that Cisco Unity searches for a matching extension or name among subscribers on other Cisco Unity servers in the dialing domain. There are separate search scopes, one for the automated attendant and one for each directory handler. See the "Setting the Directory Handler Search Scope" section on page 2-7 and the "Setting the Automated Attendant Search Scope" section on page 2-7 for details on how to set the search scopes.

Subscriber call transfer settings are not stored in the directory. Because the directory is the means by which Cisco Unity servers share subscriber data, Cisco Unity servers do not have access to the call transfer settings of subscribers on other Cisco Unity servers. By default, when calls are transferred from the automated attendant or a directory handler to subscribers who are not associated with the local server, the transfers are automatically handled by the phone system (release to switch) rather than by Cisco Unity (supervised transfer), even if these subscribers are set up for supervised transfers. Note the following limitations:

- The subscriber call screening, call holding, and announce features that are available with supervised transfers are not available on calls that have been transferred via release to switch.

- The call transfer setting that sends calls directly to the greeting of the called subscriber is not available. This means that Cisco Unity cannot take messages for subscribers (either regular Cisco Unity subscribers or AMIS, Bridge, Internet, or VPIM subscribers) who do not have phones on the phone system that Cisco Unity is integrated with. On a release to switch transfer, Cisco Unity dials the subscriber extension and hangs up. What happens to the call after that depends on how the phone system is configured. If you do not configure the phone system to handle this situation, the call may be dropped.

Identified Subscriber Messaging with Networked Cisco Unity Subscribers

When a subscriber calls another subscriber, and the call is forwarded to the greeting of the called subscriber, the ability of Cisco Unity to identify that it is a subscriber who is leaving a message is referred to as identified subscriber messaging. Because Cisco Unity is able to identify the caller as a subscriber:

- Cisco Unity plays the internal greeting of the called subscriber when the caller leaves a message.

- Cisco Unity plays the recorded voice name of the subscriber who left the message when the recipient listens to the message.

- Cisco Unity allows the recipient to record a reply.

For identified subscriber messaging to work when a subscriber on one Cisco Unity server calls a subscriber on another networked Cisco Unity server, the servers must be in the same dialing domain. Note that identified subscriber messaging between Cisco Unity servers by default is not enabled. See the "Setting Up Identified Subscriber Messaging Between Networked Cisco Unity Subscribers (Optional)" section on page 2-8 for details.

It is important to note the difference between the following two circumstances:

- A subscriber logs on to Cisco Unity, and then records and sends a message ("To send a message, press 2")

- A subscriber places a phone call to another subscriber, and then leaves a message

When the subscriber has logged on to Cisco Unity, Cisco Unity can identify the message as being from the subscriber, regardless of which Cisco Unity server the message recipient is homed on. In this case, the phone system is not involved and the recipient phone does not ring. Instead, the message is sent via Digital Networking.

Addressing Search Scopes

In addition to the automated attendant and directory handler search scopes mentioned above, a dialing domain provides a means to set the scope for searches that Cisco Unity performs in the following cases:

- When a subscriber addresses a message
- When members are being added to a public or private distribution list

By default, the addressing search scope used for the above searches is set to search only among subscribers on the local Cisco Unity server. You must expand the addressing search scope on each Cisco Unity server to either the dialing domain or the global directory to enable messaging between subscribers on different Cisco Unity servers. See the "Setting the Addressing Search Scope" section on page 2-6 for information on how to expand the Addressing search scope.

Addressing Options for Subscribers in a Dialing Domain

After expanding the addressing search scope to either the dialing domain or the global directory, subscribers address messages to subscribers on other Cisco Unity servers the same way that they address messages to subscribers on the same Cisco Unity server: either by extension or by spelling the name.

Dialing Domains Shield Against Overlapping Numbering Plans

The two requirements for grouping Cisco Unity servers into a dialing domain are that the servers access the same global directory and are integrated with the same phone system. However, the minimum requirement for the basic messaging functionality provided by Digital Networking is that all of the Cisco Unity servers access the same global directory, as Figure 2-1 illustrates.

Figure 2-1   Multiple Phone Systems But One Global Directory
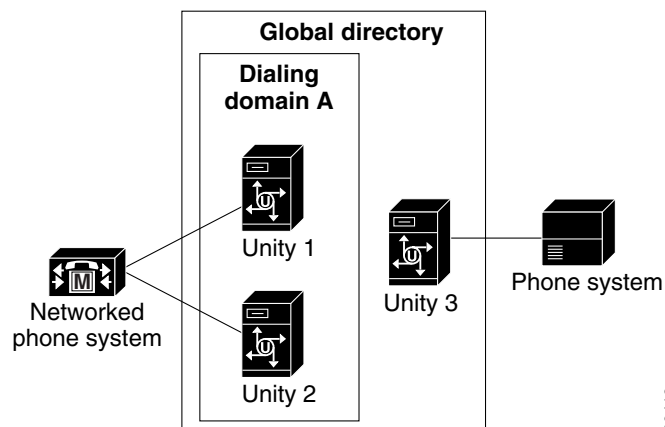
Subscribers on the Cisco Unity servers in the dialing domain can use the phone to send messages to and reply to messages from the subscribers on Unity 3, and vice versa. However, identified subscriber messaging is not available between the subscribers on Unity 3 and the subscribers on the Cisco Unity servers in dialing domain A.

Although subscriber extensions must be unique within a dialing domain, it is possible that subscribers who are associated with a Cisco Unity server outside of the dialing domain could have extensions that are the same as extensions used by subscribers who are associated with the servers within the dialing domain. In other words, it is possible that extensions may overlap in the global directory when there are Cisco Unity servers that are integrated with different phone systems.

Grouping the Cisco Unity servers into a dialing domain allows Cisco Unity to handle overlapping numbering plans. The dialing domain allows the subscribers within the dialing domain to use extensions to address messages without conflicting with the extensions of the subscribers on the other phone system. See the "How Cisco Unity Searches for a Matching Name" section on page 9-4 and the "How Cisco Unity Searches for a Matching Number" section on page 9-4 for a detailed description of how dialing domains shield against overlapping numbering plans.

Addressing Options for Non-Networked Phone Systems

If your organization has a separate phone system for each location, subscribers at one location dial a complete phone number, not just an extension, when calling someone at another location. When subscribers log on to Cisco Unity to send messages to subscribers on another Cisco Unity server, the number they enter when addressing the message depends on whether the Cisco Unity numbering plans overlap across locations, as described in the following sections.

When Numbering Plans Do Not Overlap

When Cisco Unity numbering plans do not overlap across locations—that is, when subscriber extensions are unique across locations—subscribers enter an extension when addressing a message to a subscriber who is associated with another Cisco Unity server.

As a convenience for subscribers, you may choose to add alternate extensions to each subscriber account. With alternate extensions, the number that a subscriber enters when addressing a message to someone at another location can be the same number that the subscriber dials when calling. When set up this way, subscribers do not need to remember two different numbers—one for calling a subscriber directly, and one for addressing a message.

For example, a subscriber, Kelly Bader, has subscriber extension 4060, as illustrated in Figure 2-2. Suppose that Chris, a subscriber at a remote location, dials 456-4060 to reach Kelly by phone. When Chris logs on to Cisco Unity to send a message to Kelly, he has to remember just to dial the extension (4060) and not dial the prefix (456) when addressing the message, rather than using the same number he dials to call Kelly. However, you could assign to Kelly the alternate extension 4564060. If this alternate extension has been set up, Chris can enter either 4060 or 4564060 when addressing a message to Kelly.

Figure 2-2   No Overlapping Extensions
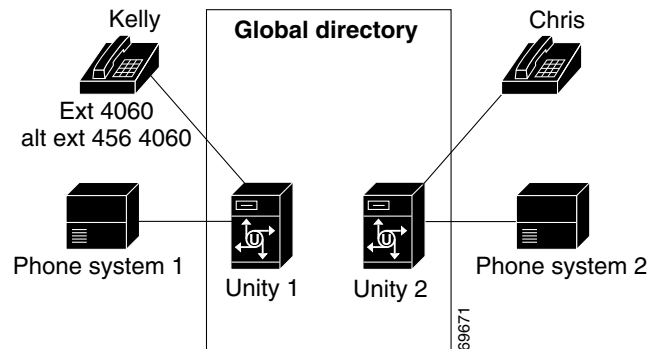
If the numbering plans for each location do not overlap, setting up alternate extensions is optional because they are simply a convenience for subscribers. However, if you do not set up alternate extensions, be sure to tell subscribers to use the extension instead of the full phone number when addressing messages to subscribers who are associated with another location.

Note that alternate extensions have other purposes beyond their use in Digital Networking, such as handling multiple line appearances on subscriber phones. Subscribers can have up to nine alternate extensions. For more information, see the "Specifying Subscriber Alternate Extension Settings" section in the "Setting Up Features That Are Controlled by Subscriber or Subscriber Template Settings" chapter of the *System Administration Guide for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

When Numbering Plans Overlap

Assume that subscriber extensions on Unity 3 in Figure 2-3 overlap with extensions in dialing domain A. To allow subscribers who are associated with Unity 3 to use the phone to address messages to subscribers in dialing domain A, and vice versa, you have the following choices:

- Instruct subscribers to enter one number that consists of the primary location Dial ID of the destination Cisco Unity server and the extension of the recipient.

- Set up alternate extensions for each subscriber account. For each subscriber, enter a number for the alternate extension that is the same as the full phone number for the subscriber. In this way, when subscribers log on to Cisco Unity to send messages, the number they enter when addressing messages is the same number that they use when calling.

- Enable the Include Locations in Searches setting. When this setting is enabled, subscribers can address a message in two steps: they first select a location (by spelling the location name or entering a Dial ID) and then spell the recipient name.

When a subscriber addresses a message, Cisco Unity searches for a matching extension on the local Cisco Unity server first. If a match is found, Cisco Unity ends the search and never looks for a matching extension at another location. Therefore, if a local subscriber and a subscriber on another Cisco Unity server have the same extension, Cisco Unity will find only the subscriber on the local Cisco Unity server. However, when one of the options described above is set up, subscribers on the local server will be able to address messages to subscribers on other Cisco Unity servers.

Cisco Unity Administrator Scope

With the exception of public distribution lists, all subscribers and other Cisco Unity objects (such as call handlers) that are created on your Cisco Unity server are associated with the primary location of your server. Because of this association, if you want to access the subscriber accounts and other objects that are created on another server, you need to run the Cisco Unity Administrator of the server that the object was created on. Note that you can view information about the primary locations of other servers and the delivery locations created on other servers, but you cannot modify or delete them.

The following sections provide information about accessing the Cisco Unity Administrator on other servers:

- Browsing to Another Cisco Unity Administrator from the Local Cisco Unity Administrator, page 2-20
- Searching for Subscriber Accounts That Were Created on Another Cisco Unity Server, page 2-21
- Using Global Subscriber Manager to Browse to Another Cisco Unity Administrator, page 2-21

Browsing to Another Cisco Unity Administrator from the Local Cisco Unity Administrator

The Cisco Unity Administrator on the local server provides links to the Cisco Unity Administrator of other servers. To access the data of any object that was created on another Cisco Unity server, you need to know the name of the server on which the object was created.

To Browse to Another Cisco Unity Administrator on a Networked Cisco Unity Server

Step 1   Near the bottom of the navigation bar on the left side of the Cisco Unity Administrator interface, click **Unity Servers**. The Server Chooser page appears.

Step 2   From the list, click the server that you want to access.

Step 3   If prompted, enter the appropriate credentials to gain access to the Cisco Unity Administrator that you want to access.

Another instance of the Cisco Unity Administrator appears in a separate browser window. This is the Cisco Unity Administrator of the server that you selected.

Searching for Subscriber Accounts That Were Created on Another Cisco Unity Server

Within the local Cisco Unity Administrator, you can search for subscribers on other Cisco Unity servers, and when you select a subscriber account to edit settings, the applicable Cisco Unity Administrator is launched. Do the following procedure to use the Cisco Unity Administrator on your local Cisco Unity server to search for subscriber accounts on other Cisco Unity servers in the network.

To Search for Subscriber Accounts That Were Created on a Cisco Unity Server Other than Your Local Cisco Unity Server

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

Step 2   Click the **Find** icon.

Step 3   Indicate whether to search by alias, extension, first name, or last name.

Step 4   Enter the appropriate alias, extension, or name. You also can enter ***** to display a list of all subscribers, or enter one or more characters or values followed by ***** to narrow your search.

Step 5   Check the **Search All Cisco Unity Servers** check box.

Step 6   Click **Find**.

Step 7   On the list of matches, click the name of the subscriber to display the record.

Step 8   If prompted, enter the appropriate credentials to gain access to the Cisco Unity Administrator that you want to access.

Another instance of the Cisco Unity Administrator appears in a separate browser window. This is the Cisco Unity Administrator website of the Cisco Unity server on which the subscriber account was created. The subscriber profile page is displayed in the new browser window.

Using Global Subscriber Manager to Browse to Another Cisco Unity Administrator

You can also use the Global Subscriber Manager (GSM) from Tools Depot to launch the Cisco Unity Administrator on another server. The GSM shows your entire Cisco Unity network broken down by dialing domains and servers. The GSM allows you to quickly locate individual subscribers and launch the Cisco Unity Administrator for the subscribers regardless of which server they are homed on. You can select any scope you want and see all of the subscribers at that level. Searching can be done by dialing domain, by server, or globally across the entire Cisco Unity network.

To Use the GSM

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

Step 2   In the left pane, double-click **Global Subscriber Manager**.

Step 3   Double-click the subscriber account that you want to edit. The applicable Cisco Unity Administrator will be displayed in a browser window. See the GSM Help file for more information.

Granting Administrative Rights to Other Cisco Unity Servers

To access the Cisco Unity Administrator on another server, the administrators on the local Cisco Unity server need the applicable class of service rights. The easiest way to set this up is to run the GrantUnityAccess utility. See the "Granting Administrative Rights to Other Cisco Unity Servers" section in the "Managing Cisco Unity Administrator Accounts" chapter in the *System Administration Guide for Cisco Unity* for instructions. (The *System Administration Guide for Cisco Unity* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.)
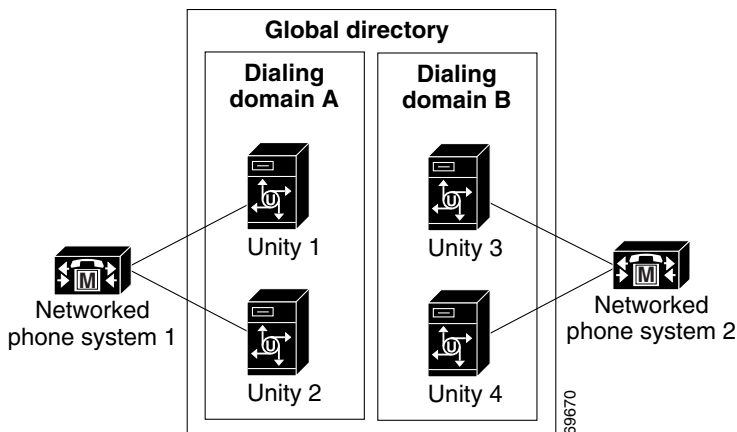
Distribution Lists

Public distribution lists are not associated with a specific Cisco Unity server. If a list has a recorded voice name, an extension, or both, subscribers can address messages to it—if allowed by their class of service—regardless of which location created the list.

New Lists

When you create a new public distribution list, keep in mind the following:

- The extension for the list must be unique in the entire directory. Therefore, you need to know which extensions are in use at other locations before assigning an extension to the new list.

- In the Cisco Unity Administrator, you can add members from multiple locations to a list, if allowed by the Addressing Options settings for the default location on your Cisco Unity server. See the "Primary Location Addressing Option Settings" section on page 9-3 for more information.

- In the Cisco Unity Administrator, you can view all members of a list regardless of the location with which the member is associated.

Predefined Public Distribution Lists

Cisco Unity includes the following predefined public distribution lists: All Subscribers, Unaddressed Messages, and System Event Messages (the System Event Messages list is no longer created during Cisco Unity installation; however, you may still have a System Event Messages list if you upgraded from a version of Cisco Unity earlier than 4.0(4), as the list is not removed during the upgrade process). Each Cisco Unity server in your organization has a distinct version of each of these lists. When you view these lists in the Cisco Unity Administrator, the Cisco Unity server name is appended to the list name.

By default, the predefined All Subscribers public distribution list on each Cisco Unity server has the same recorded voice name ("all subscribers") and extension. When setting up Digital Networking, you should modify the recorded voice name and extension of each All Subscribers list; if you do not, subscribers will hear a confusing list of choices when they address messages to an All Subscribers distribution list, and errors will be logged to the Windows Event Viewer on the Cisco Unity server because of the non-unique extensions.

> **Tip**   Distribution lists can be nested, that is, a distribution list can contain other lists. If desired, you can create one master All Subscribers distribution list that contains the All Subscribers list of each Cisco Unity server.

By default, each Unaddressed Messages and System Event Messages distribution list has the same recorded voice name, but they are not assigned an extension because subscribers typically do not address messages to these lists.

Private Lists

When creating private lists, subscribers can add members from other locations if allowed by the Addressing Options settings for your default location. The location addressing options allow you to control the search that Cisco Unity performs when a subscriber adds members to a private list and when a subscriber addresses a message. For more information, see the "Primary Location Addressing Option Settings" section on page 9-3.

Consider notifying subscribers in the event that the following members are inadvertently removed from their lists:

- When you delete a delivery location, blind addressees are removed from all private lists.
- When an external subscriber (that is, an AMIS, Bridge, or VPIM subscriber) becomes a regular subscriber, the external subscriber is removed from all private lists.

System Broadcast Messages

System broadcast messages are recorded announcements that are sent to everyone in an organization (or to particular location(s) within an organization). System broadcast messages are played immediately after subscribers log on to Cisco Unity by phone—even before they hear message counts for new and saved messages. Subscribers must listen to each system broadcast message in its entirety before Cisco Unity allows them to hear new and saved messages or to change setup options. They cannot fast-forward or skip a system broadcast message.

System broadcast messages do not light message waiting indicators (MWIs) on subscriber phones, nor do they cause distinctive dial tones to notify subscribers of a new message when they pick up their desk phone receiver. System broadcast messages also do not trigger message notifications for alternative devices, such as a pager or another phone.

System broadcast messages can be networked to all subscribers on one or more Cisco Unity servers that access the same subscriber directory by using Digital Networking. In organizations where there are multiple Cisco Unity or Cisco Unity Express servers that access different directories, system broadcast messages can be sent to all subscribers in the organization (or to all subscribers who are associated with specific sets of digitally networked servers), provided that the networks are connected by using the VPIM Networking option.

Addressing System Broadcast Messages to Digitally Networked Servers

Depending on the desired set of recipients and the options selected in the Cisco Unity Broadcast Administrator, a subscriber who has been granted permission to send system broadcast messages to subscribers on multiple servers can address messages to all subscribers on the local server, to all subscribers on one or more digitally networked servers, or to all subscribers on all servers in the domain by using Digital Networking.

For example, consider a situation in which three Cisco Unity servers share the same directory. The servers are named ChicagoUnity (dial ID 344), NewYorkUnity (dial ID 444), and AtlantaUnity (dial ID 544). A subscriber on ChicagoUnity who has been granted permission to send system broadcast messages to subscribers on multiple servers can address a message from the Cisco Unity Broadcast

Message Administrator by using the options in Table 2-1, which result in a system broadcast being transmitted to all subscribers on the local server or to all subscribers on multiple servers within the directory.

Table 2-1   Using the Cisco Unity Broadcast Administrator to Address Messages to Servers Within the Directory

Cisco Unity Broadcast Administrator Option Selected	Extension Entered	System Broadcast Recipients
Send to Subscribers on this Server	N/A	All subscribers on ChicagoUnity
Send to Subscribers at all Locations	N/A	All subscribers on all Cisco Unity servers in the directory—ChicagoUnity, NewYorkUnity, and AtlantaUnity
Send to One or More Locations, or to a Public Distribution List	444	All subscribers on NewYorkUnity (dial ID 444)
Send to One or More Locations, or to a Public Distribution List	444, then 544	All subscribers on NewYorkUnity (dial ID 444) and AtlantaUnity (dial ID 544)

Individual Cisco Unity servers within the directory can be added by location dial ID as shown in the example above. Public distribution lists are only used for sending system broadcast messages to VPIM locations. For more information on sending system broadcast messages by using VPIM, see the "Addressing System Broadcast Messages to Multiple Servers" section on page 8-7.

Note that when a system broadcast message is sent to multiple locations, a copy of the message is sent to each server and then distributed to the subscribers who are homed on that server. As a result, the subscriber who is sending the system broadcast message must make updates to each message locally. In this example, after the ChicagoUnity subscriber has sent a message, if updates need to be made to any properties on the message at a later time, he or she would need to have permission to log on to the Cisco Unity Broadcast Administrator on each server to make the updates.

How Networked System Broadcast Messages are Processed by Cisco Unity

When Cisco Unity is installed, a new Windows service called CsBMessageConnector is created, along with a special mailbox that has the display name USbms_<Servername>. The USbms mailbox is created in the default directory container for Cisco Unity, and is hidden from the address book. The CsBMessageConnector service processes messages that are placed in the USBms mailbox. For systems that use failover, the CsBMessageConnector service runs on both the primary and secondary servers, and both services access the same USbms mailbox, but only the service on the currently active server will process messages.

When a system broadcast message is addressed to multiple Cisco Unity servers, a copy of the message is placed in the USbms mailbox for each server; the CsBMessageConnector service on each server processes the message and makes it available to all Cisco Unity subscribers on the server, based on the start and end dates configured for the message.

Notable Behavior

This section provides information about notable expected behavior associated with Digital Networking.

Mapping Subscribers to Cisco Unity Servers

Each Cisco Unity server handles a distinct group of subscribers. In large organizations, it is possible that more than one Cisco Unity server will be in use at the same physical location. In this case, you need to determine which subscriber accounts to create on each of the Cisco Unity servers (the "home" Cisco Unity server for each subscriber), and keep a record of the mapping. This record is needed for the following reasons:

- Subscriber phones must forward calls to the Cisco Unity server on which the subscribers are homed.

- If subscriber phones have a "Messages" or a speed-dial button that dials the number to access Cisco Unity, the buttons must be configured to call the Cisco Unity server on which the subscribers are homed.

- To check their messages, subscribers must dial the Cisco Unity server that they are associated with; therefore you need to tell subscribers the correct number to dial when calling into Cisco Unity. Note that if your Cisco Unity servers are integrated with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager), you may want to configure cross-server logon. For more information, see the "Cross-Server Logon, Transfers, and Live Reply" chapter.

To create a record of the mapping, run the Subscribers report on each Cisco Unity server. The information in this report includes the subscriber name and primary location. See the "Subscribers Report" section in the "Reports" chapter of the *Maintenance Guide for Cisco Unity* for more information. (The *Maintenance Guide for Cisco Unity* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.)

Networking Guide for Cisco Unity Release 5.x (With Microsoft Exchange)

Cross-Server Logon, Transfers, and Live Reply

This chapter describes the cross-server logon, transfer, and live reply features for Cisco Unity servers networked via Digital Networking. Phone system and network considerations for deploying cross-server features are discussed. The underlying architecture for the cross-server features is described, and design and monitoring recommendations are provided. Also included in this chapter are the procedures for activating the cross-server features.

See the following sections:

Overview of Cross-Server Logon, Transfer, and Live Reply

The cross-server features are an extension of the existing Digital Networking feature. Digital Networking provides basic messaging functionality for subscribers who are homed on different Cisco Unity servers that access the same global directory. When the networked Cisco Unity servers are integrated with the same phone system, the servers can be grouped into a dialing domain so that calls can be transferred—via release to switch—from the automated attendant (for example, from the opening greeting) or from a directory handler on one Cisco Unity server to a subscriber on another. Even though Digital Networking and dialing domains provide basic messaging and call transfer functionality for subscribers who are homed on different Cisco Unity servers, each Cisco Unity installation in the network continues to serve only those subscribers whose accounts were created on the server. The purpose of the cross-server features is to make the subscriber experience in a Digitally-Networked environment almost the same as in a single Cisco Unity server environment, as shown in Table 3-1.

Table 3-1   *Cross-Server Features*

Feature	Description
Cross-server logon	Cross-server logon allows administrators to provide subscribers who are homed on different Cisco Unity servers in the same dialing domain with one phone number that they can call to log on to Cisco Unity. When calling from outside the organization to log on to Cisco Unity, subscribers—no matter which is their home Cisco Unity server—call the same number and are transferred to the applicable home Cisco Unity server to log on.
Cross-server transfer	Cross-server transfer enables calls from the automated attendant or from a directory handler of one Cisco Unity server to be transferred to a subscriber on another Cisco Unity server in the dialing domain, according to the call transfer and screening settings of the called subscriber.
Cross-server live reply	Cross-server live reply allows subscribers who listen to their messages by phone to reply to a message from a subscriber on another Cisco Unity server in the dialing domain by calling the subscriber (according to the call transfer and screening settings of the called subscriber).

Although the cross-server features are distinct features, they all use the same underlying functionality—an enhanced supervised call transfer:

1. The Cisco Unity server on which a logon, transfer, or live reply originates puts the caller on hold and calls the home Cisco Unity server.

2. When the destination Cisco Unity server answers, the originating Cisco Unity server sends a sequence of DTMF tones that identify the call as a cross-server logon, transfer, or live reply.

3. The destination Cisco Unity server responds with a sequence of DTMF tones, and the originating Cisco Unity server hands off the call to the destination server for processing.

4. At this point the functionality is the same as though the call had originated on the home Cisco Unity server.

In this chapter, an originating Cisco Unity server is defined as a server that calls other Cisco Unity servers. A destination Cisco Unity server is defined as a server that answers a cross-server call.

Phone System Considerations for Cross-Server Features

The cross-server features are supported for integrations with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager), integrations with phone systems through PIMG/TIMG units, and/or integrations with Cisco SIP Proxy Server (CSPS). Integrations with phone systems through voice cards are not supported.

The following factors can contribute significantly to delays in cross-server call handoff:

- Longer subscriber extensions. A four-digit extension does not take as long for Cisco Unity to dial as a ten-digit extension.

- Longer dialing strings to reach the destination Cisco Unity server. A four-digit dialing string does not take as long for Cisco Unity to dial as a ten-digit dialing string.

- Multiple elements (such as PIMG/TIMG units, voice gateways, TDM trunks, and PSTN interfaces) in the call path between the originating Cisco Unity server and the destination Cisco Unity server. More elements in the call path require more processing time for handing off cross-server calls.

In your environment, these factors can create delays that may cause the cross-server features to be unusable or unfeasible for callers. You must test your cross-server configuration on a representative call path in your environment to determine whether the delays that callers experience are acceptable.

Planning for Increased Port Usage

The cross-server features require the use of ports on both the originating and destination Cisco Unity servers. Depending on how busy your Cisco Unity servers are, you may need to add more ports or an additional Cisco Unity server before enabling these features. You may also need to adjust how ports are configured. For example, you may need to enable more ports to accept incoming calls.

After enabling the cross-server features, we recommend that you monitor activity on the Cisco Unity servers closely until you are confident that the servers can handle the increased load. You can use the Port Usage Analyzer for this task. The Port Usage Analyzer is available in the Report Tools section of Tools Depot. See Port Usage Analyzer Help for detailed instructions. Be sure to monitor the Windows Event Viewer on both the originating and destination Cisco Unity servers for event log messages related to problems with ports.

A Brief Look at Cisco Unity Data Architecture

To understand why the cross-server features are needed, it is helpful to have a basic understanding of Cisco Unity data architecture. Cisco Unity stores information about subscribers (and other Cisco Unity objects such as call handlers) in a SQL Server database on the Cisco Unity server. A small subset of information about subscribers, distribution lists, and location objects is also stored in Active Directory. Because all of the Cisco Unity servers access the same global directory, each Cisco Unity server has access to the information stored in the directory by other Cisco Unity servers. When subscriber, distribution list, and location data from other Cisco Unity servers replicates in the directory, each Cisco Unity server detects the data and updates its local SQL Server database.

The data that is stored in the directory is limited to just what is needed to provide basic Digital Networking functionality:

- Messaging between subscribers homed on different Cisco Unity servers.
- Release to switch call transfers from the automated attendant or directory handler to subscribers on different Cisco Unity servers in the dialing domain.

Why Cross-Server Logon Is Needed

Without cross-server logon, subscribers have to call the specific Cisco Unity server they are homed on to log on to their mailboxes over the phone. There are several reasons for this restriction:

- The subscriber conversation requires access to subscriber greetings and subscriber call handler, call transfer, and call screening information. However, subscriber greetings and most of the other subscriber information is stored only on the Cisco Unity server on which the subscriber account was created. This data is not replicated across the directory because of size considerations.
- The message store services on each Cisco Unity server log on with a domain account that has the permissions needed to access local subscriber mailboxes. If different domain accounts are assigned to the message store facing services on other Cisco Unity servers, the message store services on one Cisco Unity server may be unable to log on to the mailboxes of subscribers on other Cisco Unity servers.

Why Cross-Server Transfer Is Needed

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 call transfer and screening settings are replicated. For example, in Figure 3-1, 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 instead "Yes, Ring Subscriber's Extension," the number 3047 would be replicated.

Figure 3-1   Only the Call Transfer Number Is Replicated
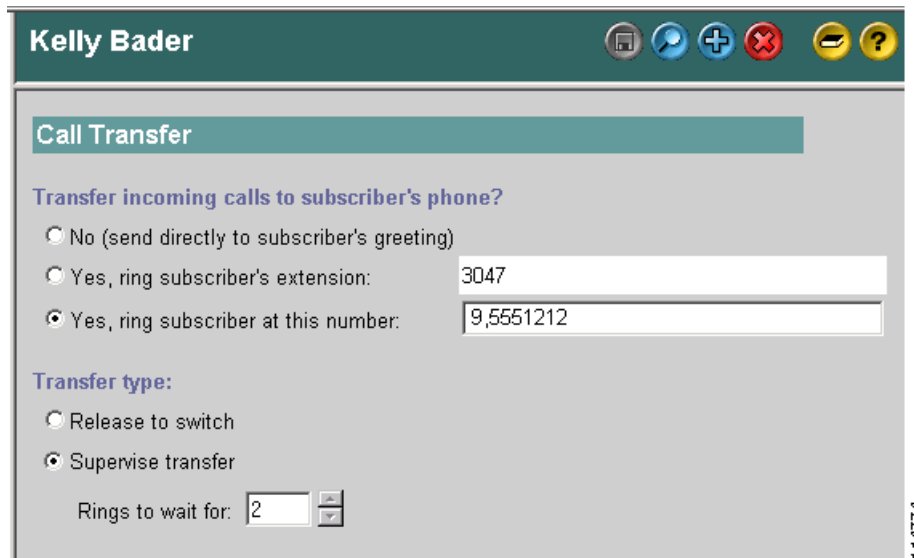
When the call transfer setting is set to "No (Send Directly to Subscriber's Greeting)," the call transfer number is automatically set to the subscriber extension (3047 in the example in Figure 3-1), which is replicated to the other networked Cisco Unity servers.

Without cross-server transfer, call transfers to subscribers whose accounts were 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 example in Figure 3-1). On a release to switch transfer, Cisco Unity dials the call transfer number configured for the subscriber and hangs up, leaving the phone system to handle the call. Note the following limitations with release to switch transfers:

- The 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 subscriber extension and hangs up. If the subscriber extension is a valid extension on the phone system that Cisco Unity is integrated with, 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.

Why Cross-Server Live Reply Is Needed

Cross-server live reply is needed for the same reasons detailed in the "Why Cross-Server Transfer Is Needed" section on page 3-4:

- Only the subscriber call transfer number is replicated to the networked Cisco Unity servers.

- The subscriber call transfer, call screening, call holding, and announce features are ignored.

Cross-Server Logon

Without cross-server logon, subscribers need to call the Cisco Unity server on which their accounts were created to log on and access their messages. This is particularly problematic for sites that move subscribers between different Cisco Unity servers for load balancing, because each time a subscriber account is moved to another Cisco Unity server, the subscriber must be notified to access a different Cisco Unity server when calling in from outside the organization.

Cross-server logon solves the problem when the networked Cisco Unity servers are integrated with the same phone system and grouped in a dialing domain. When enabled, cross-server logon allows you to provide subscribers with one phone number that they can call to log on to Cisco Unity from outside your organization. After cross-server logon is configured, subscribers call the pilot number for one Cisco Unity server and are transferred correctly to their home Cisco Unity server to log on. The call is handled as follows:

1. A subscriber calls the Cisco Unity server configured for cross-server logon and logs on to Cisco Unity.

2. The conversation looks up the caller's ID in the SQL Server database to determine whether the subscriber account is homed on the local Cisco Unity or another Cisco Unity server in the dialing domain.

- If the subscriber account is homed on the local server, the logon proceeds as usual.

- If the subscriber account is homed on another server, Cisco Unity plays a "Please wait" prompt (if configured to do so), puts the subscriber on hold, and calls the subscriber home Cisco Unity server by using the same port that the subscriber called in on. Note that if the subscriber is calling from a number that matches a primary or alternate extension, the "Please wait" prompt is the first prompt that the subscriber hears.

   When the destination Cisco Unity server answers, the originating Cisco Unity server sends a sequence of DTMF tones that identifies the call as a cross-server logon.

3. The destination Cisco Unity server responds with a sequence of DTMF tones.

4. The origination server hands off the call to the destination Cisco Unity server for processing. The conversation on the destination Cisco Unity server prompts for the subscriber password. At this point, the behavior is as though the subscriber had called the destination Cisco Unity server directly.

The intended use of this feature is limited to subscribers calling in from outside your organization. Also note that:

- Subscriber phones must still forward calls to the subscriber home Cisco Unity server.

- On subscriber phones, the "Messages" or speed-dial button that dials the number to access Cisco Unity must still be configured to call the home Cisco Unity server of the subscriber.

Although cross-server logon will transfer the calls to the home server in the above cases, doing so for a large number of subscribers will increase the load on the Cisco Unity servers. Therefore, when a subscriber account is moved to another Cisco Unity server, the subscriber phone still must be configured to call the home server.

Prerequisites: Enabling Cross-Server Logon

- All of the Cisco Unity servers must be configured for Digital Networking as described in the "Setting Up Digital Networking" section on page 2-3.

- The cross-server features are supported for integrations with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager), integrations with phone systems through PIMG/TIMG units, and/or integrations with Cisco SIP Proxy Server (CSPS). Integrations with phone systems through voice cards are not supported. See the "Phone System Considerations for Cross-Server Features" section on page 3-2 for more information.

Task List: Enabling Cross-Server Logon

Use the following task list to enable cross-server logon. The cross references take you to detailed procedures.

1. Verify that all of the networked Cisco Unity servers are configured to be in the same dialing domain, as described in the "Customizing the Primary Location" section on page 2-6.

2. On the destination Cisco Unity servers, verify that the Cisco Unity call routing rules are set to route calls to the Opening Greeting call handler. (This is the default when Cisco Unity is initially installed.) See the "Verifying That Call Routing Rules Are Set to Route Calls to the Opening Greeting" section on page 3-6.

3. On the Cisco Unity server that you have designated to handle cross-server logons (the server that subscribers will be calling), enable cross-server logon and enter the pilot numbers of the destination Cisco Unity servers. See the "Enabling Cross-Server Logon and Entering the Pilot Numbers of Destination Cisco Unity Servers" section on page 3-7.

4. Test the cross-server logon functionality. See the "Testing Cross-Server Logon" section on page 3-7.

✎ **Note** Subsequently, if a new Cisco Unity server is added to the dialing domain, you will have to add the pilot number of the new server to the Network > Dialing Domain Options page.

Procedures: Enabling Cross-Server Logon

Verifying That Call Routing Rules Are Set to Route Calls to the Opening Greeting

Do the following procedure on each of the destination servers. For failover systems, do the procedure on both the primary and secondary servers.

To Verify That Call Routing Rules Are Set to Route Calls to the Opening Greeting

Step 1 In the Cisco Unity Administrator, go to the **Call Routing > Direct Calls** page.

Step 2   Verify that calls to the pilot number for the server are routed to the Opening Greeting.

The Default Call Handler routing rule (which cannot be deleted or modified) sends calls to the Opening Greeting. Therefore, if you have not added any routing rules, the server is already set to correctly process cross-server calls.

Enabling Cross-Server Logon and Entering the Pilot Numbers of Destination Cisco Unity Servers

If the system is using failover, do the following procedure on both the primary and secondary server, because most of the settings on the Network > Dialing Domain Options page are stored in the registry. (Registry settings are not replicated to the secondary server.)

To Enable Cross-Server Logon and to Enter the Pilot Numbers of Destination Cisco Unity Servers

Step 1   In the Cisco Unity Administrator, go to the **Network > Dialing Domain Options** page.

Step 2   In the Cross Server Logon section, check the **Subscribers Dial the Same Number to Log On to Cisco Unity** check box.

Step 3   In the Pilot Numbers for Cross-Server Logon, Transfer, and Live Reply section, enter the pilot number in the Dial String field for each Cisco Unity server displayed in the table. (Note that the pilot numbers that you enter are stored in the SQL Server database UnityDb on the Cisco Unity server. Therefore, if the system is using failover, the pilot numbers will be replicated to the secondary server.)

Step 4   Check the **Play Prompt During Cross-Server Logon, Transfer, and Live Reply so That Callers Know Something Is Happening** check box. Although playing the "Please wait" prompt is optional, we recommend that you check the check box because the cross-server process can take several seconds before the destination Cisco Unity prompts subscribers to enter their passwords.

> **Note**   It is particularly important for the "Please wait" prompt to be played when a subscriber calls from a phone number configured as a primary or alternate extension, because the originating Cisco Unity server will not prompt for the subscriber ID. If the "Please wait" prompt is not played, the first prompt that the subscriber hears will be when the destination server prompts for a password, which could take several seconds.

Step 5   Click the **Save** icon.

Testing Cross-Server Logon

We recommend that you test cross-server logon before allowing subscribers to use the feature.

For failover systems, first test that the primary destination servers answer cross-server calls. Then manually fail over the destination servers to verify that the secondary server answers cross-server calls. If the destination servers are properly configured for failover, the secondary server should answer cross-server calls when the primary server is unavailable.

To Test Cross-Server Logon

Step 1 For each number listed in the Pilot Numbers section on the Network > Dialing Domain Options page, use a phone to call the number and verify that the call is routed to the Opening Greeting of the destination Cisco Unity server.

Step 2 Create a new subscriber account (or use an existing account) on each of the destination servers for testing purposes. Be sure to verify that the subscriber account information has replicated to all of the Cisco Unity servers that you will be testing. The time that it takes for the subscriber data to replicate depends on your network configuration and replication schedule.

Step 3 For each subscriber account, call the pilot number for the server configured for cross-server logon, and attempt to logon. Verify that:

- The "Please wait" prompt is played (if configured to do so).

- You successfully log on.

Cross-Server Transfer from the Automated Attendant and Directory Handlers

A cross-server transfer is a special kind of supervised transfer that passes control of a call from the automated attendant or a directory handler to the home Cisco Unity server of the called subscriber.

1. A caller calls a Cisco Unity server on which an audio text application has been configured.

2. The caller does one of the following:

   – In a call handler (such as the opening greeting), enters the extension of a subscriber on another Cisco Unity server in the dialing domain, or

   – In a directory handler, spells the name of a subscriber on another Cisco Unity server in the dialing domain.

3. The Cisco Unity server that is handling the call puts the caller on hold, and calls the subscriber home Cisco Unity server.

4. When the destination Cisco Unity server answers, the originating Cisco Unity server sends a sequence of DTMF tones that identify the call as a cross-server transfer.

5. The destination server responds with a sequence of DTMF tones.

6. The originating server hands off the call to the destination Cisco Unity server for processing. At this point, the behavior is as though the caller had directly called the automated attendant or directory handler on the destination Cisco Unity server.

When cross-server transfers have been configured, subscriber call transfer, call screening, call holding, and announce features are available.

Prerequisites: Enabling Cross-Server Transfer

- All of the Cisco Unity servers must be configured for Digital Networking as described in the

- The cross-server features are supported for integrations with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager), integrations with phone systems through PIMG/TIMG units, and/or integrations with Cisco SIP Proxy Server (CSPS). Integrations with phone systems through voice cards are not supported. See the "Phone System Considerations for Cross-Server Features" section on page 3-2 for more information.

Task List: Enabling Cross-Server Transfer

Use the following task list to enable cross-server transfer. The cross references take you to detailed procedures.

1. Verify that all of the networked Cisco Unity servers are configured to be in the same dialing domain, as described in the "Customizing the Primary Location" section on page 2-6.

2. Verify that the directory handler and automated attendant search scopes have been set to the dialing domain, as described in the "Setting the Addressing, Directory Handler, and Automated Attendant Search Scopes" section on page 2-6.

3. On the destination Cisco Unity servers, verify that the Cisco Unity call routing rules are set to route calls to the Opening Greeting call handler. (This is the default setting when Cisco Unity is initially installed.) See the "Verifying That Call Routing Rules Are Set to Route Calls to the Opening Greeting" section on page 3-9.

4. On the Cisco Unity server that has the audio-text application that handles calls from outside callers, enable cross-server transfer and enter the pilot numbers of the destination Cisco Unity servers. See the "Enabling Cross-Server Transfer and Entering the Pilot Numbers of Destination Cisco Unity Servers" section on page 3-10.

5. Optionally, if you want to enable cross-server transfers to external subscribers, change the "Networking—Cross-Server Transfer Behavior for External Subscribers" setting in the Advanced Settings Tool. Both the originating and destination Cisco Unity servers must be at version 5.0(1) or later to enable this feature. See the "Optional: Enabling Cross-Server Transfer for External Subscribers" section on page 3-10.

6. Optionally, if you want to enable the transfer override digit sequence for subscribers that are homed on other Cisco Unity servers, change the "Networking—Allow Transfer Override on Cross-Server Transfer Handoff" setting in the Advanced Settings Tool. Both the originating and destination Cisco Unity servers must be at version 5.0(1) or later to enable this feature. See the "Optional: Enabling Transfer Override on Cross-Server Transfer Handoff" section on page 3-11.

7. Test the cross-server logon functionality. See the "Testing Cross-Server Transfer" section on page 3-11.

Note   Subsequently, if a new Cisco Unity server is added to the dialing domain, you will need to add the pilot number of the new server to the Network > Dialing Domain Options page.

Procedures: Enabling Cross-Server Transfer

Verifying That Call Routing Rules Are Set to Route Calls to the Opening Greeting

Do the following procedure on each of the destination servers. For failover systems, do the procedure on both the primary and secondary servers.

To Verify That Call Routing Rules Are Set to Route Calls to the Opening Greeting

Step 1   In the Cisco Unity Administrator, go to the **Call Routing > Direct Calls** page.

Step 2   Verify that calls to the pilot number for the server are routed to the Opening Greeting.

The Default Call Handler routing rule (which cannot be deleted or modified) sends calls to the Opening Greeting. Therefore, if you have not added any routing rules, the server is already set to correctly process cross-server calls.

Enabling Cross-Server Transfer and Entering the Pilot Numbers of Destination Cisco Unity Servers

If the system is using failover, do the following procedure on both the primary and secondary server, because most of the settings on the Network > Dialing Domain Options page are stored in the registry. (Registry settings are not replicated to the secondary server.)

To Enable Cross-Server Transfer and to Enter the Pilot Numbers of Destination Cisco Unity Servers

Step 1   In the Cisco Unity Administrator, go to the **Network > Dialing Domain Options** page.

Step 2   Click **Pass Control to the Called Subscriber's Cisco Unity Server**.

Step 3   In the Pilot Numbers for Cross-Server Logon, Transfer, and Live Reply section, enter the pilot number in the Dial String field for each Cisco Unity server displayed in the table. (Note that the pilot numbers that you enter are stored in the SQL Server database UnityDb on the Cisco Unity server. Therefore, if the system is using failover, the pilot numbers will be replicated to the secondary server.)

Step 4   Check the **Play Prompt During Cross-Server Logon, Transfer, and Live Reply so That Callers Know Something Is Happening** check box. Although playing the "Please wait" prompt is optional, we recommend that you check the box because the cross-server process can take several seconds before the caller is transferred.

Click the **Save** icon.

Optional: Enabling Cross-Server Transfer for External Subscribers

By default, transfers to external subscribers (AMIS, Bridge, VPIM, Internet, and Trusted Internet subscribers) who are homed on a server in the dialing domain other than the server from which the transfer is initiated will be conducted as release to switch transfers. Do the following procedure if you want transfers to external subscribers who are homed on another Cisco Unity server to be done via cross-server transfer. Note that both the originating and destination Cisco Unity servers must be at Cisco Unity version 5.0(1) or later to enable this feature.

To Enable Cross-Server Transfer for External Subscribers

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—Cross-Server Transfer Behavior for External Subscribers**.

Step 4 In the New Value list, click **0**, and then click **Set**.

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

You do not need to restart the Cisco Unity software or server when you make a change.

> **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.

Optional: Enabling Transfer Override on Cross-Server Transfer Handoff

When a caller enters an extension in the automated attendant followed by the digits "#2," the caller will be routed directly to the greeting for the extension entered without a transfer being attempted. This is known as the transfer override digit sequence. By default, the transfer override digit sequence is ignored when the subscriber who is associated with the extension preceding the "#2" is homed on another Cisco Unity server in the dialing domain. If you want to enable the transfer override digit sequence for subscribers who are homed on other Cisco Unity servers, do the following procedure. Both the originating and destination Cisco Unity servers must be at version 5.0(1) or later to enable this feature.

To Enable Transfer Override on Cross-Server Transfers

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—Allow Transfer Override on Cross-Server Transfer Handoff**.

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

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

You do not need to restart the Cisco Unity software or server when you make a change.

> **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.

Testing Cross-Server Transfer

We recommend that you test cross-server transfer before allowing subscribers to use the feature.

For failover systems, first test that the primary destination servers answer cross-server calls. Then manually fail over the destination servers to verify that the secondary server answers cross-server calls. If the destination servers are properly configured for failover, the secondary server should answer cross-server calls when the primary server is unavailable.

To Test Cross-Server Transfer

Step 1   For each number listed in the Pilot Numbers section on the Network > Dialing Domain Options page, use a phone to call the number and verify that the call is routed to the Opening Greeting of the destination Cisco Unity server.

Step 2   Create a new subscriber account (or use an existing account) on each of the destination servers for testing purposes.

Step 3   For each subscriber account, call the pilot number for the server configured for cross-server transfer, and enter the subscriber extension at the opening greeting. Verify that:

- The "Please wait" prompt is played.

- The call is transferred to the subscriber phone or the greeting, according to the call transfer settings of the called subscriber.

Cross-Server Live Reply

Live reply, when enabled, allows a subscriber who is listening to messages by phone to reply to another subscriber message by calling the subscriber directly. Note that whether subscribers have access to the live reply feature is controlled by the class of service.

In order for the live reply option to be offered when a subscriber listens to a message that was left by a subscriber on another Cisco Unity server in the dialing domain, cross-server live reply must be enabled and the Cisco Unity server on which the message was recorded must have identified the sender of the message as a subscriber. By default, live reply between subscribers who are homed on different Cisco Unity servers is not enabled.

When live reply and cross-server live reply are enabled:

1. After listening to a message from a subscriber on another Cisco Unity server in the dialing domain, a subscriber chooses to call the subscriber who left the message.

   Note that if identified subscriber messaging (ISM) between networked servers has not been set up, or if ISM is disabled on the Cisco Unity server that recorded the message, the live reply option will only be available for messages that are sent by subscribers who log on to Cisco Unity and address and send the message from their mailboxes.

2. Cisco Unity puts the subscriber on hold and looks up the extension in the SQL Server database to determine whether the subscriber who is being replied to is on the same server or is on another Cisco Unity server in the dialing domain. If the subscriber is on the same server, processing proceeds as usual.

   However, if the subscriber who is being replied to is on another Cisco Unity server, the local Cisco Unity server calls the applicable home Cisco Unity server.

3. When the destination Cisco Unity server answers, the originating Cisco Unity server sends a sequence of DTMF tones that identify the call as a cross-server live reply.

4. The destination server responds with a sequence of DTMF tones.

5. The originating server hands off the call to the destination Cisco Unity server for processing. Note, however, that if the subscriber account on the destination server is set to disable call transfers (that is, the call transfer option is set to send calls to the subscriber greeting), the live reply call fails. In

this case, the subscriber conversation on the originating Cisco Unity plays a prompt to the caller saying that live reply is unavailable and suggesting that the caller reply to the message instead of calling the subscriber directly.

Prerequisites: Enabling Cross-Server Live Reply

- All of the Cisco Unity servers must be configured for Digital Networking as described in the "Setting Up Digital Networking" section on page 2-3.
- The cross-server features are supported for integrations with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager), integrations with phone systems through PIMG/TIMG units, and/or integrations with Cisco SIP Proxy Server (CSPS). Integrations with phone systems through voice cards are not supported. See the "Phone System Considerations for Cross-Server Features" section on page 3-2 for more information.
- Subscribers must belong to a class of service for which live reply is enabled. Live reply is enabled on the Subscribers > Class of Service > Messages page in the Cisco Unity Administrator, by checking the Subscribers Can Reply to Messages from Subscribers by Calling Them check box.
- Transfer numbers must be configured for each Cisco Unity subscriber.
- For live reply to be available to messages that were sent when the sender called the recipient from a recognized phone number and was forwarded to Cisco Unity, identified subscriber messaging must be set up between networked Cisco Unity servers. See the "Setting Up Identified Subscriber Messaging Between Networked Cisco Unity Subscribers (Optional)" section on page 2-8.

Task List: Enabling Cross-Server Live Reply

Use the following task list to enable cross-server live reply. The cross references take you to detailed procedures.

1. Verify that all of the networked Cisco Unity servers are configured to be in the same dialing domain, as described in the "Customizing the Primary Location" section on page 2-6.

2. Verify that the directory handler and automated attendant search scopes have been set to the dialing domain, as described in the "Setting the Addressing, Directory Handler, and Automated Attendant Search Scopes" section on page 2-6.

3. On the destination Cisco Unity servers, verify that the Cisco Unity call routing rules are set to route calls to the Opening Greeting call handler. (This is the default when Cisco Unity is initially installed.) See the "Verifying That Call Routing Rules Are Set to Route Calls to the Opening Greeting" section on page 3-14.

4. On each Cisco Unity server in the dialing domain, enable cross-server live reply and enter the pilot numbers of the destination Cisco Unity servers. See the "Enabling Cross-Server Live Reply and Entering the Pilot Numbers of Destination Cisco Unity Servers" section on page 3-14.

5. Test the cross-server live reply functionality. See the "Testing Cross-Server Live Reply" section on page 3-14.

Note   Subsequently, if a new Cisco Unity server is added to the dialing domain, you will need to add the pilot number of the new server to the Network > Dialing Domain Options page of each Cisco Unity server in the dialing domain.

Procedures: Enabling Cross-Server Live Reply

Verifying That Call Routing Rules Are Set to Route Calls to the Opening Greeting

Do the following procedure on each Cisco Unity server in the dialing domain. For failover systems, do the procedure on both the primary and secondary servers.

To Verify That Call Routing Rules Are Set to Route Calls to the Opening Greeting

Step 1 In the Cisco Unity Administrator, go to the **Call Routing > Direct Calls** page.

Step 2 Verify that calls to the pilot number for the server are routed to the Opening Greeting.

The Default Call Handler routing rule (which cannot be deleted or modified) sends calls to the Opening Greeting. Therefore, if you have not added any routing rules, the server is already set to correctly process cross-server calls.

Enabling Cross-Server Live Reply and Entering the Pilot Numbers of Destination Cisco Unity Servers

Do the following procedure on each Cisco Unity server in the dialing domain. If the system is using failover, do the following procedure on both the primary and secondary server, because most of the settings on the Network > Dialing Domain Options page are stored in the registry. (Registry settings are not replicated to the secondary server.)

To Enable Cross-Server Live Reply and to Enter the Pilot Numbers of Destination Cisco Unity Servers

Step 1 In the Cisco Unity Administrator, go to the **Network > Dialing Domain Options** page.

Step 2 In the Cross-Server Live Reply section, check the **Subscribers Can Call Back a Cisco Unity Subscriber on a Different Cisco Unity Server** check box.

Step 3 In the Pilot Numbers for Cross-Server Logon, Transfer, and Live Reply section, enter the pilot number in the Dial String field for each Cisco Unity server displayed in the table. (Note that the pilot numbers that you enter are stored in the SQL Server database UnityDb on the Cisco Unity server. Therefore, if the system is using failover, the pilot numbers will be replicated to the secondary server.)

Step 4 Check the **Play Prompt During Cross-Server Logon, Transfer, and Live Reply so That Callers Know Something Is Happening** check box. Although playing the "Please wait" prompt is optional, we recommend that you check the box because the cross-server process can take several seconds before the caller is transferred.

Step 5 Click the **Save** icon.

Testing Cross-Server Live Reply

We recommend that you test cross-server transfer before allowing subscribers to use the feature.

For failover systems, first test that the primary destination servers answer cross-server calls. Then manually fail over the destination servers to verify that the secondary server answers cross-server calls. If the destination servers are properly configured for failover, the secondary server should answer cross-server calls when the primary server is unavailable.

To Test Cross-Server Live Reply

Step 1   For each number listed in the Pilot Numbers section on the Network > Dialing Domain Options page, use a phone to call the number and verify that the call is routed to the Opening Greeting of the destination Cisco Unity server.

Step 2   Create a new subscriber account (or use an existing account) on each Cisco Unity server in the dialing domain for testing purposes. Make sure that the test subscribers belong to a class of service in which live reply is enabled, and that call transfers are enabled in the subscriber accounts.

Step 3   Log on as a subscriber on one Cisco Unity server and send a message to the test subscribers on the other Cisco Unity servers.

Step 4   For each subscriber that receives the test message, log on, listen to the message, and choose to call the subscriber. Verify that:

- The "Please wait" prompt is played (if configured to do so).

- The call is transferred to the subscriber phone of the subscriber who left the message.

Troubleshooting

You can use the following tools to troubleshoot problems with cross-server logon, transfer, and live reply, on both the originating and destination Cisco Unity servers:

- The Windows application event logs

- The Port Status Monitor, available in Tools Depot

- The Unity Diagnostic tool, available in Tools Depot. In the Unity Diagnostic tool, enable the following micro traces:

  - CDE: 10 State Machine Trace

  - Conversation: 10 Call Progress

  - MiuCall: All traces

  - MiuGeneral: 12, 13, 14, 16
    (12 Tapi Events, 13 Tone Generation/Detection, 14 Digit Generation/Detection, 16 Event Wait Result)
    For SIP or PIMG integrations, also enable: 20, 21, 22
    (20 Sip Media, 21 Sip Call Control State Machine, and 22 Sip Media State Machine)

  - MiuMethods: All traces

  - For SCCP (skinny) integrations: All Skinny TSP traces.

- When gathering log files in the Unity Diagnostic tool, select the applicable AvCsMgr log file. For SCCP (skinny) integrations, gather the applicable svchost log file.

Dialing Domain Options Page Reference

For information about dialing domain options settings, see the "Dialing Domain Options Page" section in the "Network Settings" chapter of the *Interface Reference Guide for the Cisco Unity Administrator*, available at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Internet Subscribers

See the following sections:

Overview: Internet Subscribers

By creating Internet subscriber accounts, you enable Cisco Unity subscribers to send voice messages to recipients whose computers are connected to the Internet. Messages are sent over the Internet or any TCP/IP network via the Simple Mail Transfer Protocol (SMTP). The recipient receives a voice message as an e-mail with a WAV attachment.

In this chapter, you will find procedures for creating Internet subscriber accounts, followed by detailed discussions of the concepts and terminology you need to understand.

Prerequisites for Setting Up Internet Subscriber Accounts

Before creating the Internet subscriber accounts, verify that the following prerequisites have been met.

- Cisco Unity is already installed on the server(s), and they are connected to the network as applicable for your installation.
- The Exchange servers have been configured as applicable for your installation such that Cisco Unity subscribers can send e-mail to the people who will have Internet subscriber accounts. Cisco Unity hands off messages to Exchange for delivery; therefore, if e-mail is successfully delivered, there should not be a problem with the delivery of voice messages.
- If you will be creating Trusted Internet subscribers, you must first configure at least one Trusted Internet Location, and install the Voice Connector for Exchange 2000 for Trusted Internet Locations.

In installations with multiple Cisco Unity servers networked together via Digital Networking, Internet subscriber accounts can be created on any Cisco Unity server. After the Cisco Unity servers have been set up for Digital Networking as described in the "Digital Networking" chapter, verify the following settings:

- Verify that the addressing search scope is set to either the dialing domain or the global directory on all of the networked servers, so that Cisco Unity subscribers, no matter which server they are associated with, can send messages to Internet subscribers. See the "Setting the Addressing Search Scope" section on page 2-6 for details.

- If you want outside callers to be able to reach Internet subscribers from the automated attendant (for example, from the opening greeting) or from directory assistance:

  – Verify that the Cisco Unity server(s) on which the Internet subscribers will be created are in the same dialing domain as the Cisco Unity server that outside callers call into. See the "Customizing the Primary Location" section on page 2-6 for details on creating the dialing domain, and the "Dialing Domains" section on page 2-15 for background information.

  – Verify that the automated attendant and directory handler(s) search scopes are set to the dialing domain scope. See the "Setting the Directory Handler Search Scope" section on page 2-7 and the "Setting the Automated Attendant Search Scope" section on page 2-7.

Creating Internet Subscriber Accounts

You can create Internet subscriber accounts by using the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator. See the following sections:

- Before Creating Internet Subscriber Accounts, page 4-2
- Before Creating Trusted Internet Subscriber Accounts, page 4-4
- Using the Cisco Unity Bulk Import Wizard to Create Multiple Internet Subscriber Accounts, page 4-6
- Correcting Import Errors, page 4-8
- Using the Cisco Unity Administrator to Create Internet Subscriber Accounts, page 4-9
- Enabling Cross-Server Transfer for Internet Subscribers, page 4-10
- After Creating Internet Subscriber Accounts, page 4-10

Before Creating Internet Subscriber Accounts

This section lists—in order—the issues that you must consider before creating Internet Subscriber accounts.

1. **Cisco Unity Configuration and Permissions**

If you are unsure whether the account that you are using has sufficient rights and permissions to create Internet subscribers, or whether Cisco Unity is properly configured to work with your message store, use the following procedure to run the SysCheck diagnostic tool.

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 check 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 Internet 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 Internet subscriber account is based. Cisco Unity includes predefined classes of service that you can modify. You can also create new classes of service. For details, see the "Managing Classes of Service" chapter in the *System Administration Guide for Cisco Unity*.

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 that you can modify.

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

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 Internet subscriber account is based. For details, see the "Managing Distribution Lists" chapter in the *System Administration Guide for Cisco Unity*.

5.   Subscriber Templates

In the Cisco Unity Administrator, you can specify settings for a group of Internet 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 Internet subscriber accounts as they are created. Cisco Unity comes with a default subscriber template that you can modify, and you can create an unlimited number of additional templates. For more details, see the "Managing Subscriber Templates" chapter in the *System Administration Guide for Cisco Unity*.

Internet subscribers correspond to contacts in Active Directory. The contacts are listed in the address book for Microsoft Outlook (or other e-mail client), unless they are explicitly hidden. You may prefer that the associated contacts do not appear in the Outlook address book at all, or you may want to alter how contacts appear in the Outlook address book.

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

Before Creating Trusted Internet Subscriber Accounts

Before creating Trusted Internet subscriber accounts, you must also consider the following two issues in addition to the issues listed in the "Before Creating Internet Subscriber Accounts" section on page 4-2:

1.   **Trusted Internet Locations**

You must first create as least one Trusted Internet Location.

You can create Trusted Internet delivery locations by using the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard.

To Create Trusted Internet 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, which identifies the location in Cisco Unity, and which subscribers use to blind address messages to recipients at this location.

Step 5   Select **Trusted Internet** as the Destination Type for the location.

Step 6   Click **Add**.

Step 7   Record a voice name for the location.

Step 8   If you are using Secure Messaging, indicate whether to have outgoing messages decrypted.

Step 9   Click the **Save** icon.

If you prefer to create Trusted Internet delivery locations by using the Cisco Unity Bulk Import wizard, see the Cisco Unity Bulk Import wizard Help for instructions.

2.   **Voice Connector for Exchange 2000**

You must install the Voice Connector for Trusted Internet Locations.

Caution   The Voice Connector for Exchange 2000 can be installed on an Exchange 2000 or an Exchange 2003 server, but it cannot be installed on an Exchange 2007 server.

Do the following two procedures in the order listed.

The following procedure is for installing Voice Connector version 12.0(1), which ships with Cisco Unity 5.0(1). We recommend that you first check for a later version of the Voice Connector, and that you install that version instead. Follow the installation instructions in the release notes for the applicable version. To check for a later version, go to the Cisco Unity Voice Connector for Exchange Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity-voice-connector.

To Install the Voice Connector for Exchange 2000

Step 1   Log on to the Exchange server on which you are installing the Voice Connector.

Step 2   Disable any virus-scanning services on the Exchange server.

Step 3   If Cisco Unity is also on the server on which you are installing the Voice Connector, disable the Cisco Security Agent service, if applicable.

Step 4   If you are installing the Voice Connector from a Cisco Unity DVD or CD, insert the disc in the computer, and browse to the **VoiceConnector-Ex2000** directory.

If you downloaded the Voice Connector files from the Software Center website, browse to the directory in which the files were extracted.

Step 5   Double-click **Install.exe**, and click **Next**.

Step 6   On the Voice Connector Setup Wizard Select Components dialog box, check the **Voice Connector for Exchange** check box.

Step 7   If you are setting up secure messaging and if Cisco Unity is not on the Exchange server, check the **Cisco Secure Messaging Service** check box.

Step 8   Click **Next**.

Step 9   On the Welcome screen, click **Next**.

Step 10   On the Confirm SMTP Pickup Directory screen, click **Next**.

Step 11   In the Address Types dialog, check the **Trusted Internet Location** check box.

Step 12   If you are setting up the system to use other networking options, check the check boxes of the applicable address types.

> **Note**   Setting up VPIM Networking also requires the installation of the Transport Event Sink.

Step 13   Click **Next**.

Step 14   On the Confirm Directory dialog box, click **Next** to launch the setup.

Step 15   If you did not check the Cisco Secure Messaging Service check box in Step 7, skip to Step 16. Otherwise, do the following sub-steps in the Cisco Unity Secure Messaging Service Setup wizard:

    a.   On the Welcome screen, click **Next**.

    b.   On the Choose Destination Folder dialog, specify the destination, and click **Next**.

    c.   Optionally, on the Message Security Settings screen, check the **Enable Message Aging** check box, and enter the number of days that encrypted messages should be available. (If the check box is unchecked, Cisco Unity will not limit the number of days that encrypted messages will be available.)

    d.   Click **Next**.

    e.   On the Ready to Install Software screen, click **Install**.

Step 16   When the setup is complete, click **Finish** to exit Setup and restart the server.

Step 17   Enable virus-scanning and the Cisco Security Agent services, if applicable.

To view Voice Connector properties in Exchange System Manager, Windows Script Host version 5.6 or later must be installed on the Exchange server. (Note that if the Exchange server uses an earlier version of Windows Script Host, the Voice Connector functions properly, but you will not be able to view Voice Connector properties in Exchange System Manager.)

To Determine Whether to Update Windows 2000 Script Host

Step 1 On the Exchange server on which the Voice Connector has been installed, browse to **Winnt\System32**.

Step 2 Right-click the file **Wshom.ocx**, and click **Properties**.

Step 3 Click the **Version** tab.

Step 4 In the Item Name list, click **Product Version** to view the version in the Value box.

Step 5 If the version is earlier than 5.6, update Windows Script Host so the Voice Connector properties can be displayed in Exchange System Manager. (Go to the downloads page of the Microsoft website, and do a keyword search for Windows Script Host. Follow the installation instructions.)

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

The Cisco Unity Bulk Import wizard allows you to create multiple Internet subscriber accounts at once by importing user data directly from Active Directory, or 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 the user data contained in the CSV file is formatted correctly, you can use it to create new Active Directory contacts at the same time that you create Internet subscriber accounts. Alternatively, the Cisco Unity Bulk Import wizard allows you to use a CSV file to create Internet Subscriber accounts with existing Active Directory contact data.

To create Internet subscriber accounts by importing user data directly from Active Directory, see the "To Create Internet Subscriber Accounts by Using the Cisco Unity Bulk Import Wizard" procedure on page 4-7. Otherwise, use the following "To Prepare a CSV File for Creating Internet Subscriber Accounts" procedure to prepare your CSV file. See the Cisco Unity Bulk Import wizard Help to find additional information about using the wizard to create Internet subscriber accounts, or about the required and optional column headers for your CSV file.

To Prepare a CSV File for Creating Internet Subscriber Accounts

Step 1 Save the data that 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 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 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.

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 a 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, and then by the remote address:

Abade,Alex,aabade@cisco.com
Bader,Kelly,kbader@cisco.com
Campbell,Terry,tcampbell@cisco.com
Cho,Li,lcho@cisco.com

> **Note**   The example in this procedure illustrates how to set up a CSV file so that the Cisco Unity Bulk Import wizard creates Internet subscriber accounts and new Active Directory contacts at the same time. If you choose to create new Internet subscriber accounts with data on existing Active Directory contacts, you must also include the ALIAS column header and data in your CSV file. Also note that to create Trusted Internet subscriber accounts, last name, first name, DTMF access ID, and remote address fields are required.

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,REMOTE_ADDRESS

For Trusted Internet subscribers, the headers should be spelled as follows:

LAST_NAME,FIRST_NAME,DTMF_ACCESS_ID,REMOTE_ADDRESS

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 each optional column header.
- Any data that includes a space, quotes, or commas is contained within quotes.

Step 7 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 8 Confirm that each row contains the applicable data corresponding to each column header.

Step 9 Save the file as a CSV file.

Step 10 Continue with the following "To Create Internet Subscriber Accounts by Using the Cisco Unity Bulk Import Wizard" procedure.

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

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. See the Cisco Unity Bulk Import wizard Help for procedures.

Step 1 On the Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Bulk Import**.

Step 2 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 3   When prompted to choose the type of subscriber to create, click **Internet** or **Trusted Internet**, as applicable.

Step 4   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 for details.

Step 5   When the Internet Subscriber accounts are created, click **Finish**.

Step 6   If you had import errors, but in you chose to correct them later, see the .

Step 7   If you had no import errors, or if all errors have now been corrected, see the .

Correcting Import Errors

The error log file contains data that the Cisco Unity Bulk Import wizard could not import. The Cisco Unity Bulk Import wizard reports the first error it detects in any user mailbox or row in a CSV file. Once you correct that error, the wizard may detect additional errors in the same mailbox or 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, use one of the following procedures:

-
-

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

Step 1   Browse to the directory location of the error log file that 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 that 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 8   Repeat this procedure until all Internet subscriber accounts are created without error, and then proceed to the "After Creating Internet Subscriber Accounts" section on page 4-10.

To Correct Errors That Occurred When Importing Data from the Directory

Step 1   Browse to the directory location of the error log file that 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   Open Active Directory Users and Computers.

Step 4   Double-click a contact that contains an error to see the properties.

Step 5   Enter corrections in the applicable boxes in the contact.

Step 6   Click **OK**.

Step 7   Repeat Step 4 through Step 6 for each contact listed in the error log file.

Step 8   Run the Cisco Unity Bulk Import wizard again.

Step 9   Repeat this procedure until all Internet subscriber accounts are created without error, and then proceed to the "After Creating Internet Subscriber Accounts" section on page 4-10.

Using the Cisco Unity Administrator to Create Internet Subscriber Accounts

By using the Cisco Unity Administrator, you can create an Internet subscriber account by adding a new account, or by importing existing data for an Active Directory contact. When you add a new Internet subscriber account, Cisco Unity creates a contact in Active Directory.

To create an Internet subscriber account, do one of the following procedures:

- To Create an Internet Subscriber Account by Adding a New Contact, page 4-9
- To Create an Internet Subscriber Account by Importing Existing User Data, page 4-10

To Create an Internet Subscriber Account by Adding a New Contact

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

Step 2   Click the **Add** icon.

Step 3   Click **New Subscriber**, and then select **Internet** or **Trusted Internet** from the list.

Step 4   Enter the First Name and Last Name.

Step 5   Enter the Extension of the Internet subscriber on Cisco Unity. This is the number that other Cisco Unity subscribers will use when addressing a message to the Internet subscriber that you are about to create.

Step 6   Select the Subscriber Template to use.

Step 7   Enter the SMTP Address in the applicable format.

Step 8   If you are creating a Trusted Internet subscriber, select a Trusted Internet location.

Step 9   Click **Add**.

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

To Create an Internet Subscriber Account by Importing Existing User Data

---

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

Step 2 Click the **Add** icon.

Step 3 Select **Import Existing Exchange User**.

Step 4 Click **Select**.

Step 5 Select **Internet**.

Step 6 In the Find By list, indicate whether to search by first name, last name, or Exchange alias. You can also indicate the domain for the search.

Step 7 Enter the applicable name or alias. You also can enter ***** to display a list of all users, or enter one or more characters followed by ***** to narrow your search.

Step 8 Click **Find**.

Step 9 On the list of matches, click the name of the user to import.

Step 10 Enter the applicable information on the Add Subscriber page.

Step 11 Click **Add**.

Step 12 On the subscriber record, customize settings as applicable, and then click the **Save** icon.

Enabling Cross-Server Transfer for Internet Subscribers

By default, call transfers to Internet subscribers that are 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. Optionally, you can configure Cisco Unity to use the cross-server transfer settings when transferring calls to Internet subscribers homed on a different Cisco Unity server. For more information about cross-server transfers, see the "Cross-Server Transfer from the Automated Attendant and Directory Handlers" section on page 3-8. If you already have cross-server transfer configured, see the "Optional: Enabling Cross-Server Transfer for External Subscribers" section on page 3-10 for details on expanding the cross-server transfer functionality to include Internet subscribers.

After Creating Internet Subscriber Accounts

After creating Internet subscriber accounts, consider the following:

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

- You can make changes to the settings for individual Internet subscriber accounts in the Cisco Unity Administrator.

- When you want to modify settings for multiple subscribers at once, you can (re)run the Cisco Unity Bulk Import wizard. To learn more, see 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 Internet subscriber account. See the "Deleting Internet Subscribers" section on page 4-12 for details.

Internet Subscriber Concepts and Definitions

Internet subscribers are a representation in Cisco Unity of users who do not have mailboxes on the local Exchange network. Instead, messages for Internet subscribers are sent to an e-mail address that you specify when you create the Internet subscriber account. The recipient receives voice messages as e-mails with attached WAV files.

Trusted Internet subscribers are Internet subscribers that are trusted with decrypted secure messages. Trusted Internet subscribers must be associated with a Trusted Internet Location. Based on the security settings of the Trusted Internet location, secure messages to Trusted Internet subscribers are decrypted by the Cisco Unity Voice Connector for Microsoft Exchange before they are sent by the Exchange server. (Messages to regular Internet subscribers are sent directly by the Exchange server and cannot be decrypted and therefore cannot be played by the recipient.)

Trusted Internet subscribers are the same as Internet subscribers except the following differences:

- Trusted Internet subscribers are associated with a Trusted Internet location.
- Messages to Trusted Internet subscribers are processed by the Voice Connector.
- Trusted Internet subscribers must have a DTMF extension, whereas extensions are optional for Internet subscribers.

The concepts discussed in this section apply to both regular Internet subscribers and Trusted Internet subscribers, except where specifically noted.

Internet subscribers are represented as mail-enabled contacts in Active Directory. You create and manage Internet subscriber accounts in much the same way that you do regular subscriber accounts. For example, a subscriber template is used when the Internet subscriber accounts are created, and you can adjust the call transfer settings for Internet subscriber accounts as needed.

Extensions are optional for Internet subscribers whereas they are mandatory for regular subscribers and Trusted Internet subscribers. If an Internet subscriber has not been assigned an extension, subscribers can address messages to that Internet subscriber only in spelled-name mode (if the Internet subscriber has a voice name). Subscribers can also address messages to Internet subscribers without extensions by using Cisco Unity ViewMail for Microsoft Outlook or by using the Cisco Unity Inbox.

If you have specified extensions for the Internet subscribers, you can configure the call transfer settings for the Internet subscribers so that they can be reached by outside callers.

Internet subscribers do not require additional Exchange 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 Internet subscribers.

Other than receiving messages (and possibly calls), Internet subscribers do not have access to other Cisco Unity features, and some sections of the Cisco Unity Administrator are disabled for Internet subscribers. Internet 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, so their recorded names and greetings can only be recorded or changed in the Cisco Unity Administrator.
- Cannot use Cisco Unity ViewMail for Microsoft Outlook or the Cisco Unity Inbox.

- Cannot own private lists.
- Cannot set up or receive message notifications.
- Cannot receive message waiting indications.

Subscriber Experience with Internet Subscribers

Provided that Internet subscribers have extensions, are listed in the phone directory, and have had voice names and greetings recorded for them:

- Subscribers can address messages to Internet subscribers by using the phone, ViewMail, or the Cisco Unity Inbox.
- Contacts that correspond to Internet subscribers are included in Exchange address lists, which means that they are listed in the Outlook address book (unless the contact has been explicitly prevented from appearing there) and the Cisco Unity Inbox address book. Therefore, message addressing to Internet subscribers—either by using Outlook or the Cisco Unity Inbox—is the same as for regular subscribers.
- When using the phone, subscribers can address messages to Internet subscribers by spelled-name mode (if enabled on the system) or by extension or alternate extension.
- Subscribers get voice name confirmation when addressing a message to an Internet subscriber.
- Internet subscribers can be added to distribution lists.
- You can configure call transfer settings for the Internet subscribers just as you can for Cisco Unity subscribers so that unidentified callers and subscribers can call an Internet subscriber and leave a message.

Extensions are optional for Internet subscribers whereas they are mandatory for regular subscribers. If an Internet subscriber has not been assigned an extension:

- The Internet subscriber cannot be listed in the phone directory.
- Unidentified callers will be unable to leave messages for the Internet subscriber.
- When addressing messages to the Internet subscriber, subscribers are limited to spelled-name mode, provided that the Internet subscriber has a recorded voice name. If neither an extension nor a voice name has been set, messages cannot be addressed to the Internet subscriber.

Deleting Internet Subscribers

Each Internet subscriber is associated with an Active Directory contact. When you delete Internet subscribers in the Cisco Unity Administrator, you are offered the option to delete the associated directory objects.

AMIS Networking

Overview: AMIS

Cisco Unity supports the Audio Messaging Interchange Specification analog (AMIS-a) protocol, which provides a mechanism for transferring voice messages between different voice messaging systems.

AMIS Networking is a licensed feature. If your organization has multiple Cisco Unity servers networked together by using Cisco Unity Digital Networking (and, therefore, accessing subscriber data in the same directory), only one server in the Digital Network needs to be licensed and configured for AMIS Networking. The Cisco Unity server that is configured for AMIS Networking is referred to as the bridgehead server. For more information about obtaining licenses for Cisco Unity features, see the applicable *Licensing for Cisco Unity* white paper, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

To use AMIS Networking, you must choose the applicable options when you run the Cisco Unity Permissions wizard. For detailed information, see the Permissions wizard Help, which is available in Tools Depot on the Cisco Unity server.

In this chapter, you will find procedures for setting up AMIS Networking, followed by detailed discussions of the concepts and terminology that you need to understand. See the following sections:

Setting Up Cisco Unity to Use AMIS

See the following sections:

- Considerations for Deploying AMIS with Cisco Unified Communications Manager and Cisco Gateways, page 5-3
- Task List: Setting Up Cisco Unity to Use AMIS, page 5-3

Prerequisites

Before starting the setup, verify that the following prerequisites have been met.

- Cisco Unity is already installed on the server(s), and they are connected to the network as applicable to your installation.

- A license file with an AMIS license has been obtained and installed on the Cisco Unity bridgehead server.

- Cisco Unity meets the requirements as described in the "AMIS Networking Requirements" section of the *Networking Options Requirements for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

- The voice messaging system with which Cisco Unity will be networked meets the requirements listed in the "Support Policy for AMIS Voice Messaging Systems" section of the *Supported Hardware and Software, and Support Policies for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

- Verify that the Cisco Unity call routing rules route calls to a call handler, such as the Opening Greeting. (This is the default when Cisco Unity is initially installed.)

For installations with multiple Cisco Unity servers that access the same directory, you should first set up the servers for Digital Networking as described in the "Digital Networking" chapter before setting up AMIS Networking. After the Cisco Unity servers have been set up for Digital Networking, verify the following settings:

- Verify that the addressing search scope is set to either the dialing domain or the global directory on all of the networked servers so that Cisco Unity subscribers, no matter which server they are associated with, can address messages to AMIS delivery locations and/or AMIS subscribers. See the "Setting the Addressing Search Scope" section on page 2-6 for details.

- If you want outside callers to be able to reach AMIS subscribers from the automated attendant (for example, from the opening greeting) or directory assistance:

    - Verify that the Cisco Unity server(s) on which the AMIS subscribers will be created are in the same dialing domain as the Cisco Unity server that outside callers call into. See the "Customizing the Primary Location" section on page 5-12 for details on creating the dialing domain, and the "Dialing Domains" section on page 2-15 for background information.

    - Verify that the automated attendant and directory handler(s) search scopes are set to the dialing domain scope. See the "Setting the Directory Handler Search Scope" section on page 2-7 and the "Setting the Automated Attendant Search Scope" section on page 2-7.

Considerations for Deploying AMIS with Cisco Unified Communications Manager and Cisco Gateways

In a Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) environment where AMIS calls may traverse one or more Cisco gateways or routers, we recommend that customers (or their systems integration partners) test the interoperability of such gateways with Cisco Unity before the products are deployed. Consider the following when deploying AMIS:

- Call forwarding, call waiting or other tones can sometimes interfere with transmission of DTMF sequences.
- Where applicable for Cisco Unified CM and gateways, set DTMF duration and interdigit timing to 100 milliseconds.

Task List: Setting Up Cisco Unity to Use AMIS

Use this task list to set up Cisco Unity to use AMIS. The cross-references take you to detailed procedures for the setup.

1. Install the Voice Connector on an Exchange server. See the "Setting Up the Voice Connector for AMIS Networking" section on page 5-4.

Do the Following Tasks on Each Cisco Unity Server That Is Licensed for AMIS

2. During Cisco Unity installation, when you ran the Cisco Unity Permissions wizard to grant the necessary permissions to the installation and service accounts, if you did not check the Set Permissions Required by AMIS, Cisco Unity Bridge, and VPIM check box on the Choose Whether to Enable Voice Messaging Interoperability page, do the following steps:

   a. Log on to a Cisco Unity server that is licensed for AMIS by using an account that:

   – Is a member of the Domain Admins group in the domain that the Cisco Unity server belongs to, or that has permissions equivalent to the default permissions for the Domain Admins group.

   – Is either an Exchange Full Administrator or a member of the Domain Admins group in the domain that contains all of the domains from which you want to import Cisco Unity subscribers.

   b. Re-run the Permissions wizard, and follow the on-screen prompts until the Choose Whether to Enable Voice Messaging Interoperability page appears.

   c. Check the Set Permissions Required by AMIS, Cisco Unity Bridge, and VPIM check box.

   d. Follow the on-screen prompts to complete the Permissions wizard.

   e. If you have more than one Cisco Unity server that is licensed for AMIS, repeat Step a. through Step d. on each server that is licensed for AMIS.

   For more information on running the Permissions wizard, see the Permissions wizard Help, PWHelp_<language>.htm, in the directory where the Permissions wizard is installed.

   If you do not know whether you checked the check box, run the Permissions wizard in report mode. For more information, see the Report Mode Help, PWReportHelp_<language>.htm, in the directory where the Permissions wizard is installed.

3. Create the UAmis account. See the "Creating the UAmis Account" section on page 5-8.

4. Designate voice ports for outbound AMIS calls. See the "Designating Voice Ports for Outbound AMIS Calls" section on page 5-11.

5. Set the AMIS delivery options. See the "Setting AMIS Delivery Options" section on page 5-11.

6. Customize the AMIS Restriction Table as needed. See the "Customizing the AMIS Restriction Table" section on page 5-11.

7. Set up the AMIS schedule. See the "Setting Up the AMIS Schedule" section on page 5-12.

8. Customize the primary location profile settings. See the "Customizing the Primary Location" section on page 5-12.

9. Create a delivery location for each remote voice messaging system. See the "Creating AMIS Delivery Locations" section on page 5-13.

10. Optionally, create AMIS subscribers. See the "Creating AMIS Subscribers" section on page 5-16.

11. Optionally, extend identified subscriber messaging to include AMIS subscribers. See the "Extending Identified Subscriber Messaging to Include AMIS Subscribers" section on page 5-22.

12. Optionally, enable cross-server transfers for AMIS subscribers. See the "Enabling Cross-Server Transfer for AMIS Subscribers" section on page 5-24.

Finish the Setup

13. Set up the other voice messaging system for AMIS. The other voice messaging system will require the number to dial into Cisco Unity, and the Node ID that was entered on the primary location.

14. Test the setup to verify that Cisco Unity can exchange messages with the other voice messaging system. Optionally, you can configure the macro trace "Basic Incoming and Outgoing AMIS Message" in the Unity Diagnostic tool (on the Windows Start menu, click Programs > Cisco Unity > Unity Diagnostic Tool) to verify that Cisco Unity can send and receive AMIS messages.

Procedures for Setting Up Cisco Unity to Use AMIS

This section contains all of the procedures necessary to set up Cisco Unity to use AMIS. Consult the "Task List: Setting Up Cisco Unity to Use AMIS" section on page 5-3 for information on the order in which the procedures must be completed.

Setting Up the Voice Connector for AMIS Networking

The Voice Connector installation program is included on Cisco Unity DVD 1 and CD 1. Voice Connector for Exchange 2000 version 11.0(1) or later can be installed on either an Exchange 2000 or an Exchange 2003 server.

The Voice Connector installation program does not prompt with a choice of languages for the installation; it always installs in English. To run the Voice Connector installation program by using one of the localized versions (FRA, DEU, or JPN) instead of English, see the "Running the Voice Connector Setup Program in Another Language" section on page 5-42.

Setting Up the Voice Connector for Exchange 2000

Install the Voice Connector on any Exchange 2000 or Exchange 2003 server that is not part of an Exchange cluster (Microsoft does not support third-party connectors on an Exchange cluster server). Although the Voice Connector can be installed on the Cisco Unity server (when Exchange is also on the server), this is not recommended for performance reasons.

⚠️
Caution   Installing the Voice Connector on an Exchange 2007 server is not supported.

If the Exchange server on which the Voice Connector will be installed is in a different routing group than the Exchange servers on which Cisco Unity subscribers are homed, routing group connectors must be configured between the routing groups.

The Voice Connector service is automatically configured to log on as the account that is associated with the Exchange server on which the Voice Connector is installed (sometimes referred to as the "Local System" account). The account that the service logs on as should not be changed.

⚠️
Caution   Do not change the default permissions for the Local System account. In addition, do not change the permissions granted to Exchange administrative groups during Exchange installation. The Voice Connector logs on using that account, and if you change permissions, the Voice Connector may not function properly.

The following procedures are for installing Voice Connector version 12.0(1), which ships with Cisco Unity 5.0(1). We recommend that you first check for a later version of the Voice Connector, and that you install that version instead. Follow the installation instructions in the release notes for the applicable version. To check for a later version, go to the Cisco Unity Voice Connector for Exchange Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity-voice-connector.

To Install the Voice Connector for Exchange 2000

As a best practice, back up the Exchange server before installing the Voice Connector.

Step 1   Uninstall any previous versions of the Voice Connector. See the "Uninstalling the Cisco Unity Voice Connector" section on page 10-4.

Step 2   Log on to the Exchange server on which you are installing the Voice Connector.

Step 3   Disable any virus-scanning services on the Exchange server.

Step 4   If Cisco Unity is also on the server on which you are installing the Voice Connector, disable the Cisco Security Agent service, if applicable.

Step 5   If you are installing the Voice Connector from a Cisco Unity DVD 1, insert the disc in the computer, and browse to the **VoiceConnector-Ex2000** directory.

    If you downloaded the Voice Connector files from the Software Center website, browse to the directory in which the files were extracted.

Step 6   Double-click **Install.exe**, and click **Next**.

Step 7   On the Voice Connector Setup Wizard Select Components dialog box, check the **Voice Connector for Exchange** check box.

Step 8   If you are setting up secure messaging and if Cisco Unity is not on the Exchange server, check the **Cisco Secure Messaging Service** check box.

Step 9   Click **Next**.

Step 10   On the Welcome screen, click **Next**.

Step 11   On the Confirm SMTP Pickup Directory screen, click **Next**.

Step 12   In the Address Types dialog, check the **AMIS** check box.

Step 13   If you are setting up the system to use other networking options, check the check boxes of the applicable address types.

✏️
Note   Setting up VPIM Networking also requires the installation of the Transport Event Sink.

Step 14 Click **Next**.

Step 15 On the Confirm Directory dialog box, click **Next** to launch the setup.

Step 16 If you did not check the Cisco Secure Messaging Service check box in Step 7, skip to Step 17. Otherwise, do the following sub-steps in the Cisco Unity Secure Messaging Service Setup wizard:

    a. On the Welcome screen, click **Next**.

    b. On the Choose Destination Folder dialog, specify the destination, and click **Next**.

    c. Optionally, on the Message Security Settings screen, check the **Enable Message Aging** check box, and enter the number of days that encrypted messages should be available. (If the check box is not checked, Cisco Unity will not limit the number of days that encrypted messages will be available.)

    d. Click **Next**.

    e. On the Ready to Install Software screen, click **Install**.

Step 17 When the setup is complete, click **Finish** to exit Setup and restart the server.

Step 18 Enable virus-scanning and the Cisco Security Agent services, if applicable.

In order to view Voice Connector properties in Exchange System Manager, Microsoft Windows Script Host version 5.6 or later must be installed on the Exchange server. Continue with the following "To Determine if the Microsoft Windows Script Host Should Be Updated" procedure. (Also note that if the Exchange server uses an earlier version of Windows Script Host, the Voice Connector will function properly, but you will not be able to view Voice Connector properties in the Exchange System Manager.)

To Determine if the Microsoft Windows Script Host Should Be Updated

Step 1 On the Exchange server on which the Voice Connector has been installed, browse to **Winnt\System32**.

Step 2 Right-click the file **Wshom.ocx**, and click **Properties**.

Step 3 Click the **Version** tab.

Step 4 In the Item Name list, click **Product Version** to view the version in the Value box.

If the version is earlier than 5.6, update Windows Script Host so the Voice Connector properties can be displayed in Exchange System Manager. (Go to the downloads page of the Microsoft website, and do a keyword search for Windows Script Host. Follow the installation instructions.)

To Verify the Voice Connector for Exchange 2000 Installation

To verify that the Voice Connector for Exchange 2000 installed properly, verify that the Voice Connector service is running, and that the Voice Connector mailbox has been created.

Step 1 Open the Services applet on the Exchange server on which the Voice Connector is installed. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 2 Verify that the Status for the Exchange 2000 Voice Connector (<Server name>) service is **Started**, and that the Startup Type is set to **Automatic**.

Step 3 Exit the **Services** applet.

Step 4 Open Exchange System Manager on the Exchange server on which the Voice Connector is installed. (On the Windows Start menu, click **Programs > Microsoft Exchange > Exchange System Manager**.)

Step 5   In the tree in the left pane, expand the **Servers** container. If the organization properties at the top of the tree have been set such that administrative groups are displayed in the tree, the Servers container is nested within the administrative group container.

Step 6   Within the Servers container, expand the **<Server name>\<Storage group>\Mailbox Store (<Server name>)** container for the server on which the Voice Connector is installed.

Step 7   In the expanded tree, click **Mailboxes**.

In the right pane, you should see the mailbox for "Exchange 2000 Voice Connector (<Server name>)" or "AvExchangeIVC_<Server name>." (The name changes from "AvExchangeIVC_<Server name>" to "Exchange 2000 Voice Connector (<Server name>)" after you run Cleanup Agent.)

Step 8   Exit **Exchange System Manager**.

Controlling What Happens to Messages That Cannot Be Delivered

When the Voice Connector encounters a message that cannot be delivered, and the sender information is incomplete or incorrect such that a nondelivery receipt (NDR) cannot be sent to the message sender, the Voice Connector saves the message in the Archive folder in the Voice Connector mailbox. The Archive folder is accessible only when using tools available from Microsoft. If you want more control over archived messages, you can add to the registry either the AliasToForwardBadMailsTo value or the DeleteArchiveFolderMessages value (but not both).

When you add the AliasToForwardBadMailsTo registry value and set it to the SMTP address of a user or distribution list, when the Voice Connector encounters a problematic message, information about the message is sent to the specified address instead of being saved in the Archive folder. When a problematic AMIS message is encountered, the informational message that the Voice Connector sends to the specified user (or distribution list) includes the MIME header of the problematic message as a text attachment. The MIME header contains the "To" and "From" addresses, which may help in troubleshooting the problem.

When you add the DeleteArchiveFolderMessages registry value and set it to 1, the Voice Connector continues to save problematic messages in the Archive folder, but periodically, the Voice Connector automatically deletes the messages in the Archive folder.

When a message is saved to the Archive folder or sent to the address specified in the AliasToForwardBadMailsTo registry value, an entry is made in the Voice Connector log file. (The information is logged when the Voice Connector properties are set to the default logging level or a higher logging level.) The Voice Connector logs are located on the Exchange server on which the Voice Connector is installed in the directory <ExchangeServerPath>\VoiceGateway\LogFiles. The files are named in the format GwIvc_<YyMmDd >.log, where Yy in the year, Mm is the month, and Dd is the day.

To add the registry values, do the following procedure.

To Control What Happens to Messages That Cannot Be Delivered

Step 1   On the Exchange server on which the Voice Connector is installed, start Regedit.

⚠
Caution   Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (See the "Restoring" topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

Step 2   If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 3   Expand the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Active Voice\AvIvc

Step 4   If you want information about the messages to be sent to a user or distribution list instead of being saved to the Archive folder, do the following sub-steps. Otherwise, skip to Step 5.

    a.   On the Edit menu, click **New > String Value**.

    b.   Enter **AliasToForwardBadMailsTo** as the value name.

    c.   Double-click **AliasToForwardBadMailsTo**.

    d.   In the Edit String dialog box, enter the SMTP address of the recipient (for example unityadministrator@company.com). This must be the SMTP address of a user, contact, or distribution list object in Exchange. An e-mail with the failed message and information about the message will be sent to this address.

    e.   Click **OK**.

    f.   Exit Regedit.

    g.   Skip to Step 6.

Step 5   If you want messages that are saved in the Archive folder to be automatically deleted, do the following sub-steps:

    a.   On the Edit menu, click **New > DWORD** Value.

    b.   Enter **DeleteArchiveFolderMessages** as the value name.

    c.   Double-click **DeleteArchiveFolderMessages**.

    d.   In the Edit DWORD dialog box, enter **1**.

    e.   Click **OK**.

    f.   Exit Regedit

Step 6   Open the Services MMC on the Exchange server on which the Voice Connector is installed. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 7   Right-click **Exchange 2000 Voice Connector (<Server name>)**, and click **Restart**.

Step 8   Exit the Services MMC.

Creating the UAmis Account

In installations with multiple Cisco Unity servers networked together via Digital Networking, ConfigMgr.exe, the utility that creates the UAmis account, needs to be run only on the Cisco Unity server(s) licensed for AMIS.

Do one of the following two procedures, depending on whether the partner Exchange server is running Exchange 2000/2003 or Exchange 2007:

To Create the UAmis Account When the Partner Exchange Server Is Running Exchange 2000 or Exchange 2003

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 **ConfigMgr.exe**. The ConfigMgr dialog box appears.

Step 3   Click **Create and Configure AMIS Account and Mailbox**.

Step 4   Click **OK** on the dialog box that displays when the UAmis account is successfully configured.

Step 5   Click **Exit** to close ConfigMgr.

Step 6   On the Cisco Unity server, start the Services tool. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 7   Right-click **AvNotifierMgr**, and select **Restart**. The CPU usage on the Cisco Unity server will spike for a few minutes while the AvNotifierMgr reinitializes connections with subscriber mailboxes.

Step 8   Close the Services tool.

To Create the UAmis Account When the Partner Exchange Server Is Running Exchange 2007

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 **ConfigMgr.exe**. The ConfigMgr dialog box appears.

Step 3   Click **Create and Configure AMIS Account and Mailbox**.

Step 4   In the Create the PowerShell Script That Creates the UAmis Account and Mailbox dialog box, choose the path and file name for the script that will create the UAmis account.

You must run the script on the partner server or another server on which Exchange Management Shell is installed, so choose one of the following locations to save the script:

   • The server that you will run the script on.

   • A network location that is accessible to that server.

   • A removeable disk.

Step 5   Click **Create Script**.

Step 6   Click **OK**.

Step 7   Click **Exit** to close ConfigMgr.

Step 8   Log on to the Exchange 2007 server on which you want to run the script by using an account that has the right to run a PowerShell script.

Step 9   If necessary, copy the script locally to the Exchange server.

Step 10   Run **Exchange Management Shell**. (From the Start menu, click **All Program > Microsoft Exchange Server 2007 > Exchange Management Shell**.)

Step 11   Run the script. In the Exchange Management Shell window, enter the full pathname of script. For example:

   d:\scripts\UAmis_<ServerName>.PS1

Alternatively, you can change to the directory where the script is located by using the "cd" command, and then run the script by entering:

.\UAmis_<ServerName>.PS1

For more information, refer to Microsoft documentation.

Step 12   On the Cisco Unity server, browse to the directory in which Cisco Unity is installed (the default location is C:\CommServer).

Step 13   Double-click **ConfigMgr.exe**. The ConfigMgr dialog box appears.

Step 14   Click **Create and Configure AMIS Account and Mailbox** to complete the configuration.

Step 15   Click **OK**.

Step 16   Click **Exit** to close ConfigMgr.

Step 17   On the Cisco Unity server, start the Services tool. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 18   Right-click **AvNotifierMgr**, and select **Restart**. The CPU usage on the Cisco Unity server will spike for a few minutes while the AvNotifierMgr reinitializes connections with subscriber mailboxes.

Step 19   Close the **Services** tool.

To Verify That the UAmis Account Was Created When the Partner Exchange Server Is Running Exchange 2000 or Exchange 2003

If the partner Exchange server is running Exchange 2007, do the "To Verify That the UAmis Account Was Created When the Partner Exchange Server Is Running Exchange 2007" procedure on page 5-10.

The mailbox for the UAmis account is located on the partner Exchange server, which is the Exchange server that was selected in the Message Store Configuration wizard during Cisco Unity setup.

Step 1   Open **Exchange System Manager** on the partner Exchange server.

Step 2   In the tree control in the left pane, expand the **Servers > <ExchangeServerName>** container (where <ExchangeServerName> is the name of the partner Exchange server).

Depending on your installation, the Servers container may be nested within an administrative group and a site container.

Step 3   Expand **<Storage Group> > Mailbox Store (<ExchangeServerName>) > Mailboxes**.

Step 4   Verify that **UAmis_<ServerName>** is in the list of mailboxes in the right pane.

Step 5   Close **Exchange System Manager**.

To Verify That the UAmis Account Was Created When the Partner Exchange Server Is Running Exchange 2007

Step 1   Open Exchange Management Console on the partner Exchange server.

Step 2   In the tree control in the left pane, expand **Recipient Configuration**, and click **Mailbox**.

Step 3   Verify that **UAmis_<ServerName>** is in the list of mailboxes in the right pane.

Step 4   Close **Exchange Management Console**.

Designating Voice Ports for Outbound AMIS Calls

In installations with multiple Cisco Unity servers networked together via Digital Networking, designate voice ports for AMIS calls only on those Cisco Unity server(s) that are licensed for AMIS. See the "Port Usage and Schedules" section on page 5-26 for guidelines on configuring the ports.

To Designate Voice Ports for Outbound AMIS Calls

Step 1   In the Cisco Unity Administrator, go to the **Systems > Ports** page.

Step 2   Designate which ports to use for outgoing AMIS calls.

Step 3   Click the **Save** icon.

Setting AMIS Delivery Options

The AMIS delivery option settings control attributes of outgoing AMIS calls on the Cisco Unity server.

In installations with multiple Cisco Unity servers networked together, set the AMIS delivery options only on those Cisco Unity server(s) that are licensed for AMIS.

To Set AMIS Delivery Options

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

Step 2   Select either the Default AMIS restriction table or another restriction table to use as the Local Dial Restriction Table.

The Local Dial Restriction Table and the AMIS schedule together determine when outgoing AMIS calls are made.

Step 3   Set the other AMIS delivery options as needed.

Step 4   Click the **Save** icon.

Customizing the AMIS Restriction Table

By default, the AMIS restriction table allows all delivery numbers; however, you can customize the restriction table as needed. The AMIS restriction table and the AMIS schedule together determine when outgoing AMIS calls are made. If a delivery number for an outgoing AMIS message is allowed by the AMIS restriction table, the message is sent immediately—the schedule settings do not apply. If the delivery number is not allowed by the AMIS restriction table, the schedule determines when the message is sent.

In installations with multiple Cisco Unity servers networked together, customize the AMIS restriction table only on those Cisco Unity server(s) that are licensed for AMIS.

To Customize the AMIS Restriction Table

Step 1   In the Cisco Unity Administrator, go to any **Call Management > Restriction Tables** page.

Step 2   Click the **Find** icon.

Step 3   Double-click the AMIS restriction, which by default is named {Default AMIS}.

> **Note**   The AMIS restriction table is specified on the Network > AMIS Options > Delivery Options page in the Local Dial Restriction Table field.

Step 4   As applicable for your installation, do one or more of the following:

- To add a dial string, click **Add Dial String** and enter settings for the new dial string as applicable.

- To delete a dial string, click the dial string number in the table in the bottom portion of the Restriction Tables page, and then click **Remove Dial String**.

- To modify a dial string, click the dial string number in the table in the bottom portion of the Restriction Tables page, and change settings as applicable.

Step 5   Click the **Save** icon.

Setting Up the AMIS Schedule

Set up the AMIS schedule for messages that are not allowed by the AMIS restriction table.

In installations with multiple Cisco Unity servers networked together, set up the AMIS schedule only on those Cisco Unity server(s) that are licensed for AMIS.

To Set Up the AMIS Schedule

Step 1   In the Cisco Unity Administrator, go to the **Network > AMIS Options > Schedule** page.

Step 2   Click boxes on the schedule grid to set the active and inactive half hours. To avoid clicking the same blocks for more than one day, use the Copy Day's Schedule box to copy the settings from one day to other days.

Step 3   Click the **Save** icon.

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. In installations with multiple Cisco Unity servers networked via Digital Networking, you enter the AMIS node ID for the primary location only on the Cisco Unity Bridgehead server (the field is displayed only on the Cisco Unity servers licensed for AMIS.)

For detailed information about the settings, see the .

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 AMIS subscribers, enter a dialing domain name.

- If your installation consists of multiple Cisco Unity servers that are 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 dialing domain names that are 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   Enter the numbers for the Node ID, which is transmitted by Cisco Unity to identify itself to other voice messaging systems during outgoing AMIS calls. The Country Code and Area Code fields can be left blank; however, the Phone Number field is mandatory.

Step 7   Click the **Save** icon.

Creating AMIS Delivery Locations

Create an AMIS delivery location on the bridgehead Cisco Unity server for each remote voice messaging system to which subscribers will send messages. If Cisco Unity will be messaging with a large number of voice messaging systems, 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 voice messaging systems for which delivery locations have been configured, you can create the rest of the delivery locations.

Carefully consider the Dial ID that you will assign to the delivery location. See the "Guidelines for Assigning Dial IDs and Extensions" section on page 9-2 for detailed information about choosing a Dial ID.

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

- Using the Cisco Unity Administrator to Create AMIS Delivery Locations, page 5-13
- Using the Cisco Unity Bulk Import Wizard to Create AMIS Delivery Locations, page 5-14
- Modifying Existing Delivery Locations by Using the Cisco Unity Bulk Import Wizard, page 5-16

Using the Cisco Unity Administrator to Create AMIS Delivery Locations

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

To Create AMIS 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 **AMIS** as the Destination Type for the location.

Step 6   Click **Add**.

Step 7   Record a voice name for the location.

Step 8   Enter the Delivery Phone Number. This is the number that Cisco Unity dials to connect to the remote voice messaging system for outgoing AMIS messages.

Step 9   Enter the numbers for the Node ID, which is used to identify the remote voice messaging system that corresponds to this delivery location. This Node ID must match the Node ID that the corresponding remote voice messaging system transmits during incoming calls. If desired, the Country Code and Area Code fields may be left blank; however, the Phone Number field is mandatory.

Step 10   In the Outgoing Messages to This Location field, select the applicable option:

- **Do Not Decrypt Messages**—The Voice Connector will not decrypt or send secure messages and will send an NDR back to the sender.

- **Decrypt Non-Private Messages**—The Voice Connector will not decrypt or send secure messages that are flagged as private. An NDR will be sent back to the sender. All other messages will be decrypted before sending them to the remote location.

- **Decrypt All Messages**—The Voice Connector will decrypt all secure messages before sending them to the remote location. Depending on the configuration at the remote location, the message may or may not be re-encrypted before being delivered to the recipient.

Step 11   Click the **Save** icon.

Using the Cisco Unity Bulk Import Wizard to Create AMIS 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—see the Cisco Unity Bulk Import wizard Help.

To Prepare a CSV File for Creating AMIS 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, DELIVERY_PHONE_NUMBER

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

Although the Cisco Unity Bulk Import wizard does not require that you provide the AMIS_NODE_ID column in the CSV file, we recommend that you add the column with the Node ID data to the CSV file.

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

- Confirm that every 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   Every 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 AMIS Delivery Locations by Using the Cisco Unity Bulk Import Wizard" procedure.

To Create AMIS 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 **AMIS**, 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\AMIS_Locations.csv, the default output file will be C:\Temp\AMIS_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\AMIS_Locations.csv, the default output file will be C:\Temp\AMIS_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 AMIS Subscribers

You may prefer to begin by creating only a few AMIS subscribers for testing purposes, until you verify that Cisco Unity and the remote system can successfully exchange messages. After you have confirmed that messaging between Cisco Unity and the remote system is working correctly, you can finish creating the AMIS subscribers. Note that the AMIS subscribers must be created on the same Cisco Unity server as the AMIS delivery locations.

You can create AMIS subscriber accounts by using the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator. See the following sections:

- Before Creating AMIS Subscriber Accounts, page 5-17
- Using the Cisco Unity Bulk Import Wizard to Create Multiple AMIS Subscriber Accounts, page 5-18
- Using the Cisco Unity Administrator to Create AMIS Subscriber Accounts, page 5-21
- After Creating AMIS Subscriber Accounts, page 5-22

Before Creating AMIS Subscriber Accounts

This section lists—in order—the issues that you must consider before creating AMIS subscriber accounts. AMIS 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 AMIS 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 AMIS subscribers, or whether Cisco Unity is properly configured to work with your message store, do 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 check 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 AMIS 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 that you can modify. You can also create new classes of service. For details, see the "Managing Classes of Service" chapter in the *System Administration Guide for Cisco Unity*.

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 that you can modify.

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

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, see the "Managing Distribution Lists" chapter in the *System Administration Guide for Cisco Unity*.

Public distribution lists correspond to distribution groups in Active Directory. The distribution lists are listed in the address book for Microsoft Outlook (or other e-mail client), unless they are explicitly hidden. To help prevent others from sending e-mail to AMIS subscribers, you may want to create lists that contain only AMIS subscribers, and then hide these distribution lists from the Outlook address book. The option to hide distribution lists is available on the Subscribers > Public Distribution Lists > Profile page in the Cisco Unity Administrator.

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 that you can modify, and you can create an unlimited number of additional templates. For more details, see the "Managing Subscriber Templates" chapter in the *System Administration Guide for Cisco Unity*.

AMIS subscribers correspond to contacts in Active Directory. The contacts are listed in the address book for Microsoft Outlook (or other e-mail client), unless they are explicitly hidden. You may prefer that the associated contacts do not appear in the Outlook address book at all, or you may want to alter how contacts appear in the Outlook address book. See the "Determining How AMIS Subscribers Appear in the Outlook Address Book" section on page 5-34 for details.

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

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

The Cisco Unity Bulk Import wizard allows you to create multiple subscriber accounts 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.

As long as the user data contained in the CSV file is formatted correctly, you can use it to create new contacts in Active Directory at the same time that you create subscriber accounts. Alternatively, the Cisco Unity Bulk Import wizard allows you to use a CSV file to create subscriber accounts with existing Active Directory contact data.

If you choose to create subscriber accounts with existing contact data, note that the e-mail addresses for the imported contacts are overwritten with extension addresses 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 "To Prepare a CSV File for Creating AMIS Subscriber Accounts" 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—see the Cisco Unity Bulk Import wizard Help.

To Prepare a CSV File for Creating AMIS Subscriber Accounts

Step 1   Save the data that 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 that 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 extension (DTMF_ACCESS_ID), and then by the remote mailbox number (REMOTE_USER_ID):

Abade,Alex,2001,3000
Bader,Kelly,2002,3100
Campbell,Terry,2003,3200
Cho,Li,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,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 contacts at the same time. If you choose to create new subscriber accounts with existing contact data, you must also include the ALIAS column header 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 AMIS 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   To help prevent others from sending e-mail to AMIS subscribers, you may want to include the HIDE_IN_ADDRESS_BOOK column header, and enter a 1 (one) in each row of subscriber data.

A value of 1 indicates that subscribers will be hidden from the e-mail address book; a value of 0 indicates that subscribers will be displayed.

Step 9   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 10   Confirm that every row contains the appropriate data corresponding to each column header.

Step 11   Save the file as a CSV file.

Step 12   Continue with the following "To Create AMIS Subscriber Accounts by Using the Cisco Unity Bulk Import Wizard" procedure.

To Create AMIS 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. See 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 **AMIS**.

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 5-21 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 5-21.

Step 8   If you had no import errors, or if all errors have now been corrected, see the "After Creating AMIS Subscriber Accounts" section on page 5-22.

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 "To Correct Errors That Occurred When Importing Data from a CSV File" 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 AMIS Subscriber Accounts" section on page 5-22.

Using the Cisco Unity Administrator to Create AMIS Subscriber Accounts

By using the Cisco Unity Administrator, you can create AMIS subscriber accounts one at a time. When you add a new AMIS subscriber account, Cisco Unity creates a contact in Active Directory.

To create an AMIS subscriber account, do the following "To Add a New AMIS Subscriber by Using the Cisco Unity Administrator" procedure.

To Add a New AMIS 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 **AMIS** from the list.

Step 4   Enter the First Name and Last Name.

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

After Creating AMIS Subscriber Accounts

After creating AMIS 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.

- 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, see 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 AMIS Subscribers" section on page 5-34 for details.

Extending Identified Subscriber Messaging to Include AMIS Subscribers

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

- Installations with Multiple Cisco Unity Servers Networked via Digital Networking, page 5-22
- Single-Server Installations, page 5-23

Installations with Multiple Cisco Unity Servers Networked via Digital Networking

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

- The Cisco Unity servers must be connected to the same phone system or phone system network as described in the "Dialing Domains" section on page 2-15.

- The servers must be configured to be in the same dialing domain, as described in the "Customizing the Primary Location" section on page 5-12.

- 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 2-7.

- The applicable permissions on each server must be set, as described in the "Setting Permissions on Active Directory Containers That Are Used for Importing Subscribers" section on page 5-23.

- Identified subscriber messaging on each server must be enabled as described in the "Enabling Identified Subscriber Messaging" section on page 5-24.
- Identified subscriber messaging on each server must be extended for AMIS subscribers as described in the "Extending Identified Subscriber Messaging" section on page 5-24.

Single-Server Installations

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

- The server must be configured with a dialing domain name, as described in the "Customizing the Primary Location" section on page 5-12.
- The applicable permissions must be set, as described in the "Setting Permissions on Active Directory Containers That Are Used for Importing Subscribers" section on page 5-23.
- Identified subscriber messaging must be enabled as described in the "Enabling Identified Subscriber Messaging" section on page 5-24.
- Identified subscriber messaging must be extended for AMIS subscribers as described in the "Extending Identified Subscriber Messaging" section on page 5-24.

Setting Permissions on Active Directory Containers That Are Used for Importing Subscribers

If you will be importing contacts from two or more containers (for all of the Cisco Unity servers combined), the Cisco Unity message store services account on each Cisco Unity server must be granted SendAs permission on every container from which contacts will be imported on every Cisco Unity server in the forest. Otherwise, identified subscriber messaging may not work between Cisco Unity servers. For example, if CiscoUnityServer1 will import contacts from Container1 and Container2, and if CiscoUnityServer2 will import contacts from Container3 and Container4, Cisco Unity message store services account on each Cisco Unity server must have SendAs permission for all four containers.

To Set the Applicable Permissions

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, expand **Administration Tools**.

Step 3 Double-click **Permissions Wizard**.

Step 4 Do the following:

- Choose the same Active Directory account for the Cisco Unity message store services account:
  - Click **Next** without changing any options until you arrive at the Choose the Cisco Unity Message Store Services Account page.
  - Choose the same Active Directory account for the Cisco Unity message store services account on every Cisco Unity server.
- Choose the applicable containers:
  - Click **Next** without changing any options until you arrive at the Choose Active Directory Containers for Import page.
  - Choose all of the containers from which users will be imported for every Cisco Unity server in the forest.

Step 5 Click **Next** without changing any options until you complete the wizard.

Step 6   Repeat Step 1 through Step 5 on each Cisco Unity in the forest.

Enabling Identified Subscriber Messaging

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 **Disable Identified Subscriber Messaging** 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 AMIS 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 Cross-Server Transfer for AMIS Subscribers

By default, call transfers to AMIS subscribers that are 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. Optionally, you can configure Cisco Unity to use the cross-server transfer settings when transferring calls to AMIS subscribers who are homed on a different Cisco Unity server. For more information about cross-server transfers, see the "Cross-Server Transfer from the Automated Attendant and Directory Handlers" section on page 3-8. If

you already have cross-server transfer configured, see the "Optional: Enabling Cross-Server Transfer for External Subscribers" section on page 3-10 for details on expanding the cross-server transfer functionality to include AMIS subscribers.

AMIS Concepts and Definitions

The following sections explain AMIS concepts in detail:

Introduction to AMIS

In AMIS terminology, 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. The node that places an AMIS call and delivers messages is called the originating node. The node that answers the AMIS call and receives messages is called the destination node. If a particular system acts as both an originating node and a destination node, its Node ID is the same for both functions. AMIS nodes correspond to locations in Cisco Unity.

The Cisco Unity subscribers and the users on the other voice messaging systems are identified by mailbox numbers. On Cisco Unity, the mailbox number for a subscriber is the same as the subscriber extension.

Voice messages are transmitted between nodes by using ordinary phone connections. When one node calls another by dialing a specified delivery phone number, the originating node transmits its Node ID by using a sequence of touchtones. 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 applicable mailbox. For detailed information about the touchtones that are transmitted during an AMIS call, see the *AMIS Analog Networking Definitions* white paper, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

In compliance with the AMIS protocol, Cisco Unity batches outgoing messages by node, with a maximum of nine messages per batch. If there are more than nine messages for a particular node, Cisco Unity ends the AMIS session after sending the ninth message, hangs up for a brief period of time, and then redials the node to send the next batch of messages.

The AMIS protocol specifies that a message be a maximum of eight minutes long. During an AMIS transmission, before playing a message, the originating node sends to the destination node the length of the message. If the message is too long, the destination node may refuse the message and skip to the next message. However, some voice messaging systems will accept longer messages. If the voice messaging system refuses the message, a non-delivery receipt (NDR) is returned to the sender. If a subscriber sends a message that is longer than eight minutes, Cisco Unity will attempt to transmit it. In addition, Cisco Unity may accept messages longer than eight minutes. For each incoming message, Cisco Unity checks the space available in the subscriber mailbox and the Maximum Message Length setting on the Subscriber > Messages page to determine whether to accept the message.

Incoming AMIS messages to Cisco Unity are delivered to subscriber mailboxes only, and cannot be delivered to public distribution lists. Additionally, incoming messages must be addressed to the primary extension of the subscriber; messages addressed to an alternate extension will not be delivered. See the for additional information.

Note that for incoming AMIS calls, the initial "handshake" between the originating system and Cisco Unity must take place in a call handler, such as the Opening Greeting call handler. For AMIS Networking to be properly configured, you need to ensure that all incoming AMIS calls are routed to a call handler. When Cisco Unity is initially installed, the default setting is for the call routing table to route calls to the Opening Greeting call handler; thus it is properly configured for AMIS Networking. If the call routing table has been modified after installation, you need to make sure that a rule is in place in your call routing table to route any incoming AMIS calls to a call handler.

Port Usage and Schedules

In the Cisco Unity Telephony Integration Manager (UTIM) and in the Cisco Unity Administrator on the System > Ports page, you can designate which ports on your system are used for outgoing AMIS calls. All ports are used for incoming AMIS calls.

AMIS transmissions can be lengthy and thus tie up ports on your Cisco Unity server. For example, 10 hours of AMIS messages take at least 10 hours of port time to transmit. A 2-minute message that is sent to a public distribution list that contains 200 AMIS recipients results in 200 messages in the outbound queue, and would require at least 6.5 hours of port time to transmit.

When multiple ports have been designated for outgoing AMIS messages, Cisco Unity uses all designated ports as message traffic warrants. The total number of ports used is limited by the availability of ports that have been designated for outgoing AMIS calls. For example, if there are 10 ports available for outgoing AMIS messages, and 10 hours of messages to deliver, all 10 ports are used for message delivery, and the time to transmit all of the messages will be about one hour plus the time it takes to place the calls and establish the AMIS sessions.

Outbound messages are sorted according to their destination, and then batched into groups of 9. If there are multiple destinations, multiple ports are used to transmit the messages. If there are numerous messages to one destination, each batch of messages (with a maximum of nine per batch) is transmitted on a different port, if one is available. In other words, if you have multiple ports designated for AMIS message delivery, multiple ports will be used to handle the messages to a single node, as needed. As the number of messages for a particular node increases, an additional port is added when the number of

outgoing messages reaches a multiple of nine. For example, one port will be used for message delivery if there are nine or fewer messages to a node. For 10–18 messages, two ports will be used. For 19–27 messages, three ports will be used, and so on.

After a port starts an AMIS session, it continues sending messages as long as there are messages to be sent. The port disconnects only when there are no more outgoing messages, or after it sends the ninth message to the same node. In this case, the port disconnects briefly, and then continues sending messages if there are more messages that need to be sent.

Because the transmission of outgoing AMIS messages can tie up voice ports for long periods of time, you may want to adjust the schedule so that outgoing AMIS calls are placed during closed hours or at times when Cisco Unity is not processing many calls. Additionally, if most or all of your AMIS delivery numbers are long distance, you may want to schedule the outgoing AMIS calls when the long distance phone rates are lower. Keep in mind, however, that outgoing messages are queued up in the UAmis mailbox, so there must be sufficient storage available if you restrict the delivery window.

You can override the AMIS schedule so that messages that are marked urgent are sent immediately. Additionally, by setting up a restriction table, you can specify which delivery numbers are sent immediately and which numbers must wait for the AMIS schedule to become active.

If you adjust the AMIS schedule so that outgoing AMIS calls are made only after normal business hours, be sure to inform subscribers. They may choose to contact users on the other voice messaging system directly, or send e-mail, rather than send a voice message that will not be delivered immediately.

If your schedule is such that outbound AMIS calls are placed during normal business hours or when call volumes are heavy, you may want to dedicate certain ports exclusively for incoming calls and other ports exclusively for TRAP. By excluding AMIS outbound calls from those ports, you ensure that there will be ports available for calls of a time-sensitive nature. Use the Ports Usage Analyzer, available in Tools Depot, to monitor traffic for a few days and then adjust the ports as needed.

When Cisco Unity has an outbound AMIS call to make, it searches backwards for a port to use, starting with the last port (which is the highest numbered port), until it finds an available port that is configured for outbound AMIS calls. In dual-switch integrations, Cisco Unity starts the search for an available port with the last port in the last integration (again, this is the highest numbered port).

In organizations with multiple Cisco Unity servers networked together, you can set up a "bridgehead" Cisco Unity server to handle all AMIS calls—both inbound and outbound—for all of the Cisco Unity servers in the network. This way, the ports on just one Cisco Unity server are used for AMIS messages.

UAmis Account

Outgoing AMIS messages are placed in a special Exchange mailbox called UAmis_<Server name>. Before AMIS messages can be transmitted, you must create the UAmis account.

The mailbox for the UAmis account is located on the partner Exchange server, which is the Exchange server that was selected in the Message Store Configuration wizard during Cisco Unity setup.

The storage limits for the UAmis mailbox are set to the limits that are defined for the mailbox store in which the UAmis mailbox is created. Although you can change the storage limits for the UAmis mailbox by using the Exchange administration application, do so with caution. If the UAmis mailbox is full, subsequent outgoing messages cannot be delivered, and the sender receives a NDR.

Consider the following when determining whether limits should be set on the UAmis mailbox:

- If the AMIS dialing restrictions and schedule are configured such that AMIS messages are delivered only during specified periods of the day, messages are queued up in the UAmis mailbox. The storage limit must be high enough to store all AMIS messages during the non-delivery periods.

- There could be times during the day when the number of AMIS messages spikes. The storage limit must be high enough to handle this.

- If hard disk space on the Exchange server is limited, you may want to set a limit to ensure that available space is not exceeded.

You may want to monitor the outgoing AMIS message traffic by running the AMIS Out Traffic Report before setting limits on the UAmis mailbox. For more information, see the "AMIS Out Traffic Report" section in the "Reports" chapter of the *Maintenance Guide for Cisco Unity*. The *Maintenance Guide for Cisco Unity* is available at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

The UAmis mailbox can be moved and deleted just like any other Exchange mailbox, by using standard Microsoft tools. Be sure to let anyone who administers Active Directory and Exchange know about the UAmis account so that it is not moved or deleted by mistake. To avoid inadvertently moving or deleting the UAmis account, consider changing the Exchange display name so that the account is more clearly identified to you or the Exchange administrator as requiring "special" treatment. You can also hide the UAmis account so that it does not appear in the Outlook address book.

For information on moving the UAmis mailbox, see the "UAmis Mailbox" section in the "Cisco Unity Data and Log Files" chapter of the *Maintenance Guide for Cisco Unity*, at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Messages are sent from the UAmis mailbox at one or more of the following times:

- When a message is marked urgent, and the AMIS delivery option settings allow urgent messages to be sent immediately.

- When the AMIS restriction table allows the delivery number of a message.

- When the AMIS schedule becomes active.

Messages that have not been sent when the schedule becomes inactive remain in the UAmis mailbox until the schedule becomes active again. An error is logged in the Windows Application Event log when messages remain in the UAmis mailbox for more than 24 hours. See the "Maintenance" section on page 5-40 for information about monitoring the UAmis mailbox.

In organizations with multiple Cisco Unity servers networked together, the UAmis account needs to be created only on those Cisco Unity servers that will place and receive AMIS calls. See the "Considerations for Networked Cisco Unity Servers" section on page 5-38 for more information.

Voice Connector and AMIS Networking

The Voice Connector allows Cisco Unity to send and receive AMIS messages. When subscribers use the phone to address a message to an AMIS recipient, Cisco Unity constructs an address with the form AMIS:<Location Dial ID>_<Remote Mailbox> for the message. The Voice Connector is registered with Exchange to handle messages with the AMIS address type. For an outbound message to an AMIS recipient, the Voice Connector transforms the message properties and delivers the message to the UAmis mailbox. For installations with multiple Cisco Unity servers that are licensed for AMIS, the Voice Connector delivers the message to the UAmis mailbox that is associated with the Cisco Unity server on which the AMIS location or AMIS subscriber was created.

Install the Voice Connector for Exchange 2000. See the "Setting Up the Voice Connector for AMIS Networking" section on page 5-4 for information about setting up the Voice Connector.

The Voice Connector for Exchange 2000 version 11.0(1) or later can be installed on either an Exchange 2000 or Exchange 2003 server.

Installing the Voice Connector on an Exchange 2007 server is not supported.

Locations and AMIS Networking

Central to how you set up AMIS is a Cisco Unity object called a 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. When setting up AMIS, you give the primary location a new name and a Dial ID (which is an identifier for the location within Cisco Unity), enter the AMIS Node ID, and customize other properties as applicable. The AMIS Node ID on the primary location is transmitted on all outgoing AMIS calls and identifies your Cisco Unity system to the destination nodes. See the "Primary Location Profile Settings" section on page 9-1 for details about the settings.

You create a delivery location in Cisco Unity to correspond to each remote voice messaging system with which Cisco Unity communicates. Delivery locations contain the information that Cisco Unity needs to exchange messages with other nodes—the Delivery Phone Number and the AMIS Node ID.

In organizations with multiple Cisco Unity servers networked together, the delivery locations should be created only on those Cisco Unity servers that are licensed for AMIS. See the "Considerations for Networked Cisco Unity Servers" section on page 5-38 for more information.

Message Addressing Options

Cisco Unity provides the following message addressing options:

- Blind addressing—Allows Cisco Unity subscribers to send messages to subscribers on the remote voice messaging system even though the recipient mailbox number, name, and recorded name are not in the directory. Even though Cisco Unity cannot provide voice name confirmation (hence the term "blind addressing"), the message is addressed and sent. See the "Blind Addressing and AMIS Networking" section on page 5-30 for more information.

- AMIS subscribers—Allows Cisco Unity subscribers to get voice name confirmation when addressing messages to subscribers on the remote voice messaging system. AMIS subscribers are a representation in Cisco Unity of the subscribers on the remote messaging system. AMIS subscribers are created in Cisco Unity to enable Cisco Unity subscribers to find them in the directory and send messages to them as they would with any other subscriber. See the "AMIS Subscribers" section on page 5-31 for more information.

Message Addressing Limitations

Subscribers can use the Cisco Unity phone conversation (also known as the telephone user interface, or TUI), Cisco Unity ViewMail for Microsoft Outlook, or the Cisco Unity Inbox to reply to and forward AMIS messages just as they do with regular voice messages. However, when sending or retrieving AMIS messages, subscribers will encounter the following limitations:

- AMIS messages that are marked urgent when they are sent are not marked urgent when they are retrieved by the recipient.

- AMIS messages that are marked private when they are sent are not marked private when they are retrieved by the recipient.

- Requests for return receipts on AMIS messages are not honored.

- E-mail messages cannot be sent to AMIS recipients even though ViewMail allows subscribers to address them. Instead of being delivered, e-mail messages that are sent to AMIS recipients are returned to the sender as NDRs.

- Messages that are sent from AMIS subscribers to Cisco Unity subscribers cannot be encrypted and therefore are not affected by the message aging functionality of Secure Messaging.

Blind Addressing and AMIS Networking

AMIS blind addressing is one of the methods that Cisco Unity provides for addressing AMIS messages to users of another voice messaging system. Blind addressing allows Cisco Unity subscribers to send messages to subscribers on the remote voice messaging system even though the recipient mailbox number, name, and recorded name are not in the directory. Even though Cisco Unity cannot provide voice name confirmation (hence the term "blind addressing"), the message is addressed and sent.

One of the steps to setting up blind addressing is adjusting the Blind Addressing setting on the Primary Location > Addressing Options page. You also create a delivery location that corresponds to each voice messaging system with which Cisco Unity communicates.

You provide the following information for each delivery location:

- Delivery Phone Number—The number that Cisco Unity dials to reach the other voice messaging system.

- AMIS Node ID—The number that is used by Cisco Unity to identify the remote voice messaging system during an AMIS transmission. For incoming calls, Cisco Unity searches the AMIS delivery locations for an AMIS Node ID that matches the value transmitted by the originating node. If a corresponding location is not found, Cisco Unity follows the AMIS protocol and rejects the call without recording messages.

- Dial ID—A unique number that identifies the location to Cisco Unity. This is the number that subscribers dial when blind addressing messages to individuals who use the remote voice messaging system.

When blind addressing a message, subscribers dial a number that is made up of the delivery location Dial ID and the mailbox number of the recipient. Before addressing the message, Cisco Unity parses the number that the subscriber entered and searches for a matching delivery location. If Cisco Unity does not find a matching location, it reports the error to the sender and does not address the message. 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 that a voice name was recorded for the delivery location).

Because your Cisco Unity server does not have access to the names and extensions of the users on the other voice messaging system, subscribers cannot use spelling mode when blind addressing a message to someone on the other system.

Subscribers can also address voice messages in ViewMail for Outlook and in the Cisco Unity Inbox to someone on the remote voice messaging system by using the following format: [AMIS:<Location Dial ID>_<Remote Mailbox>]. For example, to send a message to Dial ID 206, mailbox 555, the address is: [AMIS:206_555]; the brackets must be included in the address.

For administrators of Cisco Unity, blind addressing is the option that requires the least amount of work to set up. However, subscribers will encounter some limitations when blind addressing messages to users on the other voice messaging system. Subscribers can address the message only by using number mode, so they must know the delivery location Dial ID and the mailbox number for the recipient. Additionally, 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.

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.

Note that when you delete a delivery location, blind addressees at that location are also removed from all private lists. Consider notifying subscribers of these potential changes to their private lists.

In organizations with multiple Cisco Unity servers networked together, when subscribers use blind addressing to address messages to someone at an AMIS location, the AMIS transmission originates from the Cisco Unity server on which the AMIS delivery location was created. See the "Considerations for Networked Cisco Unity Servers" section on page 5-38 for more information.

AMIS Subscribers

AMIS subscribers are a representation in Cisco Unity of the subscribers on the 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 with any other subscriber. Voice messages that are addressed to AMIS subscribers are sent to the voice messaging system that they use.

AMIS subscribers do not require additional Exchange 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 AMIS subscribers.

To set up AMIS subscribers, you first create an AMIS delivery location that corresponds to each remote voice messaging system with which Cisco Unity communicates. After creating the delivery location(s), you create an AMIS subscriber account for each remote user. When creating each AMIS subscriber account, you specify the user mailbox number on the other voice messaging system and select the AMIS delivery location with which the AMIS subscriber is associated. Cisco Unity uses the Delivery Phone Number and AMIS Node ID from the associated delivery location when delivering messages to the AMIS subscriber.

In organizations with more than one Cisco Unity server licensed for AMIS, AMIS subscribers can be associated only with AMIS delivery locations that are created on the same Cisco Unity server that the AMIS subscribers will be created on. When subscribers address messages to an AMIS subscriber, the AMIS transmission originates from the Cisco Unity server on which the AMIS subscriber was created. See the "Considerations for Networked Cisco Unity Servers" section on page 5-38 for more information.

AMIS subscribers in Cisco Unity are represented as contacts in Active Directory. When you delete AMIS subscribers in the Cisco Unity Administrator, the underlying contacts are removed automatically.

You create and manage AMIS subscriber accounts in much the same way that you do regular subscriber accounts. You can use the Cisco Unity Administrator to create, modify, and delete AMIS subscriber accounts one at a time, and you can use the Cisco Unity Bulk Import wizard to create and modify multiple AMIS subscriber accounts.

Extensions are mandatory for AMIS subscriber accounts. The extension, which must be unique across the dialing domain, is the number that Cisco Unity subscribers dial when addressing a message to an AMIS subscriber. This number may or may not be the same as the mailbox number of the subscriber on the remote voice messaging system. Callers who reach the opening greeting of your organization can dial the extension of an AMIS subscriber or look up an AMIS subscriber in directory assistance and leave a message.

Other than receiving messages, AMIS subscribers do not have access to other Cisco Unity features, and some sections of the Cisco Unity Administrator are disabled for AMIS subscribers. AMIS 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, so their recorded names and greetings can only be recorded or changed in the Cisco Unity Administrator. However, AMIS subscriber voice names can be imported by using the Cisco Unity Bulk Import wizard. See the Cisco Unity Bulk Import wizard Help for details.

- Cannot use the Cisco Unity Inbox to check messages.
- Cannot own private lists.
- Cannot set up or receive message notifications.
- Cannot receive message waiting indications.

Setting up AMIS subscribers requires more overhead for administrators of Cisco Unity than AMIS blind addressing does. However, the AMIS subscriber option allows other subscribers to address messages to AMIS subscribers the same way that they address messages to regular subscribers.

Subscriber Experience with AMIS Subscribers

Provided that AMIS subscribers are listed in the phone directory and have had voice names and greetings recorded for them:

- Subscribers can address messages to AMIS subscribers by using the phone, ViewMail for Outlook, or the Cisco Unity Inbox.
- Contacts that correspond to AMIS subscribers are included in Exchange address lists, which means that they are listed in the Outlook address book (unless the contact has been explicitly prevented from appearing there) and the Cisco Unity Inbox address book. Therefore, message addressing to AMIS subscribers—either by using Outlook or the Cisco Unity Inbox—is the same as for regular subscribers.
- When using the phone, subscribers can address messages to AMIS subscribers in spelled-name mode (if enabled on the system) or by extension.
- Subscribers get voice name confirmation when addressing a message to a AMIS subscriber.
- When subscribers use the phone to listen to messages, the conversation announces who the message is from.
- AMIS subscribers can be added to public and private distribution lists.

Note that when Cisco Unity records a message from an unidentified caller for an AMIS subscriber, the Dial ID of the primary location is used as the sending mailbox. Although AMIS subscribers are not prevented from replying to these messages, the replies are returned to the Unity Messaging System mailbox as NDRs.

Identified Subscriber Messaging

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. 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), Cisco Unity identifies 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.

Live Reply to AMIS Subscribers

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 who are listening to messages by phone can reply to a subscriber message by choosing the "call the subscriber" option to have Cisco Unity call the subscriber directly. Note that subscriber 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 AMIS 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 AMIS subscribers.

Note that a live reply to an AMIS 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 AMIS subscriber have accounts on the same Cisco Unity server. On a release to switch transfer, Cisco Unity dials the call transfer number that is configured for the AMIS subscriber and hangs up, leaving the phone system to handle the call. Note the following limitations with release to switch transfers:

- The AMIS 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 AMIS 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 AMIS subscribers is enabled automatically, and cannot be disabled.

- Live replies to AMIS 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 an AMIS subscriber with a subscriber account on another Cisco Unity server, the servers must be in the same dialing domain.

Deleting AMIS Subscribers

Each AMIS subscriber is associated with an Active Directory contact. When you delete AMIS subscribers in the Cisco Unity Administrator by deleting the subscriber accounts individually, the underlying directory objects are automatically deleted. To delete all of the AMIS subscribers that are associated with a delivery location, the underlying contacts for those subscribers, and the delivery location itself, use the Global Subscriber Manager, available in Tools Depot.

Note that when you delete an AMIS delivery location, blind addressees are also removed from all private lists. Consider notifying subscribers of these potential changes to their private lists.

Extension Addresses

When you create an AMIS subscriber, Cisco Unity automatically generates an e-mail address in the following format:

AMIS:<Location Dial ID>_<Remote Mailbox>

This special e-mail address is referred to as an extension address (or a remote address). The extension address is a combination of the delivery location Dial ID with which the AMIS subscriber is associated, and the Remote Mailbox Number of the AMIS subscriber. Each contact in Active Directory that corresponds to an AMIS subscriber contains an extension address.

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

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

Determining How AMIS Subscribers Appear in the Outlook Address Book

Depending on your installation, the users of the remote voice messaging system may already have Active Directory accounts and Exchange mailboxes on your local network that they use for e-mail. Therefore, when AMIS subscriber accounts are created for them, the Exchange address lists will contain duplicate listings—the existing user account that is used for e-mail and a new contact that is used only for voice mail. Both listings are included in the Outlook address book. This means that people may inadvertently send e-mail messages to the contact, which should be used only for addressing voice messages.

To discourage people from inadvertently sending e-mail messages to AMIS subscribers, you can prevent the associated contact from appearing in the Outlook address book. Alternatively, you can change how the display name for the contact appears in the Outlook address book so that subscribers can distinguish

the contact from a user account. In this way, you can reduce the number of e-mail messages inadvertently sent to contacts and simplify addressing for those who send voice messages to AMIS subscribers at the same time.

If you prefer that the associated contacts for subscribers do not appear in the Outlook address book at all, see the "Preventing Contacts From Appearing in the Outlook Address Book" section on page 5-35.

Alternatively, if you want to alter how contacts appear in the Outlook address book, see the "Modifying How Contacts Appear in the Outlook Address Book" section on page 5-35.

Preventing Contacts From Appearing in the Outlook Address Book

Either before or after you create AMIS subscriber accounts, you can prevent the associated contact from appearing in the Outlook address book by hiding the contacts from Exchange address lists. When you do so, Exchange will still deliver e-mail messages that are addressed to an existing user account (if one exists) and to the contact. However, the number of e-mail messages that are sent to the contact may be reduced because subscribers cannot inadvertently pick the contact from the Outlook address book when addressing messages to them.

To prevent subscribers from appearing in Outlook address books, you can use the Cisco Unity Administrator, the Cisco Unity Bulk Import wizard, Bulk Edit, or Active Directory Users and Computers:

To do so in the Cisco Unity Administrator, uncheck the Show Subscriber In E-Mail Server Address Book check box on the Profile page for the subscriber template that you plan to use when creating AMIS subscribers, or on individual subscriber Profile pages after you have created the subscriber accounts.

To do so by using the Cisco Unity Bulk Import wizard or the Bulk Edit utility, see the Help for each tool.

To do so in Active Directory Users and Computers, click View > Advanced Features to see the Exchange Advanced property page for a user, and then check the Hide From Exchange Address Lists check box on the Exchange Advanced tab.

Modifying How Contacts Appear in the Outlook Address Book

As an alternative to preventing a contact from appearing in the Outlook address book altogether, you may want to alter the display name for the contact so that subscribers can distinguish the contact from the user account. For example, you could append " - Voice mail" to the display name of each AMIS subscriber, and the names would appear in the Outlook 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 AMIS subscribers. Additionally, when subscribers use the Outlook address book to address a message to a contact, they can be confident that the address is formatted correctly.

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 "To Prevent Subscribers From Adding Individual Subscribers to Private Lists in the Cisco Unity Assistant" procedure to prevent all subscribers that are associated with the Cisco Unity server from adding individual subscribers to their private lists in the Cisco Unity Assistant. When the change has been made, 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.)

> **Note** This 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**.

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

Step 6 Click **Exit**.

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

Migrating Subscribers from Another Voice Messaging System to Cisco Unity

If you are using AMIS to migrate from another voice messaging system to Cisco Unity, there are several tools that you can use to create Cisco Unity subscribers from AMIS subscriber information.

See the following sections for more information:

- Migrating Subscribers in Bulk, page 5-37
- Migrating Subscribers One at a Time, page 5-37
- Private List Considerations for Migrating Subscribers, page 5-38

Migrating Subscribers in Bulk

Following are the general steps for migrating AMIS subscribers to Cisco Unity subscribers in bulk. See the Help files of each of the tools for more information. (Click the Tools Depot icon on the Cisco Unity server, and click the applicable tool in the left pane to view the Help file.)

1. As a best practice, back up the Cisco Unity server before proceeding.

2. If the voice names of the subscribers on the remote system were recorded in a standard format that can be played on the Cisco Unity server (such as G.711 or G.729a), copy the WAV files to the Cisco Unity server. The Cisco Unity Bulk Import wizard will import the voice names.

3. Run Subscriber Information Dump from Tools Depot, and output the AMIS subscriber information to a CSV file.

4. Modify the output CSV file as needed so that you can use it as the input file when you create Cisco Unity subscribers by using the Cisco Unity Bulk Import wizard.

5. Run Global Subscriber Manager from Tools Depot to delete the AMIS delivery locations and associated AMIS subscribers and underlying contacts.

6. If the former AMIS subscribers do not already have Active Directory accounts, create the accounts. In addition, if the former AMIS subscribers did not use Exchange for e-mail, create Exchange mailboxes for them. Alternatively, you can let the Cisco Unity Bulk Import wizard create the accounts and mailboxes.

7. Run the Cisco Unity Bulk Import wizard by using the input file that you prepared in Step 4.

Migrating Subscribers One at a Time

If you have set up AMIS subscriber accounts for the subscribers on another voice messaging system, and if they have existing Exchange mailboxes, you may want to use the Migrate Subscriber Data utility when the time comes to migrate them to Cisco Unity. The Migrate Subscriber Data utility creates a Cisco Unity subscriber account by combining the Cisco Unity-specific data from an existing AMIS subscriber account (such as the voice name) with an existing mail user. The utility then deletes the AMIS subscriber account and the associated Active Directory contact.

The Migrate Subscriber Data utility is available in Tools Depot on the Cisco Unity server. See the Help file that comes with the utility for more information.

Private List Considerations for Migrating Subscribers

When you migrate AMIS subscribers, consider notifying Cisco Unity subscribers of these potential effects on private distribution list membership:

- When you delete a delivery location, blind addressees are removed from all private lists.

- When an AMIS subscriber becomes a regular subscriber, the AMIS subscriber is removed from all private lists.

Considerations for Networked Cisco Unity Servers

In organizations with multiple Cisco Unity servers networked together, when subscribers address messages to an AMIS delivery location (by using blind addressing) or to an AMIS subscriber, the AMIS transmission originates from the Cisco Unity server on which the AMIS delivery location was created. (Note that AMIS subscribers are always created on the same Cisco Unity server as their associated AMIS delivery locations.)

When subscribers address a message to someone on the remote voice messaging system, the Voice Connector delivers the message to the UAmis mailbox that is associated with the Cisco Unity server on which the addressed AMIS delivery location was created. The AMIS schedule and the AMIS delivery options on the pertinent Cisco Unity server are applied.

Only one Cisco Unity server in the network needs to be licensed and set up for AMIS. If allowed by the primary location addressing options, all subscribers, no matter which Cisco Unity server they are associated with, can send messages to an AMIS delivery location or to an AMIS subscriber. The Cisco Unity server that is configured for AMIS acts as the AMIS "bridgehead" server for the other Cisco Unity servers in the network. For example, in Figure 5-1, there are three Cisco Unity servers in the network, but Unity 2 is the only server licensed and configured for AMIS. Unity 2 places and receives all of the AMIS calls. Thus, no matter which Cisco Unity server a subscriber is associated with, when the subscriber sends a message to someone on another voice messaging system, the message is routed to the UAmis mailbox that is associated with Unity 2. This mailbox is homed on the Exchange server that was selected in the Message Store Configuration wizard during the setup of Unity 2.

Figure 5-1   ***AMIS Bridgehead Configuration***
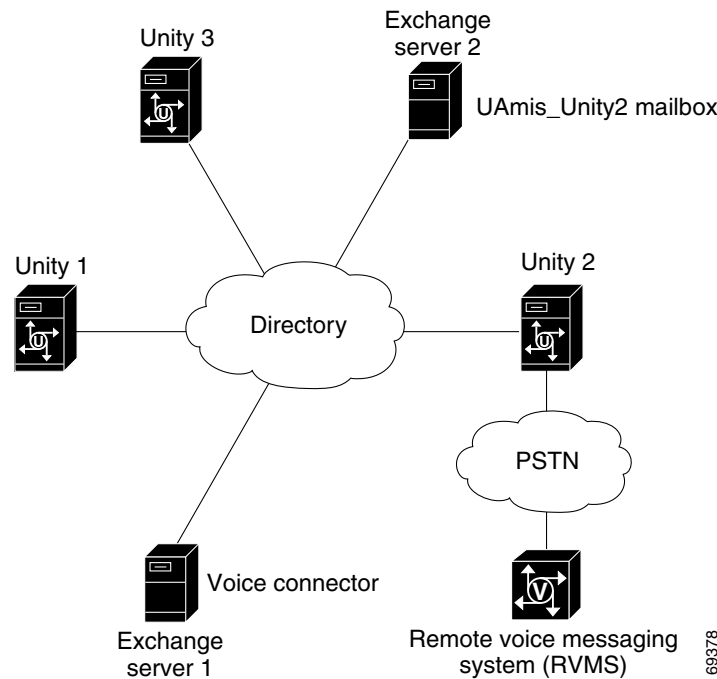
Design Considerations

Because AMIS calls are placed and answered on the Cisco Unity server on which the AMIS delivery locations were created, you can configure your Cisco Unity servers as needed to handle AMIS traffic.

- You can set up a bridgehead topology by designating one Cisco Unity server in the network to handle sending and receiving AMIS calls. See Figure 5-1.

- Recall that the dialout for an outbound AMIS message originates from the Cisco Unity server on which an AMIS delivery location was created. If the AMIS traffic is too heavy for one Cisco Unity server to handle, you can balance the load by setting up multiple AMIS bridgehead servers. In this case, you need to determine which AMIS delivery locations and AMIS subscribers to create on each of the Cisco Unity servers, and keep a record of the mapping.

  For example, assume that there are two AMIS bridgehead servers, Bridgehead A and Bridgehead B, and there are four AMIS delivery locations called London, Paris, Goose Creek, and Monks Corner. You anticipate that message delivery to the London and Paris delivery locations will be heavy, and that message delivery to the Goose Creek and Monks Corner delivery locations will not be as heavy. You can balance the load by creating the London and Goose Creek delivery locations on Bridgehead A, and create the Paris and Monks Corner delivery locations on Bridgehead B. This ensures that the AMIS traffic for the two heavy AMIS locations is split up between the two bridgehead servers, rather than one trying to deliver all of the messages by itself.

- For organizations with Cisco Unity servers deployed in different areas around the country or the world, it may be possible to set up a least-cost-routing topology to minimize or eliminate long distance phone charges related to AMIS transmissions.

  For example, assume there are Cisco Unity servers in Chicago and in New York, and that there is also another voice messaging system in New York to which subscribers in Chicago want to send messages. To avoid long distance phone charges when subscribers in Chicago send messages to

individuals who use the remote voice messaging system in New York, you create an AMIS delivery location, and optionally, AMIS subscribers, on the New York Cisco Unity server. When subscribers who are associated with the Chicago Cisco Unity server address messages to the AMIS subscribers in New York, the messages are first delivered by Exchange and the Voice Connector to the UAmis mailbox that is associated with the New York Cisco Unity server. Then the New York Cisco Unity server dials a local number to deliver the message to the remote voice messaging system, thus avoiding long distance phone charges.

Maintenance

This section provides information on various tasks that you may need to do in order to maintain your AMIS Networking configuration. See the following sections for details:

- Monitoring AMIS Message Traffic, page 5-40
- Moving the UAmis Mailbox, page 5-41

Monitoring AMIS Message Traffic

Cisco Unity monitors AMIS transmissions and the UAmis mailbox, and logs error events to the Windows Application Event log. Outgoing messages that cannot be delivered are returned to the sender, or to the Unaddressed Messages public distribution list if Cisco Unity cannot determine who the sender is.

For detailed information about the touchtones that are transmitted during an AMIS call, see the *AMIS Analog Networking Definitions* white paper, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html. To see the DTMFs that are transmitted during an AMIS call, use the Cisco Unity Diagnostic tool to enable the micro trace 28 AMIS Frames in the Conv AMIS section. You can also use the Port Status Monitor, available in the Switch Integration Tools section of Tools Depot, to observe call progress, and the Port Usage Analyzer, available in the Reporting Tools section of Tools Depot, to monitor port usage.

Cisco Unity also provides reports on AMIS message traffic. For more information, see the "AMIS Out Traffic Report" and the "AMIS In Traffic Report" sections in the "Reports" chapter of the *Maintenance Guide for Cisco Unity*. (The *Maintenance Guide for Cisco Unity* is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.)

Although Cisco Unity monitors the UAmis mailbox, you may want to check the UAmis mailbox periodically to confirm that messages are being sent in a timely manner. For example, if there are still messages to be sent when the AMIS schedule becomes inactive, they remain in the UAmis mailbox until the AMIS schedule becomes active again. If messages are often left in the UAmis mailbox, you may need to adjust the AMIS schedule or designate more voice ports for outgoing AMIS calls. Access to the UAmis mailbox is also needed when troubleshooting outbound message delivery problems.

In order to use Microsoft Outlook to access the UAmis mailbox, do the following "To Add the UAmis Mailbox to a User Profile" procedure to add the UAmis mailbox to the user profile of someone with administrative rights to Exchange. Refer to the Outlook documentation for more information.

To Add the UAmis Mailbox to a User Profile

Step 1   Start **Microsoft Outlook**.

Step 2   On the Tools menu, click **Services**.

Step 3   On the Services tab, in the field The Following Information Services Are Set Up in This Profile, click **Microsoft Exchange Server**.

Step 4   Click **Properties**.

Step 5   On the Advanced tab, click **Add**.

Step 6   In the Add Mailbox box, enter **UAmis**.

Step 7   Click **OK** three times to dismiss the dialog boxes.

Moving the UAmis Mailbox

For information on moving the UAmis mailbox, see the "UAmis Mailbox" section in the "Cisco Unity Data and Log Files" chapter of the *Maintenance Guide for Cisco Unity*, at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.)

Troubleshooting

For information on troubleshooting problems with AMIS messages, see the following sections in the *Troubleshooting Guide for Cisco Unity*, at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html.

- In the "Logs and Traces" chapter:
    - "AMIS Diagnostic Traces"
    - "Cisco Unity Voice Connector Logs"
- In the "Networking" chapter:
    - "Troubleshooting Problems with Outbound AMIS Messages"
    - "Troubleshooting Problems with Inbound AMIS Messages"

For detailed information about the touchtones that are transmitted during an AMIS call, see the *AMIS Analog Networking Definitions* white paper, at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

You can use the Port Status Monitor, available in the Switch Integration Tools section of Tools Depot, to observe call progress, and the Port Usage Analyzer, available in the Reporting Tools section of Tools Depot, to monitor port usage.

Notable Behavior

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

- Inbound Messages Are Delivered Only to Primary Extensions, page 5-42
- Inbound Search Scope, page 5-42
- Running the Voice Connector Setup Program in Another Language, page 5-42

Inbound Messages Are Delivered Only to Primary Extensions

When addressing a message to a Cisco Unity subscriber, users on the remote voice messaging system must use the primary extension of the Cisco Unity subscriber; alternate extensions are not supported. Senders will receive an NDR if they address a message with the alternate extension of a Cisco Unity subscriber.

Note also that Cisco Unity does not accept messages from a remote voice mail system that are sent to Cisco Unity public distribution lists, call handlers, and interview handlers. Cisco Unity accepts messages from a remote voice mail system only when they are sent to a subscriber primary extension.

When designing the numbering plan for Cisco Unity subscribers, as a best practice, configure the primary extension of all Cisco Unity subscribers with the extension that will be used for addressing from the remote voice mail system. Configure all other required extensions as alternate extensions, as all other functionality in Cisco Unity can use alternate extensions.

Inbound Search Scope

In installations with multiple Cisco Unity servers networked together, the search scope for a matching subscriber extension for inbound messages that are sent from another AMIS-compliant voice messaging system is controlled by the primary location addressing options in the Cisco Unity Administrator. The search scope for inbound AMIS messages can be set 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. Note that only subscriber extensions are searched. Incoming AMIS messages cannot be delivered to distribution lists.

Running the Voice Connector Setup Program in Another Language

The Voice Connector installation program does not prompt with a choice of languages for the installation; it always installs in English. To run the Voice Connector installation program by using one of the localized versions (FRA, DEU, or JPN) instead of English, do the following "To Run the Voice Connector Setup Program in Another Language" procedure.

⚠️

Caution   Installing the Voice Connector on an Exchange 2007 server is not supported.

To Run the Voice Connector Setup Program in Another Language

Step 1   From the Cisco Unity installation DVD or CD 1, copy the entire VoiceConnector-Ex2000 to your hard disk.

Step 2   In this local directory, browse to the **LocalizedFiles\ENU** directory.

Step 3   Rename the CiscoUnity_VoiceConnector.dll and SetupRes.dll files. (For example, rename the files CiscoUnity_VoiceConnector_ENU.dll and SetupRes_ENU.dll.)

Step 4   Copy the files **CiscoUnity_VoiceConnector.dll** and **SetupRes.dll** from the LocalizedFiles\<XXX> directory (where <XXX> is your language of choice) to the Localized\ENU directory.

Step 5   Run **Install.exe** from the VoiceConnector-Ex2000 directory on your hard disk. The installation program should be presented in the language you chose.

Note   Only the installation program will be in this language; currently, the Event Log messages, logging, properties, and configuration settings are not localized.

■ **Notable Behavior**

Bridge Networking

The Cisco Unity Bridge acts as a networking gateway between a Cisco Unity system and an Octel system on an Octel analog network. The Bridge communicates with Octel servers by using the Octel analog networking protocol and with Cisco Unity servers by using the Digital Networking protocol, which 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.

For more information about the Bridge, see the *Networking Guide for Cisco Unity Bridge*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

VPIM Networking

Overview: VPIM Networking

Cisco Unity supports the Voice Profile for Internet Mail (VPIM) protocol, which is an industry standard that allows different voice messaging systems to exchange voice, fax, and text messages over the Internet or any TCP/IP network. VPIM is based on the Simple Mail Transfer Protocol (SMTP) and the Multi-Purpose Internet Mail Extension (MIME) protocol.

For information about the VPIM-compliant voice messaging systems that Cisco Unity supports, see *Supported Hardware and Software, and Support Policies for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html. Note that VPIM Networking can be used for messaging between Cisco Unity servers that are in different directories, including messaging between Cisco Unity with Microsoft Exchange and Cisco Unity with IBM Lotus Domino systems.

VPIM Networking is a licensed feature. If your organization has multiple Cisco Unity servers networked together using Cisco Unity Digital Networking (and, therefore, accessing subscriber data in the same directory), only one server in the Digital Network needs to be licensed and configured for VPIM Networking. The Cisco Unity server configured for VPIM Networking is referred to as the bridgehead server. For more information on obtaining licenses for Cisco Unity features, see the applicable *Licensing for Cisco Unity* white paper, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

To use VPIM Networking, you must choose the applicable options when you run the Cisco Unity Permissions wizard. For detailed information, see Permissions wizard Help, which is available in Tools Depot on the Cisco Unity server.

See the following sections:

- Setting Up Cisco Unity to Use VPIM Networking, page 7-2—This section describes the prerequisites for setting up VPIM Networking, and provides a task list containing a high-level view of all of the tasks you need to complete for the setup, and the order in which they should be completed.

- Procedures for Setting Up Cisco Unity to Use VPIM Networking, page 7-4—This section contains all of the step-by-step procedures necessary to set up Cisco Unity for VPIM Networking.

- VPIM Concepts and Definitions, page 7-36—This section explains VPIM Networking concepts in detail. If you are unfamiliar with VPIM Networking, read this section prior to doing the setup procedures.

- Maintenance, page 7-59—This section provides information about monitoring system activity.

- Notable Behavior, page 7-61—This section documents notable behavior related to VPIM Networking.

Related Documentation

- "Using VPIM for Networking with Cisco Unity Express or Other Cisco Unity Systems"

- "Troubleshooting VPIM Transport," at http://www.ciscounitytools.com/Documents.htm.

Setting Up Cisco Unity to Use VPIM Networking

This section describes the prerequisites for setting up VPIM Networking, and provides a task list containing a high-level view of all of the tasks you need to complete for the setup, and the order in which they should be completed. If you are unfamiliar with VPIM Networking, you should first read the "VPIM Concepts and Definitions" section on page 7-36 and then review the task list and procedures before beginning the setup. Planning is essential to a successful setup.

Prerequisites

Before starting the setup, verify that the following prerequisites have been met:

- Cisco Unity is already installed on the server(s), and they are connected to the network as applicable for your installation.

- The remote voice messaging system with which Cisco Unity will be networked meets the requirements as described in the "Support Policy for VPIM Voice Messaging Systems" section of the *Supported Hardware and Software, and Support Policies for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

- A license file with a VPIM license has been obtained and installed on the Cisco Unity Bridgehead server.

- Cisco Unity and Exchange meet the requirements as described in the "VPIM Networking Requirements" section in *Networking Options Requirements for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

For installations with multiple Cisco Unity servers that access that same directory, you should first set up the servers for Digital Networking as described in the "Digital Networking" chapter before setting up VPIM Networking. After the Cisco Unity servers have been set up for Digital Networking, verify the following settings:

- Verify that the addressing search scope is set to either the dialing domain or the global directory on all of the networked servers so that Cisco Unity subscribers, no matter which server they are associated with, can address messages to VPIM delivery locations and/or VPIM subscribers. See the "Setting the Addressing Search Scope" section on page 2-6 for details.

- If you want outside callers to be able to reach VPIM subscribers from the automated attendant (for example, from the opening greeting) or directory assistance:

    - Verify that the Cisco Unity server(s) on which the VPIM subscribers will be created are in the same dialing domain as the Cisco Unity server that outside callers call into. See the "Customizing the Primary Location" section on page 7-18 for details on creating the dialing domain, and the "Dialing Domains" section on page 2-15 for background information.

    - Verify that the automated attendant and directory handler(s) search scopes are set to the dialing domain scope. See the "Setting the Directory Handler Search Scope" section on page 2-7 and the "Setting the Automated Attendant Search Scope" section on page 2-7.

Task List: Setting Up Cisco Unity to Use VPIM Networking

Use the task list that follows to set up VPIM Networking in Cisco Unity. The cross-references take you to detailed procedures for the setup. If you are setting up VPIM Networking for messaging between Cisco Unity servers in different directories, do these tasks in both Cisco Unity locations.

1. Make decisions about your numbering plan and gather information needed to configure VPIM Networking. See the "Making Design Decisions and Gathering Needed Information" section on page 7-4.

2. Determine the domain name that will be used for messaging between the remote voice messaging system and Cisco Unity. See the "Determining the Domain Name" section on page 7-5.

3. As applicable, configure DNS or HOSTS files. See the "Resolving Names with IP Addresses" section on page 7-5.

4. Verify network and SMTP connectivity with the remote voice messaging system. See the "Verifying Connectivity with the Remote Voice Messaging System" section on page 7-6.

5. Extend the Active Directory schema to enable VPIM Networking. See the "Extending the Active Directory Schema" section on page 7-8.

6. Determine whether the default recipient policy can be used for the Voice Connector Exchange mailbox, or create a new recipient policy. See the "Verifying the Recipient Policies or Creating a New One" section on page 7-9.

7. Install the Cisco Unity Voice Connector on an Exchange 2000 or Exchange 2003 server. See the "Setting Up the Voice Connector for VPIM Networking" section on page 7-10.

⚠️
Caution   Installing the Voice Connector on an Exchange 2007 server is not supported.

Do the Following Tasks on the Cisco Unity Server That Is Licensed for VPIM (the Bridgehead Server)

8. During Cisco Unity installation, when you ran the Cisco Unity Permissions wizard to grant the necessary permissions to the installation and service accounts, if you did not check the Set Permissions Required by AMIS, Cisco Unity Bridge, and VPIM check box on the Choose Whether to Enable Voice Messaging Interoperability page, do the following steps:

    a. Log on to the bridgehead server by using an account that:

    – Is a member of the Domain Admins group in the domain that the Cisco Unity server belongs to, or that has permissions equivalent to the default permissions for the Domain Admins group.

    – Is either an Exchange Full Administrator or a member of the Domain Admins group in the domain that contains all of the domains from which you want to import Cisco Unity subscribers.

    b. Re-run the Permissions wizard, and follow the on-screen prompts until the Choose Whether to Enable Voice Messaging Interoperability page appears.

    c. Check the Set Permissions Required by AMIS, Cisco Unity Bridge, and VPIM check box.

    d. Follow the on-screen prompts to complete the Permissions wizard.

    For more information on running the Permissions wizard, see the Permissions wizard Help file, PWHelp_<language>.htm, in the directory where the Permissions wizard is installed.

    If you do not know whether you checked the check box, run the Permissions wizard in report mode. For more information, see the Report Mode Help file, PWReportHelp_<language>.htm, in the directory where the Permissions wizard is installed.

9. If you plan to configure Cisco Unity to automatically update the VPIM subscriber directory, run ConfigMgr.exe in order to create the UVPIM account. See the "Creating the UVPIM Account by Using ConfigMgr.exe (Optional)" section on page 7-16.

10. Customize the primary location profile settings. See the "Customizing the Primary Location" section on page 7-18.

11. Create delivery locations for each remote voice messaging system. See the "Creating VPIM Delivery Locations" section on page 7-18.

12. Optionally, create VPIM subscribers. See the "Creating VPIM Subscribers" section on page 7-22.

13. Optionally, customize the delivery location settings that control automatic VPIM directory updates. See the "Customizing VPIM Subscriber Directory Update Settings" section on page 7-28.

14. Optionally, extend identified subscriber messaging to include VPIM subscribers. See the "Extending Identified Subscriber Messaging to Include VPIM Subscribers" section on page 7-34.

Finish the Setup

15. Set up the remote voice messaging system for VPIM. Precisely how this is done depends on the voice messaging system. However, you will need to provide the remote system with information about Cisco Unity. See the "Gathering Information About Cisco Unity to Configure Another Voice Messaging System for VPIM" section on page 7-36.

16. Test the setup to verify that Cisco Unity can exchange messages with the other voice messaging system.

Procedures for Setting Up Cisco Unity to Use VPIM Networking

This section contains all of the procedures necessary to set up Cisco Unity for VPIM Networking. If you are unfamiliar with VPIM Networking, you should first read the "VPIM Concepts and Definitions" section on page 7-36. Consult the "Task List: Setting Up Cisco Unity to Use VPIM Networking" section on page 7-3 for information on the order in which the procedures must be done.

Making Design Decisions and Gathering Needed Information

Before you begin setting up Cisco Unity for VPIM Networking, be sure to plan for the following, and gather the applicable information:

- Review your numbering plan strategy to determine whether you will need to enter prefixes on the VPIM delivery location and to determine which numbers to assign as Dial IDs for the primary and VPIM delivery locations.

- Decide whether you want Cisco Unity subscribers to use blind addressing or to address messages to VPIM subscribers. If you choose to use VPIM subscribers, determine for each remote VPIM system whether you will allow Cisco Unity to automatically create, modify, and delete VPIM subscriber entries for users on that system, based on information received in incoming VPIM messages. For each delivery location that will allow automatic updates, find out if the remote system will send a vCard with each message, or if the message headers should be used as the source of VPIM subscriber information instead. Also decide how you will map the source information to VPIM subscriber display names and extensions. For more information on automatic directory update considerations, see the "Automatic VPIM Subscriber Directory Updates" section on page 7-46.

- Make note of the following information about the remote voice messaging system: the mailbox range, the server name, the domain name, and the IP address.

- Choose the Exchange (or relay) server that will handle outgoing messages to the remote voice messaging system.

- Choose the Exchange server(s) on which to install the Voice Connector and the VPIM Transport Event Sink. Write down the FQDN and IP address of the Exchange server(s).

- Write down the FQDN and IP address of the Exchange (or relay) server(s) that handle incoming SMTP messages.

Determining the Domain Name

VPIM messages are addressed in the format <Mailbox Number>@<Domain Name>. In order for messages to be exchanged between the remote voice messaging system and Cisco Unity, you will need to decide on the domain name that the remote voice messaging system will use when addressing messages to Cisco Unity subscribers. The domain name will be configured as follows:

- On the remote voice messaging system on the location or node profile that corresponds to Cisco Unity. (Refer to the documentation for the remote voice messaging system for additional information.)

- On the SMTP Domain field, during the installation of the VPIM Transport Event Sink.

- On the SMTP Domain Name field on the Network > Primary Location page in the Cisco Unity Administrator.

- In the recipient policy for the Voice Connector Exchange mailbox.

If the remote voice messaging system location or node profile that corresponds to Cisco Unity has already been configured with a domain name, use that domain name in the procedures that follow. Otherwise, consult with the Exchange administrator for your organization to determine an appropriate domain name to use.

Domain Name Requirements

The domain name uniquely identifies the messaging system. When choosing domain names used by Cisco Unity and the remote voice messaging system, keep the following in mind:

- Cisco Unity and the remote voice messaging system cannot use the same domain name; each system must use a unique domain name.

- The complete domain name used by Cisco Unity cannot be a subset of the domain name used by the remote voice messaging system. For example, if Cisco Unity is using the domain name cisco.com, the remote voice messaging system cannot use names like london.cisco.com, paris-cisco.com, or romecisco.com. However, you could use europe.cisco.com for Cisco Unity, and then use the names london.cisco.com, paris-cisco.com, and romecisco.com.

⚠
Caution   Choosing a domain name that does not meet these requirements will result in message delivery failure.

Resolving Names with IP Addresses

VPIM messages are sent over the Internet or any TCP/IP network via SMTP. Therefore, some mechanism for name resolution is required for the remote voice messaging server and the Exchange (or relay) servers that handle incoming and outgoing SMTP messages. (Depending on your network, this may or may not be the same Exchange server on which the Voice Connector and the VPIM Transport

Event Sink will be installed.) While any method or combination of methods can 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 remote voice messaging server and the Exchange (or relay) server that handles incoming SMTP messages. The FQDN is displayed in the Windows System Control Panel on the Network Identification tab in the Full Computer Name field.

If your organization uses DNS:

- Add a host address resource (A) record and a mail exchange (MX) record in DNS for the remote voice messaging server, if they do not already exist.

- Verify that an A and MX record exist in DNS for the Exchange server (or relay server) that handles incoming SMTP messages. If the records are not in DNS, add them before continuing with the setup.

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 %windir%\System32\Drivers\Etc directory. Edit the HOSTS files as follows:

- On the Exchange (or relay) server that handles outgoing SMTP messages, add an entry to the HOSTS file with the FQDN and IP address of the remote voice messaging server.

- Refer to the remote voice messaging server documentation for information on name resolution. You may need to add an entry to the HOSTS file on the remote voice messaging server with the FQDN and IP address of the Exchange (or relay) server that handles incoming SMTP messages.

Verifying Connectivity with the Remote Voice Messaging System

Verify that the Exchange (or relay) server(s) that handle outgoing and incoming SMTP messages have network and SMTP connectivity with the remote voice messaging server, and vice versa.

For networking with another voice messaging server, you may need to install and configure an SMTP service or gateway on that server. Refer to the documentation of the other voice messaging system for information on installing the SMTP service or gateway. Before proceeding, verify that the SMTP service or gateway has been installed on the other voice messaging server.

To Verify Network Connectivity with the Remote Voice Messaging Server

Step 1   On the Exchange (or relay) server that handles outgoing SMTP messages, open a command prompt window.

Step 2   Enter **ping <IP address>**, where <IP address> is the IP address of the remote voice messaging server.

If you receive no reply, troubleshoot the network connectivity problem until the problem is resolved. Then continue with Step 3.

Step 3   Enter **ping <Domain name>** where <Domain name> is the domain name that will be used to address messages to the remote voice messaging server. The domain name in this step is the domain name that will be entered on the VPIM delivery location page in the Cisco Unity Administrator when setting up VPIM Networking.

Step 4   If you received a reply when pinging the IP address in Step 2, but no replies when pinging the domain name in Step 3, see the "Resolving Names with IP Addresses" section on page 7-5. When the problem is resolved, continue with Step 5.

Step 5   Test network connectivity in the opposite direction. For systems other than Cisco Unity, consult the documentation for information on how to conduct the test, and continue with Step 6. Note that the remaining steps in this procedure may not exactly match the steps necessary for your system, so you may need to make adjustments.

Step 6   On the remote server, ping the IP address of the local Exchange (or relay) server that handles incoming SMTP messages.

If you receive no reply, troubleshoot the network connectivity problem until the problem is resolved. Then continue with Step 7.

Step 7   On the remote server, ping the domain name, where the domain name is the one that you decided on in the "Determining the Domain Name" section on page 7-5.

Step 8   If pinging by domain name fails, see the "Resolving Names with IP Addresses" section on page 7-5. When you verify that you have basic network connectivity, continue with the following "To Verify SMTP Connectivity with the Remote Voice Messaging Server" procedure.

To Verify SMTP Connectivity with the Remote Voice Messaging Server

Step 1   In a command prompt window on the Exchange (or relay) server that handles outgoing SMTP messages, enter **telnet <RemoteDomainName> 25**, where <RemoteDomainName> is the domain name that will be used to address messages to the remote voice messaging server.

Step 2   If there is a response, enter **ehlo <DomainName>**, where <DomainName> is the domain name that you decided on in the "Determining the Domain Name" section on page 7-5.

Step 3   If the telnet test was successful, enter **quit** to end the telnet session.

Step 4   Test SMTP connectivity in the opposite direction. For systems other than Cisco Unity, consult the documentation for information on how to conduct the SMTP connectivity test, and continue with Step 5. Note that the remaining steps in this procedure may not exactly match the steps necessary for your system, so you may need to make adjustments based on your voice messaging system documentation.

Step 5   On the remote server, attempt to start a telnet session. Enter **telnet <DomainName> 25**, where <DomainName> is the domain name that you decided on in the "Determining the Domain Name" section on page 7-5.

Step 6   If there is a response, on the remote server, enter **ehlo <RemoteDomainName>**, where <RemoteDomainName> is the domain name of the remote voice messaging server.

If either of the telnet tests in Step 5 or Step 6 fails, there is a basic SMTP connectivity problem that must be resolved before proceeding with the VPIM Networking setup.

Step 7   With Cisco Unity, the processing of VPIM messages will occur on the Exchange servers on which the Voice Connector and the VPIM Transport Event Sink will be installed. If the Transport Event Sink will not be installed on the server that handles incoming and outgoing SMTP messages, and/or if the Voice Connector and the Transport Event Sink will be installed on separate Exchange servers, review your Exchange settings to verify:

   • That the server that handles incoming SMTP messages is able to route messages to the Exchange server on which the Transport Event Sink will be installed.

   • That the server on which the Transport Event Sink will be installed is able to route messages to the server on which the Voice Connector will be installed, if they will be installed on separate servers.

- That the server on which the Voice Connector will be installed is able to route messages to the server that handles outgoing SMTP messages.

- That the Exchange servers where Cisco Unity subscriber mailboxes are located can route messages to the Exchange server on which the Voice Connector is installed.

- That the Exchange server on which the Voice Connector is installed can route messages to the Exchange servers where Cisco Unity subscriber mailboxes are located.

Refer to your Exchange documentation for more information.

Extending the Active Directory Schema

Before Cisco Unity is installed, the Active Directory schema is extended to store Cisco Unity-specific information. To support VPIM Networking, the schema must be further extended. To see the schema changes that need to be made to support VPIM Networking, browse to the directory Schema\LdifScripts on Cisco Unity Disc 1, and view the file vpimgateway.ldf.

To Extend the Active Directory Schema for VPIM Networking

Do this procedure only if you did not already modify the Active Directory schema to support VPIM Networking during the Cisco Unity installation. You can verify whether the schema has already been modified by examining the log file that is generated each time the schema is updated. A shortcut to the directory where the log file is located is placed on the Windows desktop.

Step 1   Confirm that all domain controllers are on line before making the schema updates. Schema replication will occur only when all domain controllers are on line.

Step 2   On the domain controller that is the schema master, log on by using an account that is a member of the Schema Administrators group.

Step 3   On Cisco Unity DVD 1 or CD 1, or from the location to which you saved the downloaded Cisco Unity CD 1 image files, browse to the directory **ADSchemaSetup**, and double-click **ADSchemaSetup.exe**.

Step 4   In the dialog box, double-click a row to choose the language in which you will view ADSchemaSetup.

Step 5   Check **Exchange 2000 VPIM Connector**, uncheck the other check boxes, and then click **OK**.

Step 6   When the LDAP Data Interchange Format (LDIF) scripts have finished running, click **OK**.

Step 7   When the schema extension has finished, Ldif.log and LDif.err files are saved to the desktop. View the contents of the files to confirm that the extension completed successfully.

Step 8   Wait for the changes to the schema to replicate throughout the forest before adding information to the primary location and to delivery locations. Changes to the schema may take 15 minutes or more to replicate.

Note   To determine whether changes have replicated and to force replication if necessary, use the Replication Monitor, which is available when you install Support Tools from the Windows 2000 compact disc.

Verifying the Recipient Policies or Creating a New One

Depending on your Exchange organization, you may be able to use the default recipient policy for the Voice Connector Exchange mailbox, or you may need to create a new recipient policy.

To Check the Recipient Policies

Step 1   On the Exchange server on which the Voice Connector will be installed, open the **Exchange System Manager.**

Step 2   Expand the **Recipients** tree in the left pane.

Step 3   Click **Recipient Policies**.

Step 4   In the right pane, right-click a recipient policy, and click **Properties**.

Step 5   Click the **E-Mail Addresses** tab.

If the SMTP address is the same as the domain name that you previously chose in the "Determining the Domain Name" section on page 7-5, close the Properties page, exit Exchange System Manager, and skip to the "Setting Up the Voice Connector for VPIM Networking" section on page 7-10.

Step 6   Close the Properties page, and repeat Step 4 and Step 5 for each recipient policy (including the default recipient policy).

If your chosen domain name does not match the SMTP address configured in any of the recipient polices, create a new recipient policy for the Voice Connector Exchange mailbox as described in the following "To Create a Recipient Policy for the Voice Connector Exchange Mailbox" procedure.

To Create a Recipient Policy for the Voice Connector Exchange Mailbox

⚠

Caution   Consult the Exchange administrator for your organization before doing the following procedure. Misconfiguration of the Recipient Policies could result in problems routing other SMTP mail for the organization.

Step 1   In Exchange System Manager, right-click **Recipient Policies** and click **New > Recipient Policy**.

Step 2   In the New Policy window, confirm that **E-Mail Addresses** is the only selection, and click **OK**.

Step 3   On the General tab, enter a meaningful name. Do not configure any Filter rules.

Step 4   On the E-Mail Addresses (Policy) tab, click **New**.

Step 5   Select **SMTP Address** and click **OK**.

Step 6   In the Address field, enter the domain name that you previously chose in the "Determining the Domain Name" section on page 7-5.

Step 7   Verify that the check box **This Exchange Organization Is Responsible for All Mail Delivery to This Address** is checked.

Step 8   Click **OK**.

Step 9   Check the check box next to the address that you added in Step 6, and verify that the row is highlighted.

Step 10   Click **Set as Primary**.

When you click Set as Primary, the new address should change to bold text.

Step 11 Click **OK**, and then click **Yes** to the warning about updating the corresponding recipient e-mail addresses.

Setting Up the Voice Connector for VPIM Networking

Install the Voice Connector on any Exchange 2000 or Exchange 2003 server that is not part of an Exchange cluster (Microsoft does not support third-party connectors on an Exchange cluster server). Although the Voice Connector can be installed on the Cisco Unity server (when Exchange is also on the server), this is not recommended for performance reasons.

⚠ **Caution** Installing the Voice Connector on an Exchange 2007 server is not supported.

⚠ **Caution** Installing the Transport Event Sink on an Exchange 2007 server is not supported.

If the Exchange server on which the Voice Connector will be installed is in a different routing group than the Exchange servers on which Cisco Unity subscribers are homed, routing group connectors must be configured between the routing groups.

The Voice Connector service is automatically configured to log on as the account that is associated with the Exchange server on which the Voice Connector is installed (sometimes referred to as the "Local System" account). The account that the service logs on as should not be changed.

⚠ **Caution** Do not change the default permissions for the Local System account. In addition, do not change the permissions granted to Exchange administrative groups during Exchange installation. The Voice Connector logs on using that account, and if you change permissions, the Voice Connector may not function properly.

To set up VPIM Networking, the Voice Connector and the Transport Event Sink must be installed. Although you use the same Voice Connector installation program to install these components, where you install them depends on the network configuration.

In most cases, you install the Voice Connector on only one Exchange server, even if the system includes multiple Exchange servers. You install the Transport Event Sink on each Exchange server that will receive incoming VPIM messages.

The Voice Connector installation program does not prompt with a choice of languages for the installation; it always installs in English. To run the Voice Connector installation program by using one of the localized versions (FRA, DEU, or JPN) instead of English, see the "Running the Voice Connector Setup Program in Another Language" section on page 7-63.

✎ **Note** The following procedure is for installing Voice Connector version 12.0(1), which ships with Cisco Unity 5.0(1). We recommend that you first check for a later version of the Voice Connector, and that you install that version instead. Follow the installation instructions in the release notes for the applicable version. To check for a later version, go to the Cisco Unity Voice Connector for Exchange Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity-voice-connector.

To Install the Voice Connector for Exchange 2000

First uninstall any previous versions of the Voice Connector. See the "Uninstalling the Cisco Unity Voice Connector" section on page 10-4.

As a best practice, back up the Exchange server before installing the Voice Connector.

Step 1   Log on to the Exchange server on which you are installing the Voice Connector.

Step 2   Disable any virus-scanning services on the Exchange server.

Step 3   If Cisco Unity is also on the server on which you are installing the Voice Connector, disable the Cisco Security Agent service, if applicable.

Step 4   If you are installing the Voice Connector from Cisco Unity DVD 1, insert the disc in the computer, and browse to the **VoiceConnector-Ex2000 directory**.

    If you downloaded the Voice Connector files from the Software Center website, browse to the directory in which the files were extracted.

Step 5   Double-click **Install.exe** and then click **Next**.

Step 6   On the Voice Connector Setup Wizard Select Components dialog box, check the **Voice Connector for Exchange** check box.

Step 7   If you are setting up secure messaging and if Cisco Unity is not on the Exchange server, check the **Cisco Secure Messaging Service** check box.

Step 8   If you are installing the Transport Event Sink on the same server, check the **Transport Event Sink for VPIM Networking** check box.

⚠️

Caution   Installing the Transport Event Sink on an Exchange 2007 server is not supported.

Step 9   Click **Next**.

Step 10   If you did not check the Transport Event Sink for VPIM Networking check box in Step 8, skip to Step 11. Otherwise, do the following sub-steps:

    a.   On Transport Event Sink wizard welcome screen, click **Next**.

    b.   On the Choose Destination Folder dialog box, specify the destination, and click **Next**.

    c.   On the Enter Domain Name dialog box, enter the domain name that you previously decided on in the "Determining the Domain Name" section on page 7-5.

    d.   Click **Next**.

    e.   On the Ready to Install the Program screen, click **Install**.

    f.   When the installation is complete, click **Finish**.

Step 11   On the Voice Connector for Exchange Welcome screen, click **Next**.

Step 12   On the Confirm SMTP Pickup Directory screen, click **Next**.

Step 13   In the Address Types dialog box, check the **VPIM** check box.

Step 14   If you are setting up the system to use other networking options, check the check boxes of the applicable address types.

Step 15   Click **Next**.

Step 16   On the Confirm Directory dialog box, click **Next** to launch the setup.

Step 17 If you did not check the Secure Messaging Service check box in Step 7, skip to Step 18. Otherwise, do the following sub-steps in the Cisco Unity Secure Messaging Service Setup wizard:

    a. On the Welcome screen, click **Next**.

    b. On the Choose Destination Folder dialog, specify the destination, and click **Next**.

    c. Optionally, on the Message Security Settings screen, check the **Enable Message Aging** check box, and enter the number of days that encrypted messages should be available. (If the check box is unchecked, Cisco Unity will not limit the number of days for which encrypted messages will be available.)

    d. Click **Next**.

    e. On the Ready to Install Software screen, click **Install**.

Step 18 When the setup is complete, click **Finish** to exit Setup and restart the server.

Step 19 Enable virus-scanning and the Cisco Security Agent services, if applicable.

To view Voice Connector properties in Exchange System Manager, Windows Script Host version 5.6 or later must be installed on the Exchange server. (Note that if the Exchange server uses an earlier version of Windows Script Host, the Voice Connector functions properly, but you will not be able to view Voice Connector properties in Exchange System Manager.)

To Determine Whether the Microsoft Windows 2000 Script Host Should Be Updated

Step 1 On the Exchange server on which the Voice Connector has been installed, browse to **Winnt\System32**.

Step 2 Right-click the file **Wshom.ocx**, and click **Properties**.

Step 3 Click the **Version** tab.

Step 4 In the Item Name list, click **Product Version** to view the version in the Value box.

Step 5 If the version is earlier than 5.6, update Windows Script Host so that the Voice Connector properties can be displayed in Exchange System Manager. (Go to the downloads page of the Microsoft website, and do a keyword search for Windows Script Host. Follow the installation instructions.)

To Verify the Voice Connector Installation

To verify that the Voice Connector for Exchange 2000 installed properly, verify that the Voice Connector service is running, and that the Voice Connector mailbox has been created.

Step 1 Open the Services applet on the Exchange server on which the Voice Connector is installed. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 2 Verify that the Status for the Exchange 2000 Voice Connector (<Server name>) service is **Started**, and that the Startup Type is set to **Automatic**.

Step 3 Exit the Services applet.

Step 4 Open Exchange System Manager on the Exchange server on which the Voice Connector is installed. (On the Windows Start menu, click **Programs > Microsoft Exchange > Exchange System Manager**.)

Step 5 In the tree in the left pane, expand the **Servers** container. If the organization properties at the top of the tree have been set such that administrative groups are displayed in the tree, the Servers container is nested within the administrative group container.

Step 6   Within the Servers container, expand the **<Server name>\<Storage group>\Mailbox Store (<Server name>)** container for the server on which the Voice Connector is installed.

Step 7   In the expanded tree, click **Mailboxes**.

In the right pane, you should see the mailbox for "Exchange 2000 Voice Connector (<Server name>)" or "AvExchangeIVC_<Server name>." (The name changes from "AvExchangeIVC_<Server name>" to "Exchange 2000 Voice Connector (<Server name>)" after you run Cleanup Agent.)

Step 8   Exit Exchange System Manager.

To Verify or Set the Recipient Policy for the Voice Connector Exchange Mailbox

Step 1   On the Exchange server on which the Voice Connector is installed, open the **Exchange System Manager**.

Step 2   Expand the **Connectors** container in the left-hand pane.

Step 3   Right-click **Exchange 2000 Voice Connector (<Server name>)**, and select **Properties**.

Step 4   If you are using the default recipient policy for the Voice Connector Exchange mailbox:

  a.   Verify that "Recipient Policy to Calculate Enterprise GDI for MTS-IDs" on the bottom of the Options tab is set to **Default Policy**.

  b.   Close the properties page, exit **Exchange System Manager**, and go to the "Customizing the Primary Location" section on page 7-18.

If you created a new recipient policy for the Voice Connector Exchange mailbox:

  a.   Choose the new recipient policy from the "Recipient Policy to Calculate Enterprise GDI for MTS-IDs" list on the bottom of the Options tab.

  b.   Click **OK** and exit Exchange System Manager.

The following procedure is for installing the Transport Event Sink on a separate Exchange server from the server on which the Voice Connector is installed. The procedure is for running the setup program for Voice Connector version 12.0(1), which ships with Cisco Unity 5.0(1). We recommend that you first check for a later version of the Voice Connector, and that you install the Transport Event Sink from that version instead. Follow the installation instructions in the release notes for the applicable version. To check for a later version, go to the Cisco Unity Voice Connector for Exchange Software Download page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity-voice-connector.

First uninstall any previous versions of the Transport Event Sink. See the "Uninstalling the Cisco Unity Voice Connector" section on page 10-4.

⚠

Caution   Installing the Transport Event Sink on an Exchange 2007 server is not supported.

To Install the Transport Event Sink on a Separate Exchange Server

Step 1   Log on to the Exchange server on which you are installing the Transport Event Sink.

Step 2   Disable any virus-scanning services on the Exchange server.

Step 3   If Cisco Unity is also on the server on which you are installing the Transport Event Sink, disable the Cisco Security Agent service, if applicable.

Step 4 If you are installing the Transport Event Sink by running the Voice Connector installation program from a Cisco Unity DVD or CD, insert the disc in the computer, and browse to the **VoiceConnector-Ex2000 directory**.

If you downloaded the Voice Connector files from the Software Center website, browse to the directory in which the files were extracted.

Step 5 Double-click **Install.exe**, and click **Next**.

Step 6 On the Voice Connector Setup Wizard Select Components dialog box, check the **Transport Event Sink for VPIM Networking** check box, and click **Next**.

Step 7 On the Transport Event Sink wizard welcome screen, click **Next**.

Step 8 On the Choose Destination Folder dialog box, specify the destination, and click **Next**.

Step 9 On the Enter Domain Name dialog box, follow the instructions to specify the domain. (Typically, the domain entered is the same as the domain that will be entered on the Primary Location page. Note that the domain does not have to be the same domain as that of the server on which the Transport Event Sink is being installed.)

Step 10 Click **Next**.

Step 11 On the Ready to Install the Program screen, click **Install**.

Step 12 When the installation is complete, click **Finish** to exit Setup and restart the server.

Step 13 Enable virus-scanning and the Cisco Security Agent services, if applicable.

Controlling What Happens to Messages That Cannot Be Delivered

When the Voice Connector encounters a message that cannot be delivered, and the sender information is incomplete or incorrect such that a nondelivery receipt (NDR) cannot be sent to the message sender, the Voice Connector saves the message in the Archive folder in the Voice Connector mailbox. The Archive folder is accessible only when using tools available from Microsoft. If you want more control over archived messages, you can add to the registry either the AliasToForwardBadMailsTo value or the DeleteArchiveFolderMessages value (but not both).

When you add the AliasToForwardBadMailsTo registry value and set it to the SMTP address of a user or distribution list, when the Voice Connector encounters a problematic message, information about the message is sent to the specified address instead of being saved in the Archive folder. When a problematic AMIS message is encountered, the informational message that the Voice Connector sends to the specified user (or distribution list) includes the MIME header of the problematic message as a text attachment. The MIME header contains the "To" and "From" addresses, which may help in troubleshooting the problem.

When you add the DeleteArchiveFolderMessages registry value and set it to 1, the Voice Connector continues to save problematic messages in the Archive folder, but periodically, the Voice Connector automatically deletes the messages in the Archive folder.

When a message is saved to the Archive folder or sent to the address specified in the AliasToForwardBadMailsTo registry value, an entry is made in the Voice Connector log file. (The information is logged when the Voice Connector properties are set to the default logging level or a higher logging level.) The Voice Connector logs are located on the Exchange server on which the Voice Connector is installed in the directory <ExchangeServerPath>\VoiceGateway\LogFiles. The files are named in the format GwIvc_<YyMmDd >.log, where Yy in the year, Mm is the month, and Dd is the day.

To add the registry values, do the following procedure.

To Control What Happens to Messages That Cannot Be Delivered

Step 1   On the Exchange server on which the Voice Connector is installed, start Regedit.

⚠️

Caution   Changing the wrong registry key or entering an incorrect value can cause the server to malfunction. Before you edit the registry, confirm that you know how to restore it if a problem occurs. (See the "Restoring" topics in Registry Editor Help.) If you have any questions about changing registry key settings, contact Cisco TAC.

Step 2   If you do not have a current backup of the registry, click **Registry > Export Registry File**, and save the registry settings to a file.

Step 3   Expand the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Active Voice\AvIvc

Step 4   If you want information about the messages to be sent to a user or distribution list instead of being saved to the Archive folder, do the following sub-steps. Otherwise, skip to Step 5.

    a.   On the Edit menu, click **New > String Value**.

    b.   Enter **AliasToForwardBadMailsTo** as the value name.

    c.   Double-click **AliasToForwardBadMailsTo**.

    d.   In the Edit String dialog box, enter the SMTP address of the recipient (for example unityadministrator@company.com). This must be the SMTP address of a user, contact, or distribution list object in Exchange. An e-mail with the failed message and information about the message will be sent to this address.

    e.   Click **OK**.

    f.   Exit Regedit.

    g.   Skip to Step 6.

Step 5   If you want messages that are saved in the Archive folder to be automatically deleted, do the following sub-steps:

    a.   On the Edit menu, click **New > DWORD** Value.

    b.   Enter **DeleteArchiveFolderMessages** as the value name.

    c.   Double-click **DeleteArchiveFolderMessages**.

    d.   In the Edit DWORD dialog box, enter **1**.

    e.   Click **OK**.

    f.   Exit Regedit.

Step 6   Open the Services MMC on the Exchange server on which the Voice Connector is installed. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 7   Right-click **Exchange 2000 Voice Connector (<Server name>)**, and click **Restart**.

Step 8   Exit the Services MMC.

Creating the UVPIM Account by Using ConfigMgr.exe (Optional)

If you plan to configure Cisco Unity to automatically update the VPIM subscriber directory based on the information received in incoming VPIM messages, you must first configure the bridgehead server by running ConfigMgr.exe with the Create VPIM Account option. (Note that the use of automatic directory updates is optional, and that this procedure and the steps for configuring automatic updates can be done at any time after VPIM Networking has been set up, if you later decide to use this functionality.) To enable the processing of directory update information, ConfigMgr.exe does the following:

- Configures the server to automatically start and stop the CsVPIMConnector service.
- Configures the Cisco Unity Administrator to enable the link to the Delivery Locations > Subscriber Creation pages.
- Creates the UVPIM mailbox to which the Voice Connector will deliver directory messages for the CsVPIMConnector service to process. Note that the UVPIM mailbox is actually homed on the Exchange server that the Cisco Unity Bridgehead server is connected to. This server is also know as the partner Exchange server; it was selected in the Cisco Unity Server Message Store Configuration wizard during setup.

Do one of the following two procedures, depending on the version of Exchange that the partner Exchange server is running.

To Create the UVPIM Account When the Partner Exchange Server Is Running Exchange 2000 or Exchange 2003

Step 1   On the VPIM bridgehead 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 VPIM Dir Account**.

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

Step 5   Close the ConfigMgr dialog box.

Step 6   On the Cisco Unity server, start the Services tool. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 7   Right-click **AvNotifierMgr**, and select **Restart**.

> **Note**   The CPU usage on the Cisco Unity server will spike for a few minutes while the AvNotifierMgr reinitializes connections with subscriber mailboxes.

Step 8   Close the **Services** tool.

To Create the UVPIM Account When the Partner Exchange Server Is Running Exchange 2007

Step 1   On the VPIM bridgehead 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 and Configure VPIM Account and Mailbox**.

Step 4   In the Create the PowerShell Script That Creates the VPIM Account and Mailbox dialog box, choose the path and file name for the script that will create the VPIM account.

You must run the script on the partner server or another server on which Exchange Management Shell is installed, so choose one of the following locations to save the script:

- The server that you will run the script on.

- A network location that is accessible to that server.

- A removeable disk.

Step 5   Click **Create Script**.

Step 6   Click **OK**.

Step 7   Click **Exit** to close ConfigMgr.

Step 8   Log on to the Exchange 2007 server on which you want to run the script by using an account that has the right to run a PowerShell script.

Step 9   If necessary, copy the script locally to the Exchange server.

Step 10   Run **Exchange Management Shell**. (From the Start menu, click **All Program > Microsoft Exchange Server 2007 > Exchange Management Shell**.)

Step 11   Run the script. In the Exchange Management Shell window, enter the full pathname of script. For example:

d:\scripts\UVpim_<ServerName>.PS1

Alternatively, you can change to the directory where the script is located by using the "cd" command, and then run the script by entering:

.\UVpim_<ServerName>.PS1

For more information, refer to Microsoft documentation.

Step 12   On the VPIM bridgehead Cisco Unity server, browse to the directory in which Cisco Unity is installed (the default location is CommServer).

Step 13   Double-click **ConfigMgr.exe**. The ConfigMgr dialog box appears.

Step 14   Click **Create and Configure VPIM Account and Mailbox**.

Step 15   Click **OK**.

Step 16   Click **Exit** to close ConfigMgr.

Step 17   On the Cisco Unity server, start the Services tool. (On the Windows Start menu, click **Programs > Administrative Tools > Services**.)

Step 18   Right-click **AvNotifierMgr**, and select **Restart**.

> **Note**   The CPU usage on the Cisco Unity server will spike for a few minutes while the AvNotifierMgr reinitializes connections with subscriber mailboxes.

Step 19   Close the **Services** tool.

Be sure to let anyone who administers Active Directory and Exchange know about the UVPIM mailbox so that it is not moved or deleted by mistake. To avoid inadvertently moving or deleting the UVPIM mailbox, consider changing the Exchange display name so that the account is more clearly identified to you or the Exchange administrator as requiring "special" treatment. Note also that when it is created, the UVPIM account is hidden from the Outlook address book.

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. In this case, verify that the SMTP Domain Name has been entered on the primary locations of all Cisco Unity servers networked via Digital Networking. Otherwise, VPIM Networking will not work for the subscribers on the other Cisco Unity servers.

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 VPIM 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   In the SMTP Domain Name field, enter the domain name that you previously chose in the "Determining the Domain Name" section on page 7-5.

Step 7   Click the **Save** icon.

Creating VPIM Delivery Locations

Create a VPIM delivery location on the bridgehead Cisco Unity server for each remote voice messaging system to which subscribers will send messages. If Cisco Unity will be messaging with a large number of voice messaging systems, 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 voice messaging systems for which delivery locations have been configured, you can create the rest of the delivery locations.

Carefully consider the Dial ID that you will assign to the delivery location. See the "Guidelines for Assigning Dial IDs and Extensions" section on page 9-2 for detailed information about choosing a Dial ID.

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

- Using the Cisco Unity Administrator to Create VPIM Delivery Locations, page 7-19
- Using the Cisco Unity Bulk Import Wizard to Create VPIM Delivery Locations, page 7-20
- Modifying Existing Delivery Locations by Using the Cisco Unity Bulk Import Wizard, page 7-22

Using the Cisco Unity Administrator to Create VPIM Delivery Locations

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

To Create VPIM 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, which identifies the location in Cisco Unity, and which subscribers use to blind address messages to recipients at this location.

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

Step 6   Click **Add**.

Step 7   Record a voice name for the location.

Step 8   Enter the Internet-addressable SMTP domain name of the system on the TCP/IP network that handles messages for the remote voice messaging system.

Step 9   If needed to accommodate your numbering plan, or if there is more than one VPIM delivery location with the same domain name, enter a number in the Remote Phone Prefix field.

> **Note**   Subscribers do not enter this prefix when addressing messages. However, on outgoing messages, the Voice Connector adds the prefix to the beginning of the recipient mailbox number to form the To address. On incoming messages, the Voice Connector expects this same prefix to be the leading digits of the From mailbox number and strips these digits before determining the sending mailbox number.

Step 10   If needed to accommodate your numbering plan, enter a number in the Cisco Unity Phone Prefix field.

> **Note**   On outgoing messages, the Voice Connector adds this prefix to the beginning of the sender mailbox number to form the From address. On incoming messages, the Voice Connector expects this same prefix to be the leading digits of the To mailbox number and strips these digits prior to determining the matching Cisco Unity recipient ID.

Step 11   Indicate whether incoming messages from this VPIM location should be converted to another audio format.

Step 12   Indicate whether outbound messages to this VPIM location should be converted to another audio format. If the remote system is Cisco Unity, typically you choose **Do Convert Outgoing Messages**. For systems other than Cisco Unity, typically you choose **G.726**.

Step 13   Optionally, check the **Sender's Recorded Name** and/or **Sender's vCard** check box(es). Some systems have the capability of using this information to create directory entries.

Step 14   If you are using Secure Messaging, indicate whether to have incoming messages encrypted and outgoing messages decrypted.

Step 15   Click the **Save** icon.

Using the Cisco Unity Bulk Import Wizard to Create VPIM 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—see the Cisco Unity Bulk Import wizard Help.

To Prepare a CSV File for Creating VPIM 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, SMTP_DOMAIN_NAME

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 every 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 VPIM Delivery Locations by Using the Cisco Unity Bulk Import Wizard" procedure.

To Create VPIM 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 **VPIM**, 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\VPIM_Locations.csv, the default output file will be C:\Temp\VPIM_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\VPIM_Locations.csv, the default output file will be C:\Temp\VPIM_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 VPIM Subscribers

You may prefer to create only a few VPIM subscribers at this point, for testing purposes, until you verify that Cisco Unity and the remote system can successfully exchange messages. After you have confirmed that messaging between Cisco Unity and the remote system is working correctly, you can finish creating the VPIM subscribers. Note that you must first create VPIM delivery locations before creating VPIM subscribers, and the VPIM subscribers must be created on the same Cisco Unity server as the VPIM delivery locations.

If you choose not to create VPIM subscribers at this point, you can still configure Cisco Unity to automatically create, update, and delete VPIM subscriber records as VPIM messages are received from users on remote systems. With this approach, subscribers may initially need to use blind addressing to address messages to users on remote systems, but as incoming messages and replies to outgoing messages are received from those users, the directory of VPIM subscribers will be populated based on the vCard or header information in those messages. Alternatively, you can use a combination of pre-populated VPIM subscribers and automatic updates to avoid the need to use blind addressing and to keep the VPIM subscriber directory updated when changes occur to active users on the remote system.

You can create VPIM subscriber accounts by using the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator. See the following sections:

- Before Creating Subscriber Accounts, page 7-22
- Using the Cisco Unity Bulk Import Wizard to Create Multiple Subscriber Accounts, page 7-24
- Using the Cisco Unity Administrator to Create VPIM Subscriber Accounts, page 7-27
- After Creating Subscriber Accounts, page 7-27

Before Creating Subscriber Accounts

This section lists—in order—the issues that you must consider before creating VPIM subscribers. VPIM 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 VPIM 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 VPIM 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 that you can modify. You can also create new classes of service. For details, see the "Managing Classes of Service" chapter in the *System Administration Guide for Cisco Unity*.

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 that you can modify.

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

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, see the "Managing Distribution Lists" chapter in the *System Administration Guide for Cisco Unity*.

Public distribution lists correspond to distribution groups in Active Directory. The distribution lists are listed in the address book for Microsoft Outlook (or other e-mail client), unless they are explicitly hidden. To help prevent e-mail from being sent to VPIM subscribers, you may want to create lists that contain only VPIM subscribers, and hide these distribution lists from the Outlook address book. The option to hide distribution lists is available on the Subscribers > Public Distribution Lists > Profile page in the Cisco Unity Administrator.

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 that you can modify, and you can create an unlimited number of additional templates. For more details, see the "Managing Subscriber Templates" chapter in the *System Administration Guide for Cisco Unity*.

VPIM subscribers correspond to contacts in Active Directory. The contacts are listed in the address book for Microsoft Outlook (or other e-mail client), unless they are explicitly hidden. You may prefer that the associated contacts do not appear in the Outlook address book at all, or you may want to alter how contacts appear in the Outlook address book. See the "Determining How VPIM Subscribers Appear in the Outlook Address Book" section on page 7-54 for details.

You can also specify the template that Cisco Unity uses when creating VPIM subscribers based on information from incoming VPIM messages, if automatic directory updates are enabled for a particular delivery location. You can use an existing template, or you may wish to create a template specifically for this purpose. For more information, see the "Customizing VPIM Subscriber Directory Update Settings" section on page 7-28.

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

Using the Cisco Unity Bulk Import Wizard to Create Multiple 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 the user data contained in the CSV file is formatted correctly, you can use it to create new Active Directory contacts at the same time that you create VPIM subscriber accounts, or you can use it to create VPIM subscriber accounts with existing Active Directory contact data.

If you choose to create VPIM subscriber accounts with existing Active Directory contact data, note that the e-mail addresses for the imported contacts are overwritten with extension addresses that are 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—see Cisco Unity Bulk Import wizard Help.

To Prepare a CSV File for Creating VPIM Subscriber Accounts

Step 1   Save the data that 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 extension (DTMF_ACCESS_ID), and then by the remote mailbox number (REMOTE_USER_ID):

    Abade,Alex,2001,3000
    Bader,Kelly,2002,3100
    Campbell,Terry,2003,3200
    Cho,Li,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,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 contacts at the same time. If you choose to create new subscriber accounts with existing contact data, you must also include the ALIAS column header 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 VPIM 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 To help prevent others from sending e-mail to VPIM subscribers, you may want to include the HIDE_IN_ADDRESS_BOOK column header, and enter a 1 (one) in each row of subscriber data.

A value of 1 indicates that subscribers will be hidden from the e-mail address book; a value of 0 indicates that subscribers will be displayed.

Step 9 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 10 Confirm that each row contains the appropriate data corresponding to each column header.

Step 11 Save the file as a CSV file.

Step 12 Continue with the following "To Create VPIM Subscriber Accounts by Using the Cisco Unity Bulk Import Wizard" procedure.

To Create VPIM 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. See 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 **VPIM**.

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 7-26 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 7-26.

If you had no import errors, or if all errors have now been corrected, see the "After Creating Subscriber Accounts" section on page 7-27.

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 "To Correct Errors That Occurred When Importing Data from a CSV File" 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 7-27.

Using the Cisco Unity Administrator to Create VPIM Subscriber Accounts

By using the Cisco Unity Administrator, you can create VPIM subscriber accounts one at a time. When you add a new VPIM subscriber account, Cisco Unity creates a contact in Active Directory.

To create an VPIM subscriber account, do the following "To Add a New VPIM Subscriber by Using the Cisco Unity Administrator" procedure.

To Add a New VPIM 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 **VPIM** from the list.

Step 4   Enter the First Name and Last Name.

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

After Creating Subscriber Accounts

After creating VPIM 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.
- 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, see 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 VPIM Subscribers" section on page 7-54 for details.

Customizing VPIM Subscriber Directory Update Settings

In addition to manually creating, modifying, and deleting VPIM subscribers, you can configure Cisco Unity to automatically update records in the VPIM subscriber directory based on information contained in incoming VPIM messages. The settings that control whether or not the creation, modification, and deletion actions occur automatically, and how the incoming information is used to create or modify a record, can be individually configured for each delivery location. By default, no automatic directory updates will occur for any VPIM delivery locations.

Depending on the Subscriber Creation settings you choose for each delivery location, Cisco Unity will use information either from the header of an incoming VPIM message, or from a vCard attachment included with the message (if more than one vCard attachment is included, only the vCard in the most recent portion of the message will be used). If a VPIM message is received from a sender on a delivery location that is configured to allow automatic VPIM subscriber creation, and no existing VPIM subscriber matches the information of the sender, a new VPIM subscriber record will be created, provided that the VPIM message contains:

• a phone number

• a text name

• a domain name

• a recorded voice name (when required, based on the delivery location configuration)

Additional Subscriber Creation settings on the Delivery Location page allow you to specify which template to use when creating VPIM subscribers, how to map the parsed text name of the VPIM subscriber to a first name, last name, and display name, and how to map the phone number to an extension.

If a VPIM message is received from a sender on a delivery location that is configured to allow automatic VPIM subscriber modification, and an existing VPIM subscriber matches the sender information, the VPIM subscriber may be updated. You can choose whether VPIM subscriber information is updated each time a message is received from a VPIM subscriber, or only when a message is received from a VPIM subscriber whose text name has changed since the directory entry was created. You can also decide whether or not to allow an update to the display name when a modification is made.

If a message from a Cisco Unity subscriber to a VPIM subscriber results in a non-delivery receipt (NDR), indicating that the message was undeliverable because the intended recipient does not exist (SMTP 5.1.1), and if the delivery location is configured to allow automatic VPIM subscriber deletion, the VPIM subscriber will be deleted.

For additional information on how Cisco Unity uses the information from incoming VPIM messages and NDRs to create, modify, and delete VPIM subscribers, see the "Automatic VPIM Subscriber Directory Updates" section on page 7-46.

You can update the VPIM delivery location subscriber creation settings by using the Cisco Unity Administrator or the Cisco Unity Bulk Location Import wizard. See the following sections:

- Changing the AD Location in Which Automatically Created VPIM Subscribers Are Created (Optional), page 7-31

Before Configuring VPIM Subscriber Creation Settings

Before configuring the VPIM delivery location subscriber creation settings, consider the following:

- If an incoming VPIM message or NDR does not contain a vCard, and the delivery location is configured to use the vCard as the source of directory update information, no update will be made.

- If you have pre-populated VPIM subscribers with specific display names that should not be changed, but want to allow automatic modification of other fields in the subscriber record, you may choose to keep the Allow VPIM Subscriber Display Name Updates check box unchecked. In this case, the first name, last name, and spoken name of a subscriber may be modified during an automatic update. This may result in a mismatch if the spoken name is updated and the display name is not.

- When the Allow VPIM Subscribers Without Recorded Voice Names check box is unchecked, new VPIM subscribers will not be created for incoming messages that do not contain an Originator-Spoken-Name attachment. In addition, if automatic modification of VPIM subscribers is enabled, and if the sender of an incoming message matches an existing VPIM subscriber, the VPIM subscriber will be deleted if the attachment is not present in the message.

- When the Allow VPIM Subscribers Without Recorded Voice Names check box is checked, and automatic modification of VPIM subscribers is enabled, if the sender of an incoming message that does not include an Originator-Spoken-Name attachment matches an existing VPIM subscriber, the existing recorded voice name will be deleted.

- If the phone number in an incoming message can not be successfully mapped to an extension by using the option selected for the Map VPIM Subscriber Extensions To setting, a VPIM subscriber will not be created for the sender.

When determining whether to use vCards or message headers as the source from which to obtain the VPIM subscriber information, consider the following:

- Not all VPIM-compliant voice messaging systems send vCards with every message; for such systems, use message headers as the source.

- Every VPIM message includes a message header, but it is possible that the header may not include the text name of the sender, in which case it would be necessary to use vCards for obtaining sender information.

- vCards can provide information about the sender in a more detailed format. For example, the vCard can include names already parsed into first name and last name, so that Cisco Unity does not need to make a determination as to how to parse a single name field from the message header. The vCard may also include a phone number that could be mapped directly to the extension of the VPIM subscriber, so that Cisco Unity does not need to parse the header information to create an extension in the format desired. Or, it may contain a distinct number that it would not be possible for Cisco Unity to generate from the message header based on the set of rules available.

- If the remote voice messaging system is also a Cisco Unity server, it is possible to turn on or off the transmission of vCards, so the configuration of the locations should be coordinated between systems.

Using the Cisco Unity Administrator to Configure VPIM Subscriber Creation Settings

After you create a delivery location, you can configure the settings that control automatic directory updates for that specific delivery location by using the Cisco Unity Administrator.

To Configure VPIM Subscriber Creation Settings by Using the Cisco Unity Administrator

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

Step 2   Check the check box for each type of update—creation, modification, or deletion—that you would like to allow for this location. If you choose to enable automatic modification of VPIM subscribers for this location, indicate whether modifications should occur:

- **Only When the Text Name Changes**—The VPIM subscriber record will be updated only when the text name received in the VPIM message does not match the name of the VPIM subscriber.

- **With Each VPIM Message**—Every incoming VPIM message from a remote sender at this delivery location will result in an update to the corresponding VPIM subscriber.

Step 3   Select an option for the source from which to obtain the VPIM subscriber information—either the vCard or the message headers.

Step 4   Select the template on which to base newly created VPIM subscriber accounts.

Step 5   Indicate whether VPIM subscriber display name updates should be allowed.

Step 6   Indicate whether VPIM subscribers without recorded voice names should be allowed.

Step 7   Indicate how text names that do not contain commas should be parsed into first and last names for auto-created VPIM subscribers, if the remote messaging system transmits the text name as one single field. Select one of the following:

- **Treat as FirstName LastName**

- **Treat as LastName FirstName**

Step 8   Indicate how text names on incoming messages should be mapped to the display names for auto-created VPIM subscriber entries. Select one of the following:

- **Directly to VPIM Subscriber Display Names**—Click this option to have the display names for VPIM subscribers match their corresponding text names.

- **Custom Mapping**—Click this option and enter a rule that defines how text names will be mapped to VPIM 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 semicolon unless it appears at the beginning of the rule. In addition, always follow one of these tokens with a space, comma or semicolon unless it appears at the end of the rule. No additional characters are required at the beginning or end of a rule.

Step 9   Indicate how the phone number on incoming messages should be mapped to the extension for auto-created VPIM subscribers. Select one of the following:

- **Phone Number**—Click this option for extensions to be the same as the phone numbers that are parsed from incoming VPIM messages.

- **Phone Number – Remote Phone Prefix**—Click this option for extensions to be formed by removing the remote phone prefix from the beginning of the phone number.

- **Location Dial ID + Phone Number**—Click this option for extensions to be formed by adding the location Dial ID in front of the phone number.

- **Phone Number + Location Dial ID – Remote Phone Prefix**—Click this option for extensions to be formed by removing the remote phone prefix from the beginning of the phone number, and then adding the location Dial ID in front of the resulting number.

This mapping is applied only to create the extension for the VPIM subscriber; it is not applied to the remote mailbox number.

Step 10   Click the **Save** icon.

Using the Cisco Unity Bulk Import Wizard to Configure VPIM Subscriber Creation Settings

After you have created delivery locations and reviewed the considerations for creating subscriber accounts, you can customize the subscriber creation settings that control automatic VPIM subscriber directory updates for multiple existing delivery locations by using the Cisco Unity Bulk Import wizard. Or, you can create new delivery locations and customize the subscriber creation settings for the new locations at the same time. In either case, you configure each of the subscriber creation settings by including an optional column in the CSV file that you create for use in the wizard (the columns are not required when creating or modifying a delivery location, but if you include any one of the subscriber creation columns, you must include them all).

See the Cisco Unity Bulk Import wizard Help for a description of each of the optional columns that control subscriber creation. For more information on using the wizard to create or modify delivery locations, see the "Using the Cisco Unity Bulk Import Wizard to Create VPIM Delivery Locations" section on page 7-20 or the "Modifying Existing Delivery Locations by Using the Cisco Unity Bulk Import Wizard" section on page 7-22.

Changing the AD Location in Which Automatically Created VPIM Subscribers Are Created (Optional)

By default, all automatically created VPIM subscribers are placed in the Active Directory container that was specified in the Message Store Configuration wizard during Setup. If you want to have auto-created VPIM subscribers created in a different location, you can configure Cisco Unity to use any properly configured container or organizational unit. Separating the auto-created contacts from other AD objects allows you to more easily monitor and control these objects. However, we do not recommend that you attempt to change the container used for subscriber creation unless you are familiar with Active Directory objects and permissions.

If you choose to change the container for auto-created contacts, note the following:

- New VPIM subscribers that are created manually by using the Cisco Unity Administrator will still be created in the default AD container that was selected in the Message Store Configuration wizard.

- Existing VPIM subscribers that have been manually created will not be relocated to the container selected for auto-created contacts. However, if an automatic modification or deletion is initiated for one of these accounts, Cisco Unity will update the account properly in the default container.

- If auto-created VPIM subscribers have already been created in the current container, or you wish to move existing manually created VPIM subscribers, you can move the existing contacts to the new container by using Active Directory Users and Computers.

Use the following task list to set up the container or organizational unit and to configure Cisco Unity to use it when automatically creating VPIM subscribers:

1. Identify the Active Directory location in which the auto-created contacts will be created. This can be an object of the class Container or Organizational Unit (OU). To create a new container, use a tool such as ADSI Edit. Or, to create a new OU, see the "To Create a New Organizational Unit" procedure on page 7-32.

2. Set applicable permissions for the Cisco Unity service account on the Active Directory container or OU that you selected in Task 1. To set up permissions by using the Permissions wizard, see the "To Set Permissions on the AD Location by Using the Permissions Wizard" procedure on page 7-32. Or, to manually set the specific permissions required on the container, see the "To Set Permissions on the AD Location by Using Active Directory Users and Computers" procedure on page 7-32.

3. Obtain the distinguished name of the container or OU. See the .

4. Use the Advanced Settings tool to change the container in which auto-created VPIM subscribers will be created. See the .

To Create a New Organizational Unit

Step 1   On the Windows Start menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.

Step 2   In the console tree, right-click any node or folder, and click **New > Organizational Unit**.

Step 3   Enter a name for the organizational unit, and click **OK**.

To Set Permissions on the AD Location by Using the Permissions Wizard

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

Step 2   In the left pane of the Tools Depot window, expand **Administration Tools**.

Step 3   Double-click **Permissions Wizard**.

Step 4   Click **Next** without changing any options until you arrive at the Set Active Directory Containers for New Objects page.

Step 5   Select the domain and the applicable container or organizational unit in which Cisco Unity will create new users (in this case, VPIM subscribers).

> **Note**   The Permissions wizard only has the ability to grant permissions—it does not remove any permissions. Following this procedure will add the necessary permissions on the container or OU that you select, but will not remove permissions that are already granted on other containers for Cisco Unity.

Step 6   Click **Next** and follow the prompts to complete the Permissions wizard.

To Set Permissions on the AD Location by Using Active Directory Users and Computers

Step 1   On the Windows Start menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.

Step 2   Click **View > Advanced Features** (if it is not already selected).

Step 3   Right-click the container or OU in which the auto-created contacts are to be created, and click **Properties**.

Step 4   Click the **Security** tab.

Step 5   Click **Add**.

Step 6   Select from the list the account that Cisco Unity directory services log on as (typically this is UnityDirSvc).

Step 7   Click **Add**, then click **OK**.

Step 8   Click **Advanced**.

Step 9   Select the permission entry for the account that you selected in Step 6, and then click **View/Edit**.

Step 10   In the Apply Onto list, select **This Object Only** (if it is not already selected).

Step 11   In the Allow column of the Permissions list, check the **Create Contact Objects** check box, and click **OK**.

Step 12   Click **View/Edit**.

Step 13   In the Allow column of the Permissions list, check the **Read All Properties, Write All Properties** check box, and click **List Contents**.

Step 14   Click **OK** twice, and exit Active Directory Users and Computers.

To Obtain the Distinguished Name of the Container or Organizational Unit

Step 1   On the Windows Start menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.

Step 2   Right-click the container or OU in which the auto-created contacts are to be created, and click **Properties**.

Step 3   Click the **Object** tab. The fully qualified domain name of the object is displayed in the dialog box. For example, if the fully qualified domain name is ecsbu-paris.cisco.com/Unity-VPIM:

- If the object is a Container, the distinguishedName is
  CN=Unity-VPIM,DC=ecsbu-paris,DC=cisco,DC=com

- If the object is an Organizational Unit, the distinguishedName is
  OU=Unity-VPIM,DC=ecsbu-paris,DC=cisco,DC=com

To Change the AD Location in Which Automatically Created VPIM Subscribers Are Created

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 – Change AD Location Where VPIM Contacts Are Created**.

Step 4   In the New Value box, enter the distinguished name of the container to use.

Step 5   Click **Set**.

Step 6   Click **Exit**.

Step 7   Stop and restart the CsVPIMConnector service on the VPIM bridgehead server(s). You do not need to restart Cisco Unity to enable the change.

Extending Identified Subscriber Messaging to Include VPIM Subscribers

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

- Installation with Multiple Cisco Unity Servers Networked via Digital Networking, page 7-34
- Single-Server Installations, page 7-34
- Setting Permissions on Active Directory Containers Used for Importing Subscribers, page 7-35
- Enabling Identified Subscriber Messaging, page 7-35
- Extending Identified Subscriber Messaging, page 7-36

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 VPIM 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 on page 2-15.

2. The servers must be configured to be in the same dialing domain, as described in the "Customizing the Primary Location" section on page 7-18.

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 2-7.

4. The applicable permissions on each server must be set, as described in the "Setting Permissions on Active Directory Containers Used for Importing Subscribers" section on page 7-35.

5. Identified subscriber messaging on each server must be enabled as described in the "Enabling Identified Subscriber Messaging" section on page 7-35.

6. Identified subscriber messaging on each server must be enabled for VPIM subscribers as described in the "Extending Identified Subscriber Messaging" section on page 7-36.

Single-Server Installations

In installations with only one Cisco Unity server, enabling ISM to include VPIM 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 7-18.

2. The applicable permissions must be set, as described in the "Setting Permissions on Active Directory Containers Used for Importing Subscribers" section on page 7-35.

3. Identified subscriber messaging must be enabled as described in the "Enabling Identified Subscriber Messaging" section on page 7-35.

4. Identified subscriber messaging must be enabled for VPIM subscribers as described in the "Extending Identified Subscriber Messaging" section on page 7-36.

Setting Permissions on Active Directory Containers Used for Importing Subscribers

If you will be importing contacts from two or more containers (for all of the Cisco Unity servers combined), the Cisco Unity message store services account on each Cisco Unity server must be granted SendAs permission on every container from which contacts will be imported on every Cisco Unity server in the forest. Otherwise, identified subscriber messaging may not work between Cisco Unity servers. For example, if CiscoUnityServer1 will import contacts from Container1 and Container2, and if CiscoUnityServer2 will import contacts from Container3 and Container4, Cisco Unity message store services account on each Cisco Unity server must have SendAs permission for all four containers.

To Set the Applicable Permissions

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, expand **Administration Tools**.

Step 3   Double-click **Permissions Wizard**.

Step 4   Do the following:

- Choose the same Active Directory account for the Cisco Unity message store services account:
  - Click **Next** without changing any options until you arrive at the Choose the Cisco Unity Message Store Services Account page.
  - Choose the same Active Directory account for the Cisco Unity message store services account on every Cisco Unity server.
- Choose the applicable containers:
  - Click **Next** without changing any options until you arrive at the Choose Active Directory Containers for Import page.
  - Choose all of the containers from which users will be imported for every Cisco Unity server in the forest.

Step 5   Click **Next** without changing any options until you complete the wizard.

Step 6   Repeat Step 1 through Step 5 on each Cisco Unity in the forest.

Enabling Identified Subscriber Messaging

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 **Disable Identified Subscriber Messaging** 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 VPIM 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.

Gathering Information About Cisco Unity to Configure Another Voice Messaging System for VPIM

Configuring another voice messaging system to exchange VPIM messages with Cisco Unity may require the following information:

- The server name and domain name of the Exchange (or relay) server that handles incoming SMTP messages. Depending on your network, this may or may not be the same server on which the Voice Connector and VPIM Transport Event Sink are installed.

- The Cisco Unity phone prefix (if any) and Remote phone prefix (if any) entered on the corresponding delivery location page.

- Mailbox number range for Cisco Unity subscribers.

Incoming VPIM messages must be routed to the Exchange server on which the Voice Connector and VPIM Transport Event Sink are installed. When defining a location for Cisco Unity on the remote voice messaging system, use the domain name that you entered for the SMTP Transport Event Sink during the Voice Connector setup program.

Cisco Unity expects incoming VPIM messages to be formatted as follows: <UnityPhonePrefix+UnitySubscriberExtension@PrimaryLocationSMTPDomainName>. These specific properties are configured in Cisco Unity, but similar information will need to be configured in the other voice messaging system.

VPIM Concepts and Definitions

The following sections explain VPIM concepts in detail:

Introduction to VPIM

VPIM Networking allows the exchange of voice, fax, and text messages between different voice messaging systems over the Internet or any TCP/IP network. VPIM is an industry-standard protocol based on the Simple Mail Transfer Protocol (SMTP) and the Multi-Purpose Internet Mail Extension (MIME) protocol.

VPIM enables organizations to link different voice messaging systems and to provide seamless voice message sending, receiving, forwarding, and replying between these systems. An organization can exchange messages over a TCP/IP-based intranet, or over the Internet, or a combination of the two. In simplified terms, voice messages are exchanged between the systems like regular e-mail.

Figure 7-1   ***VPIM Networking Enables Messaging Between Different Systems Over a TCP/IP Network***
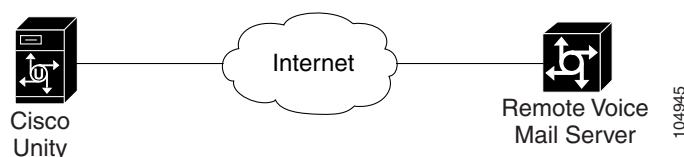
VPIM Networking also enables messaging between Cisco Unity servers that access different directories, specifically when the Cisco Unity servers are in different Active Directory forests. (When the Cisco Unity servers are in the same Active Directory forest, Digital Networking is the solution to use rather than VPIM Networking.)
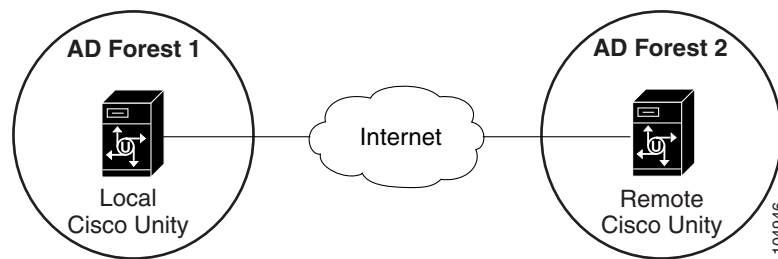
The VPIM specification defines the format of messages and message addresses, and how messages are exchanged between mail servers. VPIM does not specify how the mail servers interact with client applications, or how they interface with end users. This allows many different kinds of existing systems to support VPIM. For more information about VPIM, refer to the Open Group VPIM website.

VPIM Messages

VPIM messages are made up of one or more MIME-encoded parts. The VPIM specification allows for optional MIME parts for spoken name and for forwarded, fax, and text messages. VPIM messages can also include a vCard, an electronic business card that includes phone number, text name, and e-mail address. Cisco Unity allows you to specify whether the voice name and vCard of the sender will be sent with outgoing messages. If incoming messages include a voice name, it is played as part of the message. If a vCard is attached to an incoming message, the recipient can look at the vCard data in Cisco Unity ViewMail for Microsoft Outlook. Cisco Unity can also be configured to update the directory with information from the header or vCard data from incoming messages. For more information, see the "Automatic VPIM Subscriber Directory Updates" section on page 7-46.

VPIM fax encoding is based on the TIFF-F specification, and the vCard format is based on the Internet adaptation of the Versit vCard specification.

Figure 7-3 shows a sample VPIM message. Only a portion of the MIME encoding of the spoken name and voice message parts are shown because they are very long.

Figure 7-3   Sample VPIM Message

```
Date: Fri, 08 Nov 2002 17:39:03 GMT
From: Kelly Bader <4258001@unitydomain1.cisco.com>  ◄──────────────── From Address
To: 2534001@unitydomain2.cisco.com ◄───────────────────────────────── To Address
MIME-Version: 1.0 (Voice 2.0
Content-Type: multipart/Voice-Message; boundary="==AvVoice==1c5f4b12-
cc0f-40de-b14b-b129b17326bc"
Message-ID: edb0cc15-3ee6-44dc-aa5e-d5f88a4d68ec
Content-Transfer-Encoding: 7bit
Subject: testing


--==AvVoice==1c5f4b12-cc0f-40de-b14b-b129b17326bc
Content-Type: text/directory; charset=us-ascii; profile=vCard ◄
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment;
   filename="Kelly Bader.vcf"

BEGIN:vCard                                                            ┌── vCard Information
FN:Kelly Bader
EMAIL;TYPE=INTERNET;TYPE=VPIM:4258001@unitydomain1.cisco.com
TEL:4258001
VERSION: 3.0
END:vCard ◄

--==AvVoice==1c5f4b12-cc0f-40de-b14b-b129b17326bc
Content-Type: Audio/32KADPCM ◄
Content-Transfer-Encoding: base64
Content-Disposition: inline; voice=Originator-Spoken-Name

IkIjIyL/EiESIeId//EiIjIiHxER8fIvH+Hy/u/vHx8TH/H/H+EfEfH+/v/v/xI/ERIiLvLy8iEh
8hEeEfER/+///+/t7/3/Ee7v/e7//O8d7//+7f7+Hf///u384eL//x//8v/h8S8R8f/xER4RMR8S   ├── Spoken Name
<< The rest of the MIME encoding of the spoken name has been deleted. >>
7/8e0Q== ◄


--==AvVoice==1c5f4b12-cc0f-40de-b14b-b129b17326bc
Content-Type: Audio/32KADPCM ◄
Content-Transfer-Encoding: base64
Content-Description: VPIM Message
Content-Disposition: inline; voice=Voice-Message
Content-ID: c92d2891-1f7c-4c48-9ac3-a4194253f984

q3JT8tPcHO7vz4v+7t4e7+4/EvEy8//+/RERIjM2H/HfzPH93+79yh8+4S8hFOzBEd5Pzu0zIsFM   ┌── Voice Message
8iQT0R3tERLyMc280e4r3t3hMR4eofLPPELv4+4hP/7TIUHvHuIiH+8cv+oe7PEeH77+wR8d7CHS
/LwSXkMz4i8fztEaIfIj8fHs7d/+3xIh3KHdO97/H+7yJC7P0hFPIvIdQt8h0i4uH8T+UzHSzczT
<< The rest of the MIME encoding of the voice message has been deleted. >>

--==AvVoice==1c5f4b12-cc0f-40de-b14b-b129b17326bc-- ◄
```

114377

VPIM Addresses

A VPIM address is in the same format as a typical SMTP e-mail address: localpart@hostpart. The right-hand side of the address is the domain name of the system on the TCP/IP network that handles messages. The left-hand side of the address is a unique identifier for the user. Typically, the left-hand side is the subscriber mailbox number or the mailbox number with a prefix.

For example, an outgoing VPIM message to Terry Campbell with the remote mailbox number 2233 could be addressed:

To: 2233@remotevoicemailsystem.com

If it is necessary to accommodate the numbering plan for your organization, the address can also contain a prefix:

To: 8882233@remotevoicemailsystem.com

VPIM addresses are created by the Voice Connector when sending VPIM messages; they are not entered by subscribers when addressing messages.

VPIM Networking and Locations

Central to how you set up VPIM Networking is a Cisco Unity object called a 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. When setting up VPIM Networking, you use the Cisco Unity Administrator to give the primary location a new name and a Dial ID (which is an identifier for the location within Cisco Unity), enter the SMTP domain name, and customize other properties as applicable. See the "Primary Location Profile Settings" section on page 9-1 for more information.

You create a delivery location in the Cisco Unity Administrator to correspond to each remote voice messaging system with which Cisco Unity communicates. Delivery locations contain the information that Cisco Unity needs to exchange messages with other VPIM-compliant voice messaging systems. A VPIM delivery location contains the SMTP domain name of the system on the TCP/IP network that handles messages for the remote voice messaging system.

Location data is stored both in the SQL Server database on the Cisco Unity server and in Active Directory. In organizations with multiple Cisco Unity servers networked together, the location data replicates to all of the Cisco Unity servers in the network. This means that delivery locations need to be created only on one Cisco Unity server in the network. The Cisco Unity server on which delivery locations are created is referred to as the bridgehead server. See the "Considerations for Digitally Networked Cisco Unity Servers" section on page 7-57 for more information.

VPIM Networking and the Voice Connector

Cisco Unity uses Exchange to provide messaging between Cisco Unity and other VPIM-compliant voice messaging systems. Exchange is VPIM-transport compliant and provides the ability to send and receive messages across the Internet or any TCP/IP network to computers that support SMTP.

Before an outgoing message to a VPIM-compliant voice messaging system can be sent, it must be encoded as a MIME message. The Cisco Unity Voice Connector for Exchange 2000 handles the conversion to and from the MIME format.

The Voice Connector must be installed on an Exchange 2000 or Exchange 2003 server. If the Exchange and Cisco Unity servers are in different routing groups, a routing group connector must be installed. Although the Voice Connector can be installed on the Cisco Unity server (if Exchange is also on the server), this is not recommended for performance reasons.

The Voice Connector must not be installed on a server in an Exchange cluster. Microsoft does not support third-party connectors on an Exchange cluster server. In addition, the Voice Connector cannot be installed on an Exchange 2007 server.

How the Voice Connector Processes Outgoing VPIM Messages

When subscribers use the phone to address a message to a VPIM recipient, Cisco Unity constructs a To address for the message in the form VPIM:<Location Dial ID>_<Remote Mailbox>. As with any other message, Cisco Unity hands it off to Exchange for delivery. Because the message has a VPIM address type, it is first passed to the Voice Connector for processing.

The Voice Connector does the following tasks:

- Converts the message from MAPI to MIME format.
- Formats the To address by using the domain name and prefix specified on the corresponding VPIM delivery location page.
- Formats the From address by using the prefix from the corresponding VPIM delivery location page and the domain name from the primary location page. (If your organization has more than one Cisco Unity server networked together, the domain name is from the primary location of the Cisco Unity server with which the sending subscriber is associated.)
- Checks the delivery location for the audio format conversion setting for outbound messages to determine whether voice attachments should be converted to G.726 or remain in the format in which they were recorded.
- Checks the delivery location to determine whether messages should be decrypted.
- Attaches the recorded voice name and/or vCard, if specified on the corresponding VPIM delivery location page.

The newly formatted message is put in the SMTP pickup directory of the Windows server for delivery to the VPIM-compliant voice messaging system.

How the Voice Connector Processes Incoming VPIM Messages

When the Transport Event Sink installation program is run, a transport event sink is registered with the Windows SMTP server. A transport event sink is code that is activated through a defined trigger, such as the receipt of a new message.

The VPIM Transport Event Sink monitors all incoming messages. Messages that have the content type Multipart/Voice-Message and are addressed to the SMTP domain specified during the transport event sink installation are readdressed to the Voice Connector by the VPIM Transport Event Sink.

When the Voice Connector receives the message, it first verifies that the message is from a domain specified in a VPIM delivery location. If a VPIM delivery location with a matching domain name is not found, the Voice Connector rejects the message and sends a non-delivery receipt (NDR) to the sender.

If a VPIM delivery location with a matching location is found, the Voice Connector does the following:

- Removes the phone prefixes from the To and From addresses, if prefixes are specified on the corresponding VPIM delivery location page.
- Validates the recipient(s) of the message by looking up the extension(s) in Active Directory, and formats the address(es).
- Converts the message from MIME to MAPI format.
- Converts voice attachments to the audio format specified on the corresponding VPIM delivery location page.
- Checks the delivery location configuration to see whether automatic VPIM subscriber directory updates are enabled. If so, the Voice Connector may attempt to generate a directory update message as described in the "Automatic VPIM Subscriber Directory Updates" section on page 7-46.

- Checks the delivery location to determine whether messages should be encrypted.

- Hands the message back to Exchange for delivery to the Cisco Unity subscriber mailbox(es).

Message Addressing Options

Cisco Unity provides the following ways to address messages to individuals by using a VPIM-compliant voice messaging system:

- Blind addressing—Blind addressing allows Cisco Unity to send messages without having specific information about the recipients on the remote voice messaging system (such as their names and mailbox numbers). To address a message to someone on another voice messaging system, subscribers enter the delivery location Dial ID and the remote mailbox number of the recipient. See the "VPIM Networking and Blind Addressing" section on page 7-43 for more information.

- VPIM subscribers—With VPIM subscribers, Cisco Unity has information about the remote users, such as their names and extensions. Subscribers address messages to VPIM subscribers the same way that they address messages to regular Cisco Unity subscribers—by extension or by spelling the name of the recipient. Note that spoken name confirmation is available when a recorded name exists for the VPIM subscriber. See the "VPIM Subscribers" section on page 7-44 for more information.

Messaging Similarities and Limitations

For the most part, messaging between Cisco Unity subscribers and individuals on a VPIM-compliant voice messaging system is the same as messaging among 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.

- Subscribers can send messages to Cisco Unity distribution lists that include VPIM subscribers.

- Subscribers can send fax messages, if this is supported by the remote voice messaging system.

Note the following exceptions:

- Requests for read receipts and delivery receipts are both returned as delivery receipts.

- E-mail messages without a voice attachment cannot be sent to VPIM recipients even though ViewMail allows subscribers to address e-mail messages to them. Instead of being delivered, e-mail messages that are sent to VPIM recipients are returned to the sender as NDRs.

- When replying to VPIM messages in ViewMail, if subscribers want to send text in the reply, they must enclose the text in a text file attachment. Whether the recipient receives the text attachment depends on the capabilities of the remote voice messaging system.

- Messages that are marked as low importance in ViewMail are treated the same as regular messages.

- Messages that are sent to Cisco Unity distribution lists from subscribers on the remote voice messaging system are not delivered, and an NDR is returned to the sender. Incoming VPIM messages to Cisco Unity are delivered to subscriber mailboxes only, and cannot be delivered to public distribution lists.

- Incoming messages must be addressed to the primary extension of the subscriber; messages addressed to an alternate extension will not be delivered.

VPIM Networking and Blind Addressing

Blind addressing is one of the methods that Cisco Unity provides for addressing VPIM messages to users of another voice messaging system. Blind addressing allows Cisco Unity to address messages without having specific information about the recipients on the remote voice messaging system (such as their names and mailbox numbers). One of the steps to setting up blind addressing is to change the Blind Addressing setting on the Primary Location > Addressing Options page to something other than None. You also create a VPIM delivery location that corresponds to each voice messaging system with which Cisco Unity communicates.

You provide the following key information for each delivery location:

- Dial ID—A unique number that identifies the location to Cisco Unity. This is the number that subscribers dial when blind addressing messages to individuals who use the remote voice messaging system.

- SMTP Domain Name—The Internet-addressable SMTP domain name that is used to construct addresses for individuals who use the voice messaging system that corresponds to the delivery location.

When blind addressing a message, subscribers dial a number that is made up of the delivery location Dial ID and the mailbox number of the recipient. Before addressing the message, Cisco Unity parses the number that the subscriber enters and searches for a matching delivery location. If Cisco Unity does not find a matching location, it reports the error to the sender and does not address the message. 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 that a voice name was recorded for the delivery location).

Subscriber Experience with Blind Addressing

Subscribers can address messages by using the phone, ViewMail for Outlook, or the Cisco Unity Inbox. To address a message by using ViewMail or the Cisco Unity Inbox, subscribers enter the address in the following format:

[VPIM:<Delivery Location Dial ID>_<Remote Mailbox Number>]

Note   ViewMail requires the square brackets in the address.

Because your Cisco Unity server does not have access to the names, extensions, and recorded voice names of the people who use the other voice messaging system, subscribers will encounter some limitations with blind addressing:

- When addressing a message, the sender does not hear voice name confirmation. Cisco Unity cannot verify that the entered number is correct, so subscribers may inadvertently address a message to the wrong person or to a non-existent extension. However, subscribers will receive an NDR if the number turns out to be an invalid extension.

- When addressing a message, subscribers cannot use spelled-name mode; subscribers address the message only by using number mode, so they must know the delivery location Dial ID and the mailbox number for the recipient.

- Blind addresses cannot be added to public distribution lists.

- When subscribers use the phone to listen to messages from someone at the VPIM location, the conversation (also known as the telephone user interface, or TUI) cannot identify the sender.

- When subscribers use ViewMail for Outlook or the Cisco Unity Inbox to listen to messages from someone at the VPIM location, the From address is in the format [VPIM:<Delivery Location Dial ID>_<Remote Mailbox Number>]. Note that the sender can be identified only if the remote system included the recorded voice name of the sender in the message.

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.

Note that when you delete a delivery location, blind addressees at that location are also removed from all private lists. Consider notifying subscribers of these potential changes to their private lists.

VPIM Subscribers

VPIM subscribers are a representation in Cisco Unity of individuals who use another voice messaging system. VPIM subscribers are created in Cisco Unity to enable Cisco Unity subscribers to find them in the directory and to send them messages as they would with any other subscriber. Voice messages addressed to VPIM subscribers are sent to the voice messaging system that they use.

VPIM subscribers do not require additional Exchange 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 VPIM subscribers.

To set up VPIM subscribers, you first create a VPIM delivery location that corresponds to each remote voice messaging system with which Cisco Unity communicates. After creating the delivery locations, you create a VPIM subscriber for each remote user. When creating each VPIM subscriber, you specify the user mailbox number on the other voice messaging system, and select a VPIM delivery location with which to associate the subscriber. The Voice Connector uses the information on the associated delivery location when delivering a message to the VPIM subscriber. Note that VPIM subscribers can be created only on the VPIM bridgehead server on which the associated VPIM delivery location has been created.

You create and manage VPIM subscriber accounts in much the same way that you do regular subscriber accounts. You can use the Cisco Unity Administrator to create, modify, and delete VPIM subscriber accounts one at a time, and you can use the Cisco Unity Bulk Import wizard to create and modify multiple VPIM subscriber accounts.

Extensions are mandatory for VPIM subscribers. The extension is the number that subscribers dial when addressing a message to a VPIM subscriber. This number may or may not be the same as the mailbox number of the VPIM subscriber on the remote voice messaging system. Callers who reach the opening greeting of your organization can dial the extension of a VPIM subscriber or look up a VPIM subscriber in directory assistance and leave a message.

VPIM subscribers have corresponding contacts in Active Directory. When you delete VPIM subscribers, the underlying contacts are deleted automatically.

Other than receiving messages, VPIM subscribers do not have access to other Cisco Unity features, and some sections of the Cisco Unity Administrator are disabled for VPIM subscribers. VPIM 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, so their recorded names and greetings can only be recorded or changed in the Cisco Unity Administrator.

- Cannot use the Cisco Unity Inbox to check messages.

- Cannot own private lists.

- Cannot set up or receive message notifications.
- Cannot receive message waiting indications.

Manually setting up VPIM subscribers requires more overhead for administrators of Cisco Unity than blind addressing does. However, you can also configure automatic directory updates so that VPIM subscribers will be automatically created, modified, and deleted based on information received in incoming VPIM messages. See the "Automatic VPIM Subscriber Directory Updates" section on page 7-46 for more information.

Whether created manually or automatically, the VPIM subscriber option allows other subscribers to address messages to VPIM subscribers the same way that they address messages to regular subscribers. In general, creating VPIM subscriber accounts is a good solution in the following circumstances:

- When there are only a few subscribers at the other voice messaging system who need to receive messages from the subscribers at your location. (Note however that there are no technical constraints associated with creating large numbers of VPIM subscribers.)

- When unidentified callers need to be able to call the local Cisco Unity server to leave a message for someone on the other voice messaging system. This may provide a way for local callers to avoid long distance charges when leaving a message for a remote VPIM subscriber.

- When the functionality described in the following "Subscriber Experience with VPIM Subscribers" section is required.

Because of the administrative overhead of setting up and maintaining many VPIM subscriber accounts, you may prefer a combination of blind addressing, manual creation of VPIM subscribers, and automatic directory updates. For example, you might want to set up VPIM subscriber accounts for senior sales staff, but not for other employees. Then as Cisco Unity receives incoming messages, replies, or non-delivery receipts (NDRs) for these employees, the directory of VPIM subscribers would grow and adjust automatically.

Subscriber Experience with VPIM Subscribers

Provided that VPIM subscribers are listed in the phone directory and have had voice names and greetings recorded for them:

- Subscribers can address messages to VPIM subscribers by using the phone, ViewMail for Outlook, or the Cisco Unity Inbox.

- Contacts that correspond to VPIM subscribers are included in Exchange address lists, which means that they are listed in the Outlook address book (unless the contact has been explicitly prevented from appearing there) and in the Cisco Unity Inbox address book. Therefore, message addressing to VPIM subscribers—either by using Outlook or the Cisco Unity Inbox—is the same as for regular subscribers.

- When using the phone, subscribers can address messages to VPIM subscribers in spelled-name mode (if enabled on the system) or by extension.

- Subscribers hear voice name confirmation when addressing a message to a VPIM subscriber.

- When subscribers use the phone to listen to messages, the conversation announces who the message is from.

- VPIM subscribers can be added to private and public distribution lists.

When Cisco Unity records a message from an unidentified caller for a VPIM subscriber, "non-mail-user@<Domain Name>" is used as the sender of the message, as required by the VPIM specification. Although VPIM subscribers are not prevented from replying to these messages, the reply messages are returned to the Unity Messaging System mailbox as NDRs.

Automatic VPIM Subscriber Directory Updates

In addition to manually creating, modifying, and deleting VPIM subscribers, you can configure Cisco Unity to automatically create, update, or delete VPIM subscriber records based on information contained in incoming VPIM messages. The settings that control whether or not the creation, modification, and deletion actions occur automatically, and how the incoming information is used to create or modify a record, can be individually configured for each delivery location. By default, no automatic directory updates will occur for any VPIM delivery locations.

See the following sections for discussions of the details:

Directory Update Processing That Occurs at the Voice Connector

The directory update process begins when an incoming VPIM message is delivered from a remote voice messaging system to the Voice Connector. The Voice Connector processes the incoming message as described in the "How the Voice Connector Processes Incoming VPIM Messages" section on page 7-41. In addition to the basic process, if the delivery location that is matched to the sender is configured to allow automatic creation or automatic modification of VPIM subscribers, and if the message contains sufficient information, the Voice Connector also creates a directory update message addressed to the UVPIM_<Servername> mailbox. Depending on how the delivery location is configured, the Voice Connector will use information either from the header of an incoming VPIM message, or from a vCard attachment included with the message.

Note If more than one vCard attachment is included with a message, only the vCard in the most recent portion of the message will be used for automatic creation or modification of a VPIM subscriber account.

The vCard or header information must contain a phone number, a text name, and a domain name; if the selected source of directory information is missing one of these fields, no directory message will be created. The Voice Connector also uses this information to check for the existence of a matching contact, which will indicate whether the directory update pertains to creating a new VPIM subscriber, or to modifying an existing one.

If the processing of the incoming VPIM message at the Voice Connector results in a nondelivery receipt (NDR), the Voice Connector will not create a directory message for the sender. An NDR may instead be generated for the incoming VPIM message after it leaves the Voice Connector (for example, if the recipient mailbox is full), but in such cases, the Voice Connector will have already created the directory message.

Alternatively, the Voice Connector may receive an NDR from a remote voice messaging system in response to an outgoing message addressed to a VPIM subscriber. In this case, the Voice Connector checks the corresponding delivery location to see whether automatic deletions are enabled. For a successful deletion, the vCard or header fields in the NDR must contain a phone number and domain name, and an SMTP reason code indicating the reason for the delivery failure.

Directory Update Processing That Occurs on the Cisco Unity VPIM Bridgehead Server

The CsVPIMConnector service running on the VPIM bridgehead server monitors the UVPIM_<Servername> mailbox for directory messages. When the CsVPIMConnector service receives a directory message indicating that a new VPIM subscriber should be created, it also checks additional Subscriber Creation settings on the delivery location to determine:

- Which template to use when creating VPIM subscribers
- How to map the parsed text name of the VPIM subscriber to a first name, last name, and display name
- How to map the phone number to an extension
- Whether or not VPIM subscribers with no recorded voice names are allowed

The service uses SQL Server to create or update the VPIM subscriber on the VPIM bridgehead server. From the SQL Server database, the subscriber information is replicated to Active Directory, where a mail-enabled contact is created.

When the CsVPIMConnector service receives a directory message indicating that an existing VPIM subscriber should be modified, it checks to see whether the delivery location is configured to have the subscriber information updated with every incoming VPIM message, or only on messages where the text name has changed. The service takes the text name from the incoming message and applies the rules that have been configured to map the text name to a display name. If the option is selected that allows updates only when the text name has changed, the service compares this new display name to the display name on the VPIM subscriber record to determine whether the subscriber record should be modified. If the modification is allowed, the CsVPIMConnector service also checks to determine whether the delivery location is configured to allow display name updates. If so, the service will modify the first and last name fields and the recorded voice name, but will leave the display name unchanged. Otherwise, all of these fields will be updated.

For example, you can configure a location as follows:

- Display names will be created as "Firstname Lastname - Seattle"
- Updates are allowed only when the text name changes
- Display name updates are allowed

In this circumstance, if a VPIM subscriber exists with the display name "Jessie Smith - Seattle" and an incoming message is received from Jessie Smith, no action will be taken. If the display name for Jessie Smith on the remote system is changed to "Jess Smith," a modification will be triggered the next time Cisco Unity receives an incoming message, and the first name and display name will be updated accordingly.

In other cases, a last name may change or a given mailbox number may be reassigned to a new person, so it is not recommended that modifications be allowed while display names updates are disallowed, as this could result in a first and last name contradicting the display name. The rule for mapping display names can be configured so that most desired display name conventions can be maintained when VPIM subscribers are automatically created or modified.

When the CsVPIMConnector service receives a directory message indicating that an existing VPIM subscriber should be deleted, it checks the reason code included in the message. If the reason code indicates that the mailbox does not exist (SMTP error code 5.1.1), the CsVPIMConnector service will delete the VPIM subscriber record. All associated objects and properties, including public and private distribution list membership, will be deleted from the SQL Server database on the VPIM bridgehead server. From the SQL Server database, the change will be replicated so that the Active Directory contact is removed.

If the VPIM bridgehead server is configured for failover, automatic VPIM subscriber updates will not occur while the secondary server is active, as the CsVPIMConnector service will run only on the primary server. However, while the primary server is unavailable, the Voice Connector continues to generate directory update messages, which will be processed as soon as the primary server becomes active again.

Population of VPIM Subscriber Information

Depending on a setting configured for each delivery location, VPIM subscribers can be created, updated, or deleted by using information either from the header of an incoming VPIM message, or from a vCard attachment included with the message (if more than one vCard attachment is included, only the vCard in the most recent portion of the message will be used). Additional delivery location options allow you to specify how certain fields from the vCard or header are mapped to VPIM subscriber fields. Table 7-1 shows the source of various fields when either the vCard or header fields are used to generate VPIM subscriber information. It also includes information on the delivery location Subscriber Creation configuration settings that can affect how the CsVPIMConnector service maps this data to the fields in a VPIM subscriber record.

Table 7-1   VPIM Subscriber Information

Subscriber Field	Source for Field When vCard Is Used	Source for Field When Headers Are Used	Notes
First Name	• N property, Given Name or • Text name contained in the FN (formatted name) property	• Text name contained in the From address For example, if the From address contains "Terry Bader<8882233 @remotevoicemailsystem. com>", the text name used as the source of the first name would be Terry Bader.	If the first name is derived from a single text name field (from the FN property of a vCard or the From address of the message header), the setting When the Text Name Has No Comma can be applied to determine which part of the text name field is considered the first name.
Last Name	• N property, Family Name or • Text name contained in the FN (formatted name) property	• Text name contained in the From address For example, if the From address contains "Terry Bader<8882233 @remotevoicemailsystem. com>", the text name used as the source of the last name would be Terry Bader.	If the last name is derived from a single text name field (from the FN property of a vCard or the From address of the message header), the setting When the Text Name Has No Comma can be applied to determine which part of the text name field is considered the last name.
Display Name	• N property, Given Name and Family Name or • FN property	• Text name contained in the From address For example, if the From address contains "Terry Bader<8882233 @remotevoicemailsystem. com>," the text name used as the source of the display name would be Terry Bader.	The display name is derived from the appropriate source field according to the rule specified in the Mapping Text Names setting. If the N property of the vCard is used and Mapping Text Names set is set to Directly to VPIM Subscriber Display Names, the display name will be set to Family Name, Given Name (this corresponds to Last Name, First Name).

Table 7-1   VPIM Subscriber Information (continued)

Subscriber Field	Source for Field When vCard Is Used	Source for Field When Headers Are Used	Notes
Extension	One of the following: • TEL property with no qualifier • TEL property with qualifier TYPE=voice • Mailbox number in the header From address	• Mailbox number in the From address For example, if the From address contains "Terry Bader<8882233 @remotevoicemailsystem. com>", the mailbox number used as the source of the extension would be 8882233.	The extension is derived from the appropriate source field according to the rule specified in the Map VPIM Subscriber Extensions To setting. Note that this field is set only when the subscriber is created, and will not be changed by an automatic modification, even if the rule for mapping extensions has changed. If you wish to change the rule, extensions for existing VPIM subscribers can be changed manually using the Cisco Unity Administrator or the Bulk Edit tool.
Recorded Voice Name	• Originator-Spoken-Name attachment	• Originator-Spoken-Name attachment	The Voice Connector converts the audio, by using the codec specified for inbound audio conversion on the associated delivery location, before including it in the directory message.
Remote Mailbox Number	One of the following: • TEL property with no qualifier • TEL with qualifier TYPE=voice • Mailbox number in the header From address	• Mailbox number in the From address For example, if the From address contains "<8882233@remote voicemailsystem.com>", the Remote Mailbox Number would be 8882233.	If a remote phone prefix is specified for the delivery location, the prefix is removed from the source number to create the remote mailbox number. The rule applied to map the TEL property or mailbox number to a VPIM subscriber extension is not applied to the remote mailbox number.

Non-numeric characters in the source data for the extension field are removed when creating the VPIM subscriber extension; for example, if the TEL property is used and contains the number (555)888-2233, the subscriber extension would be formed from the digits 5558882233. If the rule that is configured for mapping the incoming phone number data cannot be successfully applied, the creation of the VPIM subscriber will fail.

When the CsVPIMConnector service automatically creates VPIM subscribers, the Active Directory contact is given an alias in the following format:

VPIM_<DeliveryLocationDialID>_Extension

The service will also apply the subscriber template that is specified in the delivery location configuration when the VPIM subscribers are created.

Subscriber Addressing Considerations with Automatic Updates

The information contained in a VPIM subscriber account can be used to aid subscribers in addressing messages to remote mailboxes (by providing spell-by-name and spoken name confirmation, for example). However, note that regardless of whether blind addressing or VPIM subscriber information is used by the sender to indicate the desired recipient of a VPIM message, ultimately the message is addressed and sent to a numerical mailbox ID on the remote system. As such, there is no mechanism for confirmation that the name information that the local subscriber uses to address an outgoing message matches the actual current owner of the remote mailbox.

Even with automatic updates in place, situations may arise where a subscriber believes he or she is sending a message to one person at a remote site, but the mailbox has changed hands since the VPIM subscriber account was created, and the new owner of the mailbox actually receives the message. Because of the usage-based nature of the updates, if no VPIM message has been received from the new owner of the remote mailbox before a local subscriber attempts to address to it, the subscriber will encounter the outdated name information belonging to the original mailbox owner (including the spoken name of the original owner), with no indication that the mailbox has changed hands.

Another situation may arise in which two VPIM subscriber accounts exist for the same person on the remote system. In the case where a subscriber on a remote VPIM system changes mailbox numbers, and a VPIM subscriber account exists for that sender on Cisco Unity, the existing account will not be updated to change the mailbox number. Instead, when a Cisco Unity subscriber addresses a message to the VPIM subscriber with the outdated mailbox number, if an NDR is received from the remote system indicating that the mailbox no longer exists, the original VPIM subscriber account will be deleted. Then, at whatever point the remote subscriber sends a message to a Cisco Unity subscriber, a new VPIM subscriber account is created for the remote subscriber. Note that these two events can happen in either order; if the remote subscriber sends a message before the local subscriber attempts to send an outgoing message to the outdated mailbox number, VPIM subscriber accounts will exist for the remote subscriber with both the old and new mailbox numbers. A local subscriber who attempts to address a message to that remote subscriber by using spell-by-name will hear both matches at this point, with different extensions. The outdated VPIM subscriber account will not be deleted unless a subscriber addresses a message to it and receives an NDR.

If the events occur in the opposite order—if a subscriber sends a message to a VPIM subscriber that results in an NDR and the deletion of the VPIM subscriber account before an incoming message is received from the new mailbox number of the remote subscriber—the sender will receive the NDR but will not have updated VPIM subscriber information to use in readdressing the message. In this case, the sender would need to use blind addressing to address further messages to the recipient, until an incoming message is received from the recipient, which will result in the creation of a new VPIM subscriber account.

CsVPIMConnector Logging

Both micro and macro traces are available for the CsVPIMConnector service. If detailed logging is required for troubleshooting purposes, these traces can be enabled and collected using the Cisco Unity Diagnostic tool (UDT). Otherwise, the CsVPIMConnector logs summary information by default for each directory message that it processes. This information is logged to a data file named data_CsVPIMConnector_<date>_<time>.txt, in the Cisco Unity trace logs directory. The default location of the trace logs is the CommServer\Logs directory.

The data is written to the file in comma-separated format. Table 7-2 describes the fields in the order that they are written to the data file.

Table 7-2   CsVPIMConnector Data Log File Columns

Field	Contents
UTC Time Stamp	Time the directory message was processed in Coordinated Universal Time (UTC).
Logging Process Name	AvRepMgr_MC
Logging Process Number	30311
Local Time Stamp	Time the directory message was processed in the time zone of the Cisco Unity server.
Subscriber Display Name	If the VPIM subscriber display name has been successfully generated according to the rule specified in the Mapping Text Names setting, the display name is listed here; otherwise, the name as received in the VPIM message is listed.
Location Dial ID	The dial ID of the delivery location from which the original VPIM message was received.
Subscriber DTMF ID	If the VPIM subscriber extension has been successfully generated according to the rule specified in the Map VPIM Subscriber Extensions To setting, the extension is displayed here; otherwise, 'Invalid' is listed.
Action Type Code	One of the following: • 13001—create • 13002—delete • 13003—modify
Action Status Code	One of the following: • 15000—error • 15001—completed successfully
Error Status Code	One of the following: • 100—success • 101—extension conflict • 102—alias conflict • 103—remote address conflict • 104—invalid name • 105—invalid parameter • 106—subscriber not local • 107—subscriber not found • 108—invalid extension See Table 7-3 for a further description of each error status code.
Subscriber Status Code	One of the following: • 0—global • 1—local • 2—not found

Table 7-3   CsVPIMConnector Error Status Code Descriptions

Error Status Code	Description
100 (success)	Successful attempt to create, modify, or delete the subscriber.
101 (extension conflict)	Attempt to create a subscriber with an extension that already exists in the directory.
102 (alias conflict)	Attempt to create a subscriber with an alias that already exists in the directory.
103 (remote address conflict)	Attempt to create a subscriber with a remote address that already exists in the directory.
104 (invalid name)	The VPIM message was received with only a single name field (both a first and last name are required to create or modify a subscriber).
105 (invalid parameter)	Parameter used for attempted creation was invalid (for example, an invalid subscriber template or container for creation was specified, or there were insufficient permissions to create the subscriber in the specified container).
106 (subscriber not local)	Modification or deletion requested for a subscriber that is found in the global subscriber table, but not in the local subscriber table.
107 (subscriber not found)	Modification or deletion requested for a subscriber that cannot be found.
108 (invalid extension)	Extension creation rules specified for the location cannot be applied to the phone number received or the extension generated is longer than 40 digits.

Identified Subscriber Messaging

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. 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.

Live Reply to VPIM Subscribers

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 choosing the "call the subscriber" option to have Cisco Unity call the subscriber directly. 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 VPIM 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 VPIM subscribers.

Note that a live reply to a VPIM 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 VPIM 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 VPIM subscriber and hangs up, leaving the phone system to handle the call. Note the following limitations with release to switch transfers:

- The VPIM 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 VPIM 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 VPIM subscribers is enabled automatically, and cannot be disabled.

- Live replies to VPIM 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 VPIM subscriber with a subscriber account on another Cisco Unity server, the servers must be in the same dialing domain.

Deleting VPIM Subscribers

Each VPIM subscriber is associated with an Active Directory contact. When you delete VPIM subscribers in the Cisco Unity Administrator by deleting the subscriber accounts individually, the underlying contacts are automatically deleted. To delete all of the VPIM subscribers associated with a delivery location, the underlying contacts associated with the subscribers, and the delivery location itself, use the Global Subscriber Manager, available in Tools Depot. Note that when you delete a VPIM delivery location, blind addressees are also removed from all private lists. Consider notifying subscribers of these potential changes to their private lists.

If enabled by the delivery location Subscriber Creation settings, Cisco Unity can automatically delete VPIM subscribers when non-delivery receipts are received from the delivery location in response to messages that are sent to VPIM subscribers. For further information, see the .

Extension Addresses

When you create a VPIM subscriber, Cisco Unity automatically generates an e-mail address in the following format:

VPIM:<Delivery Location Dial ID>_<Remote Mailbox Number>

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 VPIM subscriber is associated, and the Remote Mailbox Number of the VPIM subscriber. Each contact in Active Directory that corresponds to a VPIM subscriber contains an extension address.

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

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

Determining How VPIM Subscribers Appear in the Outlook Address Book

Depending on your installation, the users of the remote voice messaging system may already have Active Directory accounts and Exchange mailboxes on your local network that they use for e-mail. Therefore, when VPIM subscriber accounts are created for them, the Exchange address lists will contain duplicate listings—the existing user account that is used for e-mail and a new contact that is used only for voice mail. Both listings are included in the Outlook address book. This means that people may inadvertently send e-mail messages to the contact, which should be used only for addressing voice messages.

To discourage people from inadvertently sending e-mail messages to VPIM subscribers, you can prevent the associated contact from appearing in the Outlook address book. Alternatively, you can change how the display name for the contact appears in the Outlook address book so that subscribers can distinguish the contact from a user account. In this way, you can reduce the number of e-mail messages inadvertently sent to contacts and simplify addressing for those who send voice messages to VPIM subscribers at the same time.

Either before or after you create VPIM subscriber accounts, you can prevent the associated contact from appearing in the Outlook address book by hiding the contacts from Exchange address lists. When you do so, Exchange will still deliver e-mail messages addressed to an existing user account (if one exists)

and to the contact. However, the number of e-mail messages that are sent to the contact may be reduced because subscribers cannot inadvertently pick the contact from the Outlook address book when addressing messages to them.

To prevent subscribers from appearing in Outlook address books, you can use the Cisco Unity Administrator, the Cisco Unity Bulk Import wizard, Bulk Edit, or Active Directory Users and Computers:

- To do so in the Cisco Unity Administrator, uncheck the Show Subscriber In E-Mail Server Address Book check box on the Profile page for the subscriber template that you plan to use when creating VPIM subscribers, or on individual subscriber Profile pages after you have created the subscriber accounts.

- To do so by using the Cisco Unity Bulk Import wizard or the Bulk Edit utility, see the Help for each tool.

- To do so in Active Directory Users and Computers, click View > Advanced Features to see the Exchange Advanced property page for a user, and then check the Hide From Exchange Address Lists check box on the Exchange Advanced tab.

As an alternative to preventing a contact from appearing in the Outlook address book altogether, you may want to alter the display name for the contact so that subscribers can distinguish the contact from the user account. For example, you could append "- Voice mail" to the display name of each VPIM subscriber, and the names would appear in the Outlook address book as follows:

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

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

You can specify rules, per delivery location, for how the display names of auto-created VPIM subscribers are generated from the text names that Cisco Unity receives in incoming messages from senders on each remote messaging system.

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 who are 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.

Migrating Subscribers from Another Voice Messaging System to Cisco Unity

If you are using VPIM to migrate from another voice messaging system to Cisco Unity, there are several tools that you can use to create Cisco Unity subscribers from VPIM subscriber information. See the following sections for more information:

- Migrating Subscribers in Bulk, page 7-56
- Migrating Subscribers One at a Time, page 7-57
- Private List Considerations for Migrating Subscribers, page 7-57

Migrating Subscribers in Bulk

Following are the general steps for migrating VPIM subscribers to Cisco Unity subscribers, in bulk. See the Help files of the applicable tools for more detailed information. (Click the Tools Depot icon on the Cisco Unity server, and click the applicable tool in the left pane to view the Help file.)

1. As a best practice, back up the Cisco Unity server (just as a precaution, because you will be deleting data).

2. Run Subscriber Information Dump from Tools Depot, and output the VPIM subscriber information to a CSV file.

3. Modify the CSV file as needed so that you can use it as the input file when you use the Cisco Unity Bulk Import wizard to create Cisco Unity subscribers.

4. Run Global Subscriber Manager from Tools Depot to delete the VPIM delivery locations and the associated VPIM subscribers and underlying contacts.

5. If the people migrating from the remote voice messaging system do not already have Active Directory accounts and Exchange mailboxes, create them. Alternatively, you can let the Cisco Unity Bulk Import wizard create the accounts.

6. Run the Cisco Unity Bulk Import wizard by using the input file that you prepared in Step 3.

Migrating Subscribers One at a Time

If you have set up VPIM subscriber accounts for the subscribers on another voice messaging system, and if they have existing Exchange mailboxes, you can use the Migrate Subscriber Data utility when the time comes to migrate them to Cisco Unity. The Migrate Subscriber Data utility creates a Cisco Unity subscriber account by combining the Cisco Unity-specific data from an existing VPIM subscriber account (such as the voice name) with an existing mail user. The utility then deletes the VPIM subscriber account and the associated Active Directory contact.

The Migrate Subscriber Data utility is available in Tools Depot (the Tools Depot icon is installed on the Cisco Unity server desktop). See the Help file that comes with the utility for more information.

Private List Considerations for Migrating Subscribers

When you migrate VPIM subscribers, consider notifying Cisco Unity subscribers of these potential effects on private distribution list membership:

- When you delete a delivery location, blind addressees are removed from all private lists.
- When a VPIM subscriber becomes a regular subscriber, the VPIM subscriber is removed from all private lists.

Considerations for Digitally Networked Cisco Unity Servers

A small subset of subscriber and distribution list data is stored in Active Directory, as is most location data. In organizations with multiple Cisco Unity servers networked together such that they access a common directory, the Cisco Unity-specific data replicates to all Cisco Unity servers in the network. Therefore, all Cisco Unity servers on the network have the information that subscribers need to address messages to users at a VPIM location.

Because of directory replication, VPIM delivery locations and VPIM subscribers need to be created only on one Cisco Unity server in the network. If allowed by the primary location addressing options on each server, all subscribers, no matter which Cisco Unity server they are associated with, can send messages to a VPIM delivery location or to a VPIM subscriber created on another server. The Cisco Unity server configured for VPIM acts as the VPIM "bridgehead" server for the other Cisco Unity servers in the network.

Phone Prefixes

Each VPIM delivery location provides the following prefixes, which are used to accommodate various numbering plans:

- Remote Phone Prefix—This number is used to construct addresses for users at a VPIM location. On outgoing messages to the VPIM location, the Voice Connector adds the prefix to the beginning of the recipient mailbox number to form the To address. On incoming messages from the VPIM location, the Voice Connector removes the prefix from the beginning of the sender mailbox number to form the From address.

- Cisco Unity Phone Prefix—This number is used to construct addresses for Cisco Unity subscribers. On outgoing messages to the VPIM location, the Voice Connector adds the prefix to the beginning of the sender mailbox number to form the From address. On incoming messages from the VPIM location, the Voice Connector removes the prefix from the beginning of the recipient mailbox number to form the To address.

If all VPIM delivery locations have a unique domain name, prefixes are optional. If you have multiple delivery locations with the same domain name, the Remote Phone Prefix is required. Within the set of delivery locations with the same domain name, the Remote Phone Prefix must be a unique number.

For example, assume that an organization has implemented a 10-digit numbering plan, in which the mailbox numbers for Cisco Unity subscribers begin with 206, and the mailbox numbers of subscribers on a VPIM voice messaging system begin with 425.

Assume the following has been set on the VPIM delivery location:

- Dial ID = 425
- Remote Phone Prefix = 425

By setting both the Remote Phone Prefix and the Dial ID to 425, the number that a subscriber enters when blind addressing a message to someone at the VPIM location is the same number that the subscriber enters when calling the person.

Because of the prefix, VPIM subscribers are assigned a 7-digit Remote Mailbox Number. In this example, for outgoing messages the Voice Connector would add the prefix 425 to the beginning of the remote mailbox number, creating a 10-digit recipient mailbox number.

Audio Format Considerations

The Audio Format Conversion settings on the VPIM delivery location page in the Cisco Unity Administrator allow you to control the audio format of outgoing and incoming VPIM messages, as follows:

- Outbound Messages—You can set whether outbound VPIM messages are converted to G.726 or sent in the format in which they were recorded (no audio format conversion).

- Incoming Messages—You can set whether incoming VPIM messages are converted to G.711 (mu-law), GSM 6.10, G.729a, or stored in the format in which they were sent (no audio format conversion).

To make decisions about these settings, consider the following:

- The audio format that the local Cisco Unity server (or servers, if there are multiple Cisco Unity servers networked together) uses for recording and playing voice messages.

- The audio format in which the remote voice messaging system can send and receive VPIM messages. Some voice messaging systems support only the G.726 format for VPIM messages, but you will need to consult the documentation of the remote voice messaging server to be sure.

- Network bandwidth.

We recommend that incoming VPIM messages be stored in the same audio format that the local Cisco Unity server(s) use for recording and playing messages. However, if you want incoming VPIM messages to be stored in some other audio format, you will need to verify that the applicable codec is installed on all Cisco Unity servers and on other computers that access these messages. In particular:

- If your organization has multiple Cisco Unity servers networked together, all of the Cisco Unity servers must have the codec installed.

- If subscribers use ViewMail for Outlook or the Cisco Unity Inbox to listen to messages, the codec may need to be installed on each subscriber workstation.

The Voice Connector converts the audio format of incoming and outgoing VPIM messages according to the settings on the VPIM delivery location. The Voice Connector requires both the codec that the VPIM message is being converted from and the codec that the VPIM message is being converted to. Depending on the audio format conversion, you may need to install the applicable codec on the Exchange server on which the Voice Connector is installed, as follows:

- G.711 and GSM 6.10—The Voice Connector uses the codecs that Windows installs. You may want to verify that the codecs are still installed on the Exchange server.

- G.729a and G.726—The Voice Connector uses its own copies of the G.726 and G.729a codecs, so these codecs do not need to be installed on the Voice Connector Exchange server. (Note that the Voice Connector will add a RIFF header to an incoming message in the G.726 format if the header is missing. Without the RIFF header, Windows-based audio players will be unable to play messages.)

- OKI ADPCM—To convert messages from the OKI ADPCM audio format, the OKI ADPCM codec must be installed on the Exchange server on which the Voice Connector is installed.

- Other codecs—To convert messages from other audio formats, the applicable codec must be installed on the Exchange server on which the Voice Connector is installed.

Related Documentation

- For general information about audio formats supported by Cisco Unity, see the *Audio Codecs and Cisco Unity* white paper, at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

- For information specific to messaging between Cisco Unity servers in different directories, see the .

Maintenance

This section provides information on various tasks that you may need to maintain your VPIM Networking configuration. See the following sections for details:

Changing the IP Address of a Microsoft Exchange Server

Depending on your network, after changing the IP address of a Microsoft Exchange server, you may need to update the Exchange SMTP virtual server settings on all other Microsoft Exchange servers in your network to reflect the new IP address so that VPIM messages are delivered correctly.

To Check and Update the SMTP Virtual Server Relay List on Exchange 2000 or Exchange 2003

Step 1   On the Microsoft Exchange server, on the Windows Start menu, click **Programs > Microsoft Exchange > System Manager**.

Step 2   In the tree on the left, expand **Servers\<Server name>\Protocols\SMTP**.

Step 3   Right-click **Default SMTP Virtual Server** and select **Properties**.

Step 4   Click the **Access** tab.

Step 5   Click **Relay**.

Step 6   Do one of the following:

- If All Except the List Below is selected and the new server IP address does not appear in the list, skip to Step 11.

- If All Except the List Below is selected and the new server IP address appears in the list, click the IP address and click **Remove**, then skip to Step 10.

- If Only the List Below is selected, continue with Step 7.

Step 7   Click **Add**.

Step 8   Click **Single Computer**, and enter the new IP address of the server that changed addresses.

Step 9   Click **OK**.

Step 10   Verify that the **Allow All Computers Which Successfully Authenticate to Relay, Regardless of the List Above** check box is checked.

Step 11   Click **OK** twice to close the Properties dialog box.

Step 12   Close the **Exchange System Manager**.

Step 13   Repeat Step 1 through Step 12 on each Microsoft Exchange server in your network.

To Check the IP Addresses on Receive Connectors on Exchange 2007

Step 1   Open **Exchange Management Console**.

Step 2   For each Hub Transport and Edge Transport Receive connector:

a.   Right-click the **Receive** connector and click **Properties**.

b.   Click the **Network** tab.

c.   Review the listed IP addresses to see if any changes are needed.

Step 3   Close Exchange Management Console.

Moving the UVPIM Mailbox

For information on moving the UVPIM mailbox, see the "UVPIM Mailbox" section in the "Cisco Unity Data and Log Files" chapter of the *Maintenance Guide for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Notable Behavior

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

- Call Transfer Settings and VPIM Subscribers, page 7-61
- Inbound Messages Are Delivered Only to Primary Extensions, page 7-62
- Inbound Search Scope, page 7-62
- Running the Voice Connector Setup Program in Another Language, page 7-63

Call Transfer Settings and VPIM 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 7-4, 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 7-4   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 VPIM 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 VPIM subscriber. (Live replies to VPIM subscribers are always done release to switch, even when the reply is to a VPIM subscriber on the same Cisco Unity server.)

- A caller enters the extension of a VPIM subscriber from the automated attendant (for example from the opening greeting), and the VPIM subscriber account is on another Cisco Unity server.

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

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

- The VPIM 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 VPIM 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.

Inbound Messages Are Delivered Only to Primary Extensions

When addressing a message to a Cisco Unity subscriber, users on the remote voice messaging system must use the primary extension of the Cisco Unity subscriber; alternate extensions are not supported. Senders will receive an NDR if they address a message with the alternate extension of a Cisco Unity subscriber.

Note also that Cisco Unity does not accept messages from a remote voice mail system that are sent to Cisco Unity public distribution lists, call handlers, and interview handlers. Cisco Unity accepts messages from a remote voice mail system only when they are sent to a subscriber primary extension.

When designing the numbering plan for Cisco Unity subscribers, as a best practice, configure the primary extension of all Cisco Unity subscribers with the extension that will be used for addressing from the remote voice mail system. Configure all other required extensions as alternate extensions, as all other functionality in Cisco Unity can use alternate extensions.

Inbound Search Scope

In installations with multiple Cisco Unity servers networked together, the search scope for a matching subscriber extension for inbound messages that are sent from another VPIM-compliant voice messaging system 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.

If two (or more) Cisco Unity subscribers have identical extensions, messages from the remote voice messaging system will not be delivered by the Voice Connector to any of the Cisco Unity subscribers with the duplicate extensions. When the Voice Connector detects duplicate extensions, it NDRs the message back to the sender and logs a warning to the Windows Application Event log. If you are concerned that there might be duplicate extensions among Cisco Unity subscribers, you can check the Application Event log on the Exchange server on which the Voice Connector is installed for warnings from the Exchange 2000 Voice Connector.

Running the Voice Connector Setup Program in Another Language

The Voice Connector installation program does not prompt with a choice of languages for the installation; it always installs in English. To run the Voice Connector installation program by using one of the localized versions (FRA, DEU, or JPN) instead of English, do the following procedure.

⚠
Caution   Installing the Voice Connector on an Exchange 2007 server is not supported.

To Run the Voice Connector Setup Program in Another Language

Step 1   From the Cisco Unity installation DVD or CD 1, copy the entire VoiceConnector-Ex2000 to your hard disk.

Step 2   In this local directory, browse to the **LocalizedFiles\ENU** directory.

Step 3   Rename the CiscoUnity_VoiceConnector.dll and SetupRes.dll files. (For example, rename the files CiscoUnity_VoiceConnector_ENU.dll and SetupRes_ENU.dll.)

Step 4   Copy the files **CiscoUnity_VoiceConnector.dll** and **SetupRes.dll** from the LocalizedFiles\<XXX> directory (where <XXX> is your language of choice) to the Localized\ENU directory.

Step 5   Run **Install.exe** from the VoiceConnector-Ex2000 directory on your hard disk. The installation program should be presented in the language you chose.

✎
Note   Only the installation program will be in this language; currently, the Event Log messages, logging, properties, and configuration settings are not localized.

Notable Behavior

Using VPIM for Networking with Cisco Unity Express or Other Cisco Unity Systems

For the most part, configuring VPIM Networking for messaging between Cisco Unity systems, and between Cisco Unity and Cisco Unity Express, is the same as between Cisco Unity and a third-party voice mail system. For example, VPIM Networking can be used for messaging in the following cases:

- Between Cisco Unity systems where the partner Exchange servers are in different Active Directory forests.
- Between Cisco Unity with Exchange 2000 or Exchange 2003 and Cisco Unity with Domino.
- Between Cisco Unity and Cisco Unity Express.

However, there are some special considerations that you should be aware of when configuring VPIM Networking for messaging between Cisco Unity systems.

See the following sections for details:

Messaging Between Cisco Unity Servers in Different Directories

Generally, when setting up VPIM Networking for Cisco Unity servers in different directories, you configure the Cisco Unity servers just as you would for VPIM Networking with any other voice messaging system. However, there are some settings that need to be coordinated between the Cisco Unity servers, as explained in the following sections:

Correspondence Between Locations

As Figure 8-1 illustrates, you create a VPIM delivery location on the local Cisco Unity server to correspond to each remote Cisco Unity Bridgehead server. Typically, the Domain Name that you enter on the delivery location matches the Domain Name for the corresponding primary location on the remote Cisco Unity server and vice versa. However, the domain names that you enter depend on your e-mail addresses/recipient policy. In addition, the Dial ID and Display Name on the local delivery location are typically the same as the Dial ID and Display Name on the remote primary location and vice versa (this is for convenience only and is not a requirement). If prefixes are needed to accommodate numbering plans and subscriber dialing habits, enter applicable prefixes on the local and/or remote delivery locations.

Figure 8-1   *Correspondence Between Locations*
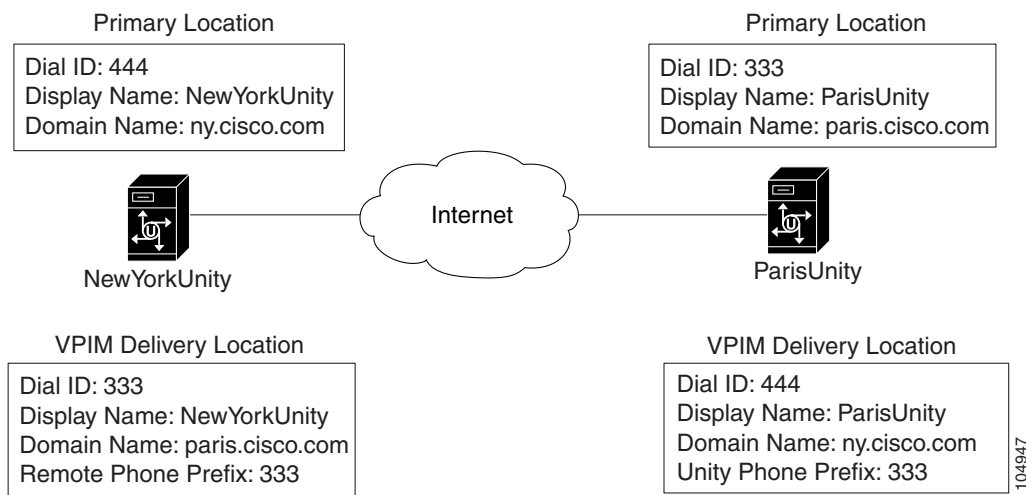
VPIM Subscribers Correspond to Remote Cisco Unity Subscribers

If you do not want to use blind addressing, you can create VPIM subscriber accounts on the local server that correspond to subscribers on the remote Cisco Unity server. On the remote Cisco Unity server, VPIM subscriber accounts can be created that correspond to the Cisco Unity subscribers on your local server. Figure 8-2 illustrates the relationship of VPIM subscribers to remote Cisco Unity subscribers.

By creating VPIM subscribers, you manually duplicate the subscriber directory of the remote Cisco Unity server on the local server, and vice versa. Such a setup provides the benefits listed in the "Subscriber Experience with VPIM Subscribers" section on page 7-45.

In addition to manually creating VPIM subscribers, you can configure Cisco Unity to automatically update the VPIM subscriber directory based on information contained in VPIM messages that are received from the remote Cisco Unity server. You configure the settings for automatic directory updates on the delivery location that corresponds to the remote Cisco Unity server. If the remote Cisco Unity server is configured to include the vCard of the sender in outgoing messages, you can specify that the vCard be used as the source of information for the directory update. Otherwise, the message headers can be used instead. By default, no automatic directory updates will occur. For further information about enabling automatic updates and configuring these settings, see the "Customizing VPIM Subscriber Directory Update Settings" section on page 7-28.

Figure 8-2   VPIM Subscribers That Correspond to Remote Cisco Unity Subscribers
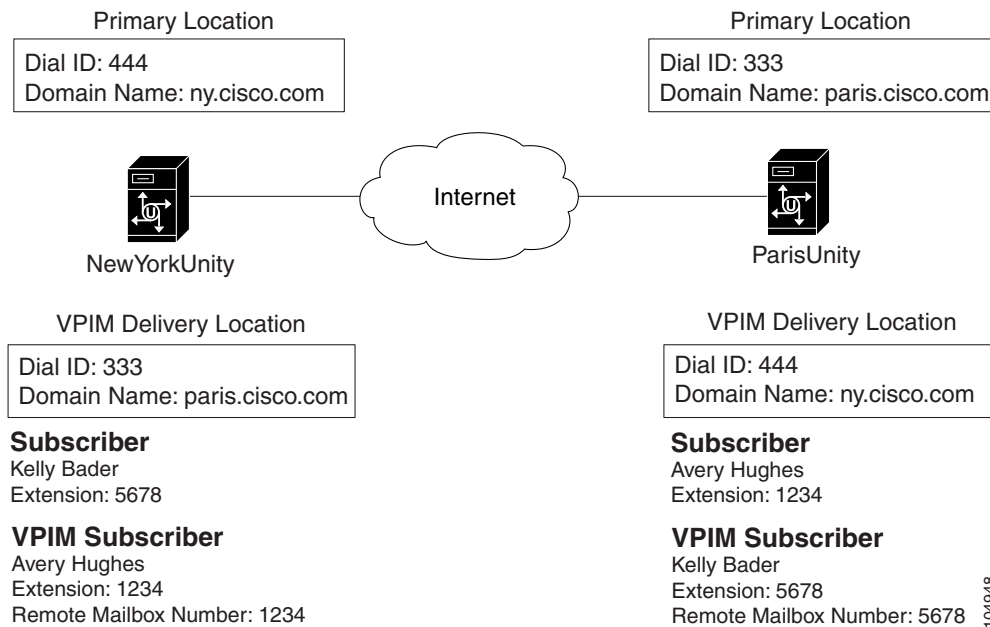
Audio Format Conversion Settings

When using VPIM Networking for messaging between Cisco Unity servers in different directories, the Audio Format Conversion Settings for outbound and incoming messages need to be coordinated on the Cisco Unity servers to avoid unnecessary conversions. When making decisions about the conversion settings:

- Consider the network bandwidth between the local and remote Cisco Unity servers, and the volume of message traffic.
- Determine which codecs are installed or will need to be installed on subscriber workstations and Cisco Unity servers in the local and remote sites.

The following examples show a few of the combinations of the Audio Format Conversion Settings to give you an idea of the options.

Example 1: Both Cisco Unity Servers Use G.729a for Recording and Storage

As shown in Figure 8-3, both the local and remote Cisco Unity servers record messages by using the G.729a codec. At 8 Kbps, the G.729a codec is recommended for use when network bandwidth is an issue. Because of theses considerations, no audio format conversions are needed when messages are transmitted between the servers.

Figure 8-3   No Audio Format Conversions
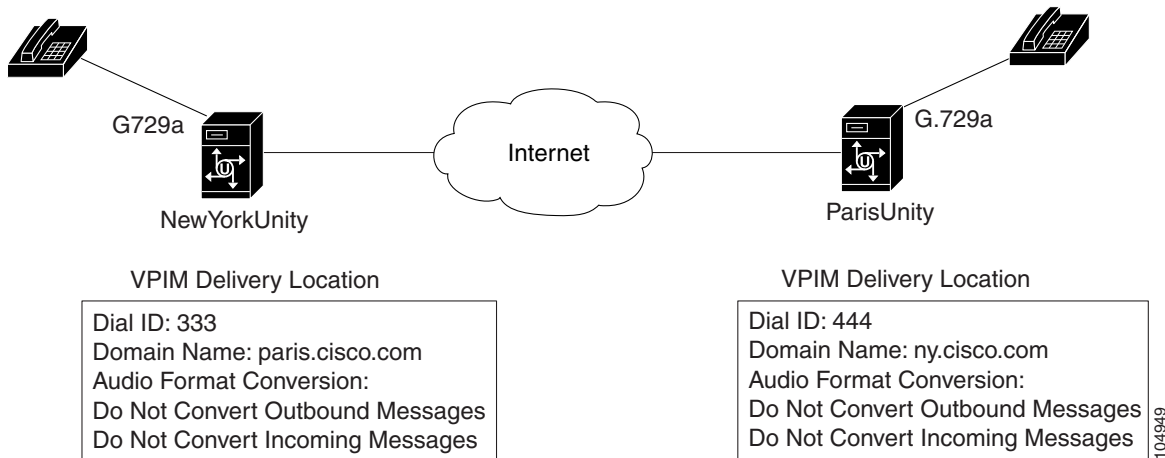
Example 2: Both Cisco Unity Servers Use G.711 for Recording and Storage

It is also possible for both the local and remote Cisco Unity servers to record messages by using the G.711 codec. At 64 Kbps, messages encoded by using the G.711 codec are very high quality, but because of their size, the messages may present a problem if network bandwidth is a concern. In this case, you have the following options:

- Do not convert outbound and incoming VPIM messages, but monitor the network for problems. Sending VPIM messages in the G.711 format may not turn out to be an issue, particularly if message traffic between the sites is light.

- Configure each server to convert outbound messages to G.726, and convert incoming messages back to G.711. At 32 Kbps, messages encoded by using the G.726 codec are half the size of those encoded by using G.711. The downside to this approach is that it results in two audio format conversions for each VPIM message. This is extra work for the Voice Connector. In addition, when incoming messages are converted back to G.711, there may be a loss in sound quality.

- Configure each server to convert outbound messages to G.726, but not to convert incoming messages. This approach solves the network bandwidth concern and results in only one audio format conversion for each VPIM message. However, G.726 is not supported as a region (line) format for a Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) integration. Also, if VPIM messages are stored in G.726, all Cisco Unity servers and subscriber workstations must have the G.726 codec installed. (The G.726 codec is installed on the Cisco Unity server during setup.)

- Change the codec that will be used by the Cisco Unity servers to record messages from G.711 to G.729a, and do not convert the audio format of VPIM messages.

Example 3: One Cisco Unity Server Uses G.711 and the Other Uses G.729a

Consider the case where one Cisco Unity server uses G.711 for recording and storage and the other uses G.729a. If network bandwidth is not an issue:

On the Cisco Unity server that uses G.711	• Do not convert outbound messages. • Do not convert incoming messages.
On the Cisco Unity server that uses G.729a	• Do not convert outbound messages. • Do not convert incoming messages.

Cisco Unity can transcode messages recorded and stored in multiple formats, so the best option is to not convert outbound or incoming VPIM messages. This approach avoids the overhead of audio format conversions.

If network bandwidth is an issue, and you want to continue recording messages in G.711:

On the Cisco Unity server that uses G.711	• Convert outbound messages to G.726. This resolves the network bandwidth issue because the outbound messages will be sent in the G.726 32Kbps format, which is half the size of G.711 messages. • Do not convert incoming messages. In general, if a message is recorded and stored in a lower quality codec, and then later converted to a higher quality codec, the sound quality does not improve, so there is no benefit to converting the incoming G.729a messages to G.711.
On the Cisco Unity server that uses G.729a	• Do not convert outbound messages. At 8Kbps, the G.729a is the best codec to use when there are network bandwidth issues. • For incoming messages, your options are: – Convert incoming messages to G.729a. Although this results in an additional audio format conversion, presumably all subscriber workstations are already configured for G.729a, because that is the codec used by the Cisco Unity server. – Do not convert incoming messages, and leave them in G.726. Although this avoids another conversion, G.726 is not supported as a region (line) format for a Cisco Unified Communications Manager integration. Also, if VPIM messages are stored in G.726, all Cisco Unity servers and subscriber workstations must have the G.726 codec installed.

Messaging Between Cisco Unity and Cisco Unity Express Servers

Generally, when setting up VPIM Networking between Cisco Unity and Cisco Unity Express, you configure the Cisco Unity servers just as you would for VPIM Networking with any other voice messaging system. However, there are some settings that need to be coordinated between the Cisco Unity and Cisco Unity Express servers, as explained in the following sections:

- Correspondence Between Locations, page 8-6
- VPIM Subscribers Correspond to Cisco Unity Express Subscribers, page 8-6

> ✎
> **Note**   For information on the versions of Cisco Unity Express that are supported for VPIM Networking with Cisco Unity, see the list of supported VPIM voice messaging systems in *Supported Hardware and Software, and Support Policies for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Correspondence Between Locations

You create a VPIM delivery location on the local Cisco Unity server to correspond to each remote Cisco Unity Express server. Typically, the Domain Name that you enter on the delivery location when configuring Cisco Unity matches the Domain Name configured for the network local location on the Cisco Unity Express server. Similarly, when configuring Cisco Unity Express, the Domain Name that you enter for the network location that corresponds to the Cisco Unity server typically matches the Domain Name configured for the primary location on Cisco Unity. For convenience, you may wish to also match the Dial ID and Display Name for each delivery location in the same way. If prefixes are needed to accommodate numbering plans and subscriber dialing habits, enter applicable prefixes on the local and/or remote delivery locations.

VPIM Subscribers Correspond to Cisco Unity Express Subscribers

If you do not want to use blind addressing, you can create VPIM subscriber accounts on the local server that correspond to subscribers on remote Cisco Unity Express servers. In addition to manually creating VPIM subscribers, you can configure Cisco Unity to automatically update the VPIM subscriber directory based on information contained in VPIM messages that are received from Cisco Unity Express servers. On the Cisco Unity server, you configure the settings for automatic directory updates on the delivery location that corresponds to each Cisco Unity Express server. If the Cisco Unity Express system is configured to include the vCard of the sender in outgoing messages, you can specify that the vCard be used as the source of information for the directory update. Otherwise, the message headers can be used instead. By default, no automatic directory updates will occur. For further information about enabling automatic updates and configuring these settings for Cisco Unity, see the "Customizing VPIM Subscriber Directory Update Settings" section on page 7-28.

On remote Cisco Unity Express servers, administrators or other privileged users can add remote users to the local directory by using the Administration via Telephone (AvT) feature. If the Cisco Unity Express system has vCard information enabled, incoming vCard information updates the remote user directory as well as a dynamic cache of remote users. For directory and cache size limits and other details on remote subscriber handling in Cisco Unity Express, see the Cisco Unity Express documentation, at http://www.cisco.com/en/US/products/sw/voicesw/ps5520/tsd_products_support_series_home.html.

Additional Functionality

In addition to the standard functionality available when using the VPIM protocol to exchange voice messages with remote voice messaging systems, certain extended functionality is available when Cisco Unity is connected via VPIM to other Cisco Unity or Cisco Unity Express servers. The following section provides further information.

Networked System Broadcast Messages

System broadcast messages are recorded announcements sent to everyone in an organization (or to particular location(s) within an organization). System broadcast messages are played immediately after subscribers log on to Cisco Unity by phone—even before they hear message counts for new and saved messages. Subscribers must listen to each system broadcast message in its entirety before Cisco Unity allows them to hear new and saved messages or to change setup options. They cannot fast-forward or skip a system broadcast message.

Note   System broadcast messages do not light message waiting indicators (MWIs) on subscriber phones, nor do they cause distinctive dial tones to notify subscribers of a new message when they pick up their desk phone receiver. System broadcast messages also do not trigger message notifications for alternative devices, such as a pager or another phone.

A system broadcast message can be sent to all subscribers on one or more Cisco Unity servers that access the same subscriber directory, by addressing the message to the delivery location Dial ID of the desired server. For more information, see the "Setting Up System Broadcast Messaging for Sending to All Subscribers in the Directory (Optional)" section on page 2-10.

In organizations where there are multiple Cisco Unity servers that access different directories, system broadcast messages can be sent to all subscribers in the organization (or to all subscribers associated with specific sets of digitally networked servers) by setting up public distribution lists that include VPIM subscribers representing each location where subscribers should receive the message. A similar approach can also be used to include all subscribers on a Cisco Unity Express server in the distribution of a system broadcast message.

Note   A system broadcast message sent to one or more VPIM locations contains special attributes that mark the message as a system broadcast, and a start date and an end date that indicate when the message should be made available to subscribers. This feature is intended for use with remote Cisco Unity and Cisco Unity Express locations that support these attributes. If the message is addressed to other types of remote locations by adding VPIM subscribers from those locations to the public distribution list, or if the public distribution list contains Cisco Unity, Internet, AMIS, or Bridge subscribers, these attributes will be ignored by those distribution list members, and they will receive the message as a regular voice message.

Addressing System Broadcast Messages to Multiple Servers

Depending on how multiple Cisco Unity and Cisco Unity Express servers are connected, system broadcast messages can be addressed to all subscribers on all servers, or to all subscribers on a subset of servers in the organization. Figure 8-4 illustrates addressing in an organization with multiple networks of servers connected via VPIM.

Figure 8-4   System Broadcast Messages Can Be Addressed to Subscribers on Multiple Servers in an Organization
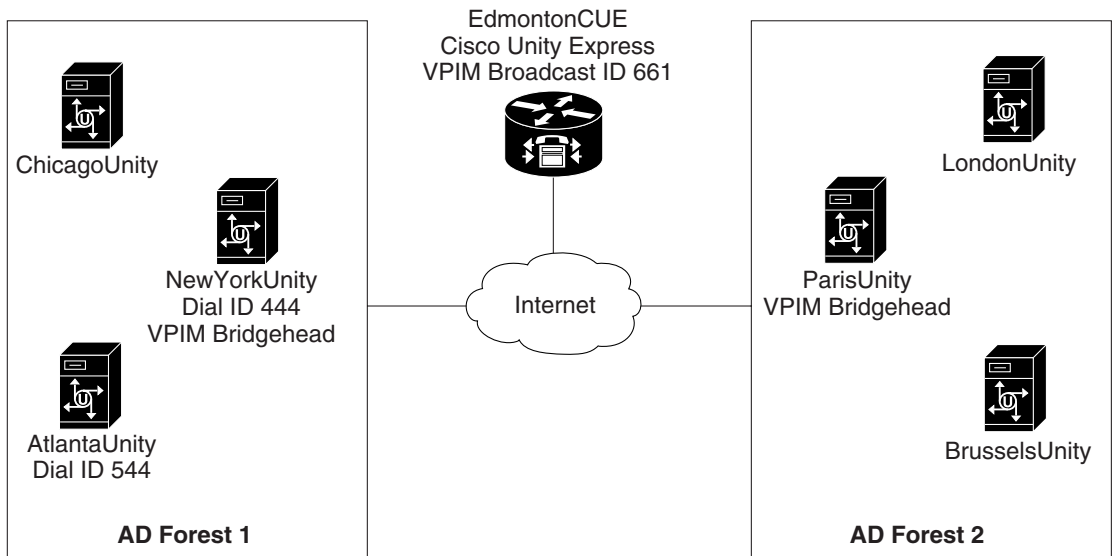
Example 1: Addressing a System Broadcast Message Within the Directory by Using the Digital Networking Configuration

A subscriber on ChicagoUnity who has been granted permission to send system broadcast messages to subscribers on multiple servers can address a message from the Cisco Unity Broadcast Message Administrator by using the options shown in Table 8-1, which result in a system broadcast message being transmitted to all subscribers on the local server or to all subscribers on multiple servers within the directory (ADForest1). These options use the existing Digital Networking configuration; no additional configuration is required.

Table 8-1   Using the Cisco Unity Broadcast Administrator to Address Messages to Servers Within the Directory

Cisco Unity Broadcast Administrator Option Selected	Extension Entered	System Broadcast Message Recipients
Send to Subscribers on This Server	N/A	All subscribers on ChicagoUnity
Send to Subscribers at All Locations	N/A	All subscribers on all Cisco Unity servers in ADForest1—ChicagoUnity, NewYorkUnity, and AtlantaUnity
Send to One or More Locations, or to a Public Distribution List	444	All subscribers on NewYorkUnity (dial ID 444)
Send to One or More Locations, or to a Public Distribution List	444, then 544	All subscribers on NewYorkUnity (dial ID 444) and AtlantaUnity (dial ID 544)

Example 2: Addressing a System Broadcast Message by Using Public Distribution Lists to Reach VPIM Locations

In the next example, an administrator configures the following objects on the VPIM bridgehead server in ADForest1:

Table 8-2 **Cisco Unity VPIM Subscriber Configuration for VPIM Example**

Name	Remote Mailbox Number	Description
SysBroadcast-HalifaxCUE	661	VPIM subscriber at location HalifaxCUE
SysBroadcast-ADForest2	Any unused remote mailbox number	VPIM subscriber at any location in ADForest2

Table 8-3 **Cisco Unity Public Distribution List Configuration for VPIM Example**

Name	Extension	Description
SBM_DL1	111	Public Distribution List Members: • SysBroadcast-HalifaxCUE
SBM_DL2	222	Public Distribution List Members: • SysBroadcast-ADForest2
SBM_DL3	333	Public Distribution List Members: • SysBroadcast-HalifaxCUE • SysBroadcast-ADForest2 • USbms_ChicagoUnity • USbms_NewYorkUnity • USbms_AtlantaUnity (The USbms_<Servername> mailbox for each of the Cisco Unity servers in ADForest1 has been manually added to the public distribution list using Exchange tools.)

With the additional configuration from Table 8-2 and Table 8-3, a subscriber on ChicagoUnity who has been granted permission to send system broadcast messages to subscribers on multiple servers can address a message from the Cisco Unity Broadcast Message Administrator by using the options shown in Table 8-4, which results in a system broadcast message being transmitted to all subscribers on multiple servers by using VPIM Networking.

Table 8-4 **Using the Cisco Unity Broadcast Administrator to Address Messages to Distribution Lists**

Cisco Unity Broadcast Administrator Option Selected	Extension Entered	System Broadcast Message Recipients
Send to One or More Locations, or to a Public Distribution List	111	All subscribers on HalifaxCUE
Send to One or More Locations, or to a Public Distribution List	222	All subscribers in ADForest2
Send to One or More Locations, or to a Public Distribution List	333	All subscribers on HalifaxCUE, in ADForest2, and in ADForest1

How Networked System Broadcast Messages Are Processed by Cisco Unity

When Cisco Unity is installed, a new Windows service called CsBMsgConnector is created, along with a special mailbox that has the display name USbms_<Servername>. The USbms mailbox is created in the default directory container for Cisco Unity, and is hidden from the address book. The CsBMsgConnector service processes messages that are placed in the USBms mailbox. For systems that use failover, the CsBMsgConnector service runs on both the primary and secondary servers, and both services access the same USbms mailbox, but only the service on the currently active server will process messages.

When a VPIM message is received with attributes indicating that it is a system broadcast message, the Voice Connector first verifies that the message is from a domain specified in a VPIM delivery location. If a VPIM delivery location with a matching domain name is not found, the Voice Connector rejects the message and sends a non-delivery receipt (NDR) to the sender.

If a VPIM delivery location with a matching domain is found, the Voice Connector does the following:

- Removes the remote phone prefix from the From address, if the prefix is specified on the corresponding VPIM delivery location page. (If a remote phone prefix is specified, the beginning digits of the sender ID must match the prefix, or the message will be rejected and an NDR sent.)

- Converts voice attachments to the audio format specified on the corresponding VPIM delivery location page.

- Addresses the message to all USbms_<Servername> mailboxes in the directory and hands the message back to Exchange for delivery.

The CsBMsgConnector service on each Cisco Unity server then processes the message and makes it available to all Cisco Unity subscribers on the server, based on the start and end dates that are configured for the message.

Note In order to update any properties on a system broadcast message after it has been sent to multiple locations, the local copy of the message on each server must be updated directly on that server. On each Cisco Unity server, a subscriber with access to the Cisco Unity Broadcast Message Administrator and permission to update system broadcast messages on the local server can change the properties or delete the message for that server. On each Cisco Unity Express server, the system administrator can change the properties or delete the message for that server by using the command-line interface.

Considerations for Networked System Broadcast Messages

To include one or more VPIM locations in the distribution of a system broadcast message, you first create an VPIM subscriber for each location, and then add the VPIM subscriber to a public distribution list. In the Cisco Unity Broadcast Message Administrator, you address the message by specifying the public distribution list number. (When you are prompted to enter the extension of a location or public distribution list, the Cisco Unity Broadcast Administrator allows you to enter only the dial ID of a digitally networked Cisco Unity server, or the extension of a public distribution list; it will not recognize extensions for VPIM subscribers or other types of objects).

Note the following considerations when setting up distribution lists to be used for sending networked system broadcast messages:

- At this time, Cisco Unity with Domino only supports sending and receiving system broadcast messages that are recorded and addressed to subscribers on the local server. Although VPIM Networking can be used for messaging between Cisco Unity with Exchange and Cisco Unity with Domino, Cisco Unity with Domino servers should not be included in networked system broadcast message distribution lists.

- Any members of the public distribution list that are not VPIM subscribers will receive the message as a regular voice message rather than as a system broadcast message, and the message properties such as start and end date will not be respected. For Cisco Unity subscribers, this also means that the message will be delivered to the subscriber mailbox and will be included in the total mailbox size for the subscriber. For these reasons, we do not recommend that you add non-VPIM subscribers to the distribution list.

- Including any VPIM subscriber at a remote Cisco Unity delivery location that supports networked system broadcast messages in the public distribution list will cause the system broadcast message to be directed to all subscribers on all Cisco Unity servers that are digitally networked with the remote VPIM bridgehead server. It is not possible to restrict the system broadcast message to a particular server or set of servers on the remote network.

- For Cisco Unity Express delivery locations, a VPIM subscriber must be created specifically for each Cisco Unity Express server. The remote mailbox number configured on the VPIM subscriber account in Cisco Unity must match the number configured for the system broadcast mailbox on the Cisco Unity Express server.

- Only one system broadcast message should be sent as a VPIM networked message to each remote location. In other words, only one VPIM subscriber per remote Cisco Unity Express system or Cisco Unity domain needs to be included in the public distribution list being used. The receiving system will distribute the message to all local users. However, if for some reason the remote location receives more than one copy of the same system broadcast message, only the first one will be processed and subsequent ones received with the same message ID will be discarded.

- To include specific digitally networked Cisco Unity servers in the distribution list along with VPIM locations, you can manually add the system broadcast mailbox of each desired server in the public distribution list. Because the Cisco Unity Administrator does not allow you to select a subscriber for these mailboxes, you must use Exchange tools to add the mailbox to the distribution list. The system broadcast mailbox is named USBms_<Servername>, and is automatically created in the default directory container for Cisco Unity during installation.

Sending Networked System Broadcast Messages

To allow one or more Cisco Unity subscriber(s) to send networked broadcast messages, you first set up and offer the subscriber(s) access to the Cisco Unity Broadcast Message Administrator, and then create one or more public distribution list(s) that can be used to network system broadcast messages. For information on setting up the Cisco Unity Broadcast Message Administrator to address and send messages to the distribution list you create, see the "Sending System Broadcast Messages" section in the "Cisco Unity Conversation" chapter of the *System Administration Guide for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Note that any subscribers who will send networked system broadcast messages must be configured such that they are allowed to send broadcast messages to subscribers on multiple servers.

Setting up Public Distribution Lists for Addressing Networked System Broadcast Messages

To set up a public distribution list for use in sending system broadcast messages, do the following tasks.

1. Create one VPIM subscriber to represent each Cisco Unity Express server or each remote Cisco Unity domain. Depending on the type of the remote location, do one of the following:

- If Cisco Unity Express servers are to be included in the distribution list, find out the broadcast message VPIM ID of each Cisco Unity Express location. For each Cisco Unity Express broadcast mailbox, create a VPIM subscriber with a remote mailbox number that matches the broadcast message VPIM ID, and the subscriber location set to the delivery location configured for the Cisco Unity Express server.

- For remote Cisco Unity locations, create a VPIM subscriber by using any unused remote mailbox number from three to ten digits in length (any existing VPIM subscriber for the delivery location can be used in this case, but for ease of administration and to avoid the possibility of the subscriber being inadvertently deleted, we recommend that you configure a subscriber account specifically for this purpose).

You can create VPIM subscriber accounts by using the Cisco Unity Bulk Import wizard or the Cisco Unity Administrator. We recommend that you hide any VPIM subscribers that are created specifically for broadcast mailboxes from the Exchange address book, so that Outlook users do not send messages to them, and that you uncheck the List in Directory setting on the VPIM subscriber profiles so that subscribers do not inadvertently address messages to them. See the "Creating VPIM Subscribers" section on page 7-22.

2. Create a public distribution list and add VPIM subscribers for each remote Cisco Unity network or Cisco Unity Express broadcast mailbox that should be included in the broadcast. See the "Creating and Modifying Public Distribution Lists" section in the "Managing Distribution Lists" chapter of the *System Administration Guide for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

3. Optionally, add the USbms mailbox for any digitally networked Cisco Unity servers that you wish to include in the system broadcast message distribution (you must use Exchange tools to add the mailbox to the distribution list).

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:

- 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 9-3—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. No matter which networking option you use, the profile settings for the primary location need to be customized.

For additional information about primary location profile settings, see the "Primary Locations Profile Page" section in the "Network Settings" chapter of the *Interface Reference Guide for the Cisco Unity Administrator*, available at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

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. We recommend the following guidelines:

- 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 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**.

For additional information about primary location settings, see the "Primary Locations Profile Page" section in the "Network Settings" chapter of the *Interface Reference Guide for the Cisco Unity Administrator*, available at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

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 public or 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.

For additional information about primary location addressing option settings, see the "Location Addressing Options Page" section in the "Network Settings" chapter of the *Interface Reference Guide for the Cisco Unity Administrator*, available at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

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 could be:

- A private distribution list ID.
- A Cisco Unity subscriber, an Internet subscriber, or an external subscriber extension. (The external subscriber could be either an AMIS, Bridge, or VPIM subscriber.)
- A Cisco Unity subscriber, an Internet subscriber, or an external subscriber alternate extension.
- A public distribution list extension.
- A primary location dial ID from a networked Cisco Unity server or a delivery 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.

Additionally, when Bridge delivery locations are defined, Cisco Unity searches for a matching Bridge delivery location prefix and the remote mailbox number of the recipient. For more information, see the "How Cisco Unity Searches for a Matching Number" section of the "Primary Location Settings" chapter

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

For example, a subscriber presses 3335678 on the phone to address a message. Table 9-1 shows some of the possible matches:

Table 9-1   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

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 9-5

2. Search for a Subscriber Extension in the Dialing Domain and Then the Global Directory, page 9-5

3. Search for a Location Dial ID and Subscriber Extension at the Matching Location, page 9-6

4. Blind Addressing Search for a Delivery Location Dial ID, page 9-7

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 the dialing domain, and finally the global directory. The scope of the search is dictated by the Subscriber Searches: Limit Searches To setting. If a match is found at any scope level, the search stops and does not continue to the next scope level.

If the subscriber entered a one- or two-digit number, the search begins with Cisco Unity 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 on a subscriber extension, whether or not the conversation plays the recorded voice name and extension of the matched subscriber for confirmation depends on if the conversation is configured to do so, and if the recorded voice name exists. You can customize how the conversation confirms subscriber message addressing matches by using the Advanced Settings tool, available 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, 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.

If the Include Locations in Searches setting is enabled, primary locations from networked Cisco Unity servers and delivery locations created on other Cisco Unity servers are included in the search at each scope level. If the entered number matches a location dial ID, after the subscriber confirms the matched location, the conversation prompts the subscriber to enter the extension of the recipient at that location.

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 Subscriber Searches: Limit Searches To setting. 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. For example, the conversation could play: "For Kelly Bader at extension 3037 at Chicago press pound."

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 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 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 Blind Addressing: Allowed Locations setting. 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 an AMIS or VPIM delivery location, the matched location is returned for confirmation.

Figure 9-1 illustrates the search that Cisco Unity performs when the subscriber search and blind addressing search (if enabled) are set to the global directory, and the Include Locations in Searches setting is disabled.

Figure 9-1   *Subscriber Addressing Search for a Matching Number*

Search for a matching extension:

On the local Cisco Unity server. → Match found? → Yes / No

Within the dialing domain. → Match found? → Yes → Match(es) returned. / No

Globally, through the entire directory. → Match found? → Yes / No

Search for a matching location dial ID and extension:

On the local Cisco Unity server. → Match found? → Yes / No

Within the dialing domain. → Match found? → Yes → Match(es) returned. / No

Globally, through the entire directory. → Match found? → Yes / No

Blind addressing enabled? → No → No matches found. / Yes

Search for a matching delivery location dial ID:

On the local Cisco Unity server. → Match found? → Yes / No

Within the dialing domain. → Match found? → Yes → Match(es) returned. / No

Globally, through the entire directory. → Match found? → Yes / No

No matches found.

69883

Location Addressing Options

For information about Location Addressing option settings, see the "Location Addressing Options Page" section of the "Network Settings" chapter of the *Interface Reference Guide for the Cisco Unity Administrator*, available at
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Upgrading and Uninstalling Networking Options

Overview

This chapter provides information on upgrading and uninstalling Cisco Unity networking options.

See the following sections:

- Upgrading with Digital Networking, page 10-1
- Upgrading with AMIS Networking, page 10-1
- Upgrading with VPIM Networking, page 10-2
- Removing AMIS Networking, page 10-2
- Removing VPIM Networking, page 10-3
- Uninstalling the Cisco Unity Voice Connector, page 10-4
- Determining the Voice Connector Version, page 10-6

Upgrading with Digital Networking

Upgrading Digital Networking does not require anything other than upgrading the Cisco Unity servers according to the instructions in the applicable *Reconfiguration and Upgrade Guide for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Upgrading with AMIS Networking

After upgrading the Cisco Unity servers, AMIS Networking should continue to work. However, we recommend that you uninstall the previous version of the Voice Connector and install the new version. Other than upgrading the Voice Connector, there are no additional upgrade steps required.

See the following sections for information on uninstalling the Voice Connector and reinstalling it:

- Uninstalling the Cisco Unity Voice Connector, page 10-4
- Setting Up the Voice Connector for AMIS Networking, page 5-4

Upgrading with VPIM Networking

The Active Directory schema must be extended for VPIM Networking. The schema should have been extended as part of upgrading Cisco Unity. After upgrading the Cisco Unity servers on which the VPIM Networking option has been previously installed, VPIM Networking should continue to work. However, we recommend that you uninstall the previous version of the Voice Connector and install the new version. Other than upgrading the Voice Connector, there are no additional upgrade steps required.

See the following sections for information on uninstalling the Voice Connector and reinstalling it:

- Uninstalling the Cisco Unity Voice Connector, page 10-4
- Setting Up the Voice Connector for VPIM Networking, page 7-10

You can configure VPIM delivery locations to allow Cisco Unity to automatically create, modify, and delete VPIM subscribers based on the information that is received in incoming VPIM messages. In order to use this feature, you must upgrade the Voice Connector, and you must run ConfigMgr.exe on the VPIM bridgehead server to create the UVPIM directory account. See the "Creating the UVPIM Account by Using ConfigMgr.exe (Optional)" section on page 7-16 for details. By default, all types of automatic directory update are disabled for each delivery location. When you have upgraded the Voice Connector and have created the VPIM directory account, you must configure the subscriber creation settings for each delivery location, either individually or in bulk, in order to enable automatic updates. For additional information on customizing the settings for automatic directory updates, see the "Customizing VPIM Subscriber Directory Update Settings" section on page 7-28.

Removing AMIS Networking

Do the following tasks to remove the AMIS Networking option from Cisco Unity:

1. Uninstall all instances of the Voice Connector. See the applicable procedures in the "Uninstalling the Cisco Unity Voice Connector" section on page 10-4.

2. Optionally, make note of the Names, Dial IDs, Node IDs, and Delivery Phone Numbers of all AMIS locations. (You may want this information if you plan to set up AMIS Networking on another Cisco Unity server.)

3. Optionally, run Subscriber Information Dump to save AMIS subscriber information to an output file. (You may want this information if you plan to set up the networking option on another Cisco Unity server.) See the "To Output Information About AMIS Subscribers" procedure on page 10-2.

4. Use Global Subscriber Manager to delete all AMIS delivery locations and associated AMIS subscribers. See the "To Delete AMIS Delivery Locations and AMIS Subscribers" procedure on page 10-3.

5. Delete the UAmis mailbox. See the "To Delete the UAmis Mailbox" procedure on page 10-3.

Procedures for Removing AMIS Networking

To Output Information About AMIS Subscribers

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

Step 2   In the left pane, double-click **Subscriber Information Dump**.

Step 3   Select **AMIS Subscribers Only** from the Subscribers to Dump list.

Step 4   Indicate the output file name and location, and how the data should be formatted.

Step 5   Select the data to include in the output file.

Step 6   Click **Start**. When the output is complete, Subscriber Information Dump displays a message box with the number of errors encountered in the process. Click **OK** to view the error log, or **Cancel** if no errors were encountered.

Step 7   Exit Subscriber Information Dump and Tools Depot.

To Delete AMIS Delivery Locations and AMIS Subscribers

Step 1   On the Cisco Unity server desktop, 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**. In the warning dialog box, click **Yes**.

All of the AMIS subscribers who are associated with the delivery location are deleted automatically when the location is deleted, as are the underlying contacts.

Step 5   Repeat Step 4 as needed to delete all of the AMIS locations.

Step 6   Close Global Subscriber Manager and Tools Depot.

To Delete the UAmis Mailbox

Step 1   On the Exchange server that Cisco Unity is connected to, or on another applicable server in the network, on the Windows Start menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.

Step 2   Expand the tree in the left pane so that the UAmis_<Server name> user is visible in the right pane.

Step 3   Right-click the UAmis_<Server name> user, and select **Delete**.

Removing VPIM Networking

Do the following tasks to remove the VPIM Networking option from Cisco Unity:

1. Uninstall all instances of the Voice Connector. See the applicable procedures in the "Uninstalling the Cisco Unity Voice Connector" section on page 10-4.

2. Optionally, make note of the names, dial IDs, and other data of all VPIM locations. (You may want this information if you plan to set up the networking option on another Cisco Unity server.)

3. Optionally, run Subscriber Information Dump to save VPIM subscriber information to an output file. (You may want this information if you plan to set up the networking option on another Cisco Unity server.) See the "To Output Information About VPIM Subscribers" procedure on page 10-4.

4. Use Global Subscriber Manager to delete all VPIM delivery locations and associated VPIM subscribers. See the "To Delete VPIM Delivery Locations and VPIM Subscribers" procedure on page 10-4.

Note   If you previously ran ConfigMgr.exe on one or more Cisco Unity server(s) to create the VPIM directory account in order to enable automatic VPIM subscriber directory updates, the CsVPIMConnector service may still be running on the server(s), and the UVPIM_<Server Name> mailbox will still exist. The service and mailbox can be safely left as is after all VPIM data has been removed; we do not recommend that you disable the service or remove the mailbox.

Procedures for Removing VPIM Networking

To Output Information About VPIM Subscribers

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

Step 2   In the left pane, double-click **Subscriber Information Dump**.

Step 3   Select **VPIM Subscribers Only** from the Subscribers to Dump list.

Step 4   Indicate the output file name and location, and how the data should be formatted.

Step 5   Select the data to include in the output file.

Step 6   Click **Start**. When the output is complete, Subscriber Information Dump displays a message box with the number of errors encountered in the process. Click **OK** to view the error log, or **Cancel** if no errors were encountered.

Step 7   Exit Subscriber Information Dump and Tools Depot.

To Delete VPIM Delivery Locations and VPIM Subscribers

Step 1   On the Cisco Unity server desktop, 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**. In the warning dialog box, click **Yes**.

All of the VPIM subscribers associated with the delivery location are deleted automatically when the location is deleted, as are the underlying contacts.

Step 5   Repeat Step 4 as needed to delete all of the VPIM locations.

Step 6   Close Global Subscriber Manager and Tools Depot.

Uninstalling the Cisco Unity Voice Connector

The uninstall procedure that you use depends on the Cisco Unity Voice Connector version in use. To determine the version of an installed Voice Connector, see the "Determining the Voice Connector Version" section on page 10-6.

Do the procedure that applies to your installation:

To Uninstall the Voice Connector for Exchange 2000: Cisco Unity 5.0 and Later, Voice Connector 12.0 and Later

Step 1   Log on to the Exchange server on which the Voice Connector is installed.

Step 2   On the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.

Step 3   Click the Voice Connector component to uninstall:

- Exchange 2000 Voice Connector
- Cisco Unity Transport Event Sink
- Cisco Unity Secure Messaging Service

Step 4   Follow the on-screen prompts to uninstall the component.

Step 5   Repeat Step 3 and Step 4 for each additional component to uninstall.

Step 6   If you did not uninstall the Exchange 2000 Voice Connector, skip to Step 12.

Step 7   On the Windows Start menu, click **Programs > Microsoft Exchange > System Manager**.

Step 8   Expand **Servers\<Server name>\<Storage group>\Mailbox Store\Mailboxes** for the server on which the Voice Connector was installed.

The mailbox for the Voice Connector is named "AvExchangeIVC_<Servername>" or "Exchange 2000 Voice Connector (<Servername>)."

Step 9   Right-click **Mailboxes** in the left pane, and click **Run Cleanup Agent**.

Step 10   After the Cleanup Agent has run, right-click each Voice Connector mailbox marked with the red X icon and click **Purge**. Click **Yes** in the warning dialog box.

Step 11   Close the Exchange System Manager.

Step 12   Close Add/Remove Programs.

To Uninstall the Voice Connector for Exchange 2000: Cisco Unity 4.x, Voice Connector 10.0 Through 11.0(3)

Step 1   Log on to the Exchange server on which the Voice Connector is installed.

Step 2   On the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.

Step 3   Click **Exchange 2000 Voice Connector**.

Step 4   Follow the on-screen prompts to uninstall the Voice Connector.

Step 5   On the Windows Start menu, click **Programs > Microsoft Exchange > System Manager**.

Step 6   Expand **Servers\<Server name>\<Storage group>\Mailbox Store\Mailboxes** for the server on which the Voice Connector was installed.

The mailbox for the Voice Connector is named "AvExchangeIVC_<Servername>" or "Exchange 2000 Voice Connector (<Servername>)."

Step 7 Right-click **Mailboxes** in the left pane, and select **Run Cleanup Agent**.

Step 8 After the Cleanup Agent has run, right-click each Voice Connector mailbox marked with the red X icon and select **Purge**. Click **Yes** in the warning dialog box.

Step 9 Close the Exchange System Manager.

To Uninstall the Voice Connector for Exchange 5.5: Cisco Unity 4.x, Voice Connector 10.0 Through 11.0(3)

Step 1 Log on to the Exchange server on which the Voice Connector is installed.

Step 2 On the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.

Step 3 Select the Voice Connector.

Step 4 Follow the on-screen prompts to uninstall the Voice Connector.

Determining the Voice Connector Version

This section contains two procedures. Do the procedure for your version of Cisco Unity.

To Determine the Voice Connector Version in Use: Cisco Unity 5.0(1) and Later, Voice Connector 12.0(1) and Later

---

Step 1 Log on to the Exchange server on which the Voice Connector is installed.

Step 2 In Windows Explorer or My Computer, browse to the **<ExchangeServerPath>\VoiceGateway\Bin** directory.

Step 3 Right-click **GwIvc.exe**, and click **Properties**.

Step 4 Click the **Version** tab in the Properties window.

Step 5 In the Item Name box, click **Product Version** to view the product version in the Value box.

To Determine the Voice Connector Version in Use: Cisco Unity 4.x, Voice Connector 10.0 Through 11.0(3)

Step 1 Log on to the Exchange server on which the Voice Connector is installed.

Step 2 In Windows Explorer or My Computer, browse to the applicable directory:

Exchange 2000 or Exchange 2003	<ExchangeServerPath>\VoiceGateway\Bin
Exchange 5.5	<ExchangeServerPath>\Connect\Voice\Bin

Step 3 Right-click **GwIvc.exe**, and click **Properties**.

Step 4 Click the **Version** tab in the Properties window.

Step 5   In the Item Name box, click **Product Version** to view the product version in the Value box.

Migrating from SMTP Networking to VPIM Networking

Overview

This chapter provides information on migrating from SMTP Networking to VPIM Networking for messaging between Cisco Unity servers that access different directories. Because Cisco Unity 4.x was the last train that supported the SMTP Networking option, customers who need to network Cisco Unity servers that access separate directories must migrate to VPIM Networking instead of using SMTP Networking after upgrading to Cisco Unity 5.0 or later.

Both SMTP Networking and VPIM Networking use SMTP as the mechanism for exchanging messages, but the message format differs. SMTP Networking uses a proprietary message format, while the message format in VPIM Networking adheres to the VPIM industry standard. In addition, VPIM Networking provides functionality that is not available in SMTP Networking. See the "VPIM Networking" chapter for more information.

Prerequisites

Before starting the migration, verify that the following prerequisites have been met:

- The servers have already been upgraded to Cisco Unity 5.x as described in the *Reconfiguration and Upgrade Guide for Cisco Unity Release 5.x (With Microsoft Exchange)*, which is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

- A license file with a VPIM license has been obtained and installed on the Cisco Unity Bridgehead server.

- Cisco Unity and Exchange meet the requirements as described in the "VPIM Networking Requirements" section in *Networking Options Requirements for Cisco Unity*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Task List for Migrating from SMTP Networking to VPIM Networking

Use the task list that follows to migrate from SMTP Networking to VPIM Networking for messaging between Cisco Unity servers that access different directories. The cross-references take you to detailed procedures, most of which are in other chapters of the Networking Guide. After finishing a procedure, return to this task list and continue with the next item. Do these tasks in both Cisco Unity locations.

1. Uninstall the older version of the Voice Connector that was used for SMTP Networking. See the "Uninstalling the Cisco Unity Voice Connector" section on page 10-4.

2. Make decisions about your numbering plan and gather information needed to configure VPIM Networking. See the "Making Design Decisions and Gathering Needed Information" section on page 7-4.

3. Determine the domain name that will be used for messaging between the remote voice messaging system and Cisco Unity. See the "Determining the Domain Name" section on page 7-5.

4. As applicable, configure DNS or HOSTS files. See the "Resolving Names with IP Addresses" section on page 7-5.

5. Verify network and SMTP connectivity with the remote voice messaging system. See the "Verifying Connectivity with the Remote Voice Messaging System" section on page 7-6.

6. If you have not already done so, extend the Active Directory schema to enable VPIM Networking. See the "Extending the Active Directory Schema" section on page 7-8.

7. Determine whether the default recipient policy can be used for the Voice Connector Exchange mailbox, or create a new recipient policy. See the "Verifying the Recipient Policies or Creating a New One" section on page 7-9.

8. Install the Cisco Unity Voice Connector on an Exchange 2000 or Exchange 2003 server. See the "Setting Up the Voice Connector for VPIM Networking" section on page 7-10.

⚠

Caution   Installing the Voice Connector on an Exchange 2007 server is not supported.

9. During the Cisco Unity 5.x upgrade, when you ran the Cisco Unity Permissions wizard to grant the necessary permissions to the installation and service accounts, if you did not check the Set Permissions Required by AMIS, Cisco Unity Bridge, and VPIM check box on the Choose Whether to Enable Voice Messaging Interoperability page, do the following steps:

   a. Log on to the bridgehead server by using an account that:

   – Is a member of the Domain Admins group in the domain that the Cisco Unity server belongs to, or that has permissions equivalent to the default permissions for the Domain Admins group.

   – Is either an Exchange Full Administrator or a member of the Domain Admins group in the domain that contains all of the domains from which you want to import Cisco Unity subscribers.

   b. Re-run the Permissions wizard, and follow the on-screen prompts until the Choose Whether to Enable Voice Messaging Interoperability page appears.

   c. Check the Set Permissions Required by AMIS, Cisco Unity Bridge, and VPIM check box.

   d. Follow the on-screen prompts to complete the Permissions wizard.

   For more information on running the Permissions wizard, see the Permissions wizard Help file, PWHelp_<language>.htm, in the directory where the Permissions wizard is installed.

If you do not know whether you checked the check box, run the Permissions wizard in report mode. For more information, see the Report Mode Help file, PWReportHelp_<language>.htm, in the directory where the Permissions wizard is installed.

10. If you plan to configure Cisco Unity to automatically update the VPIM subscriber directory, run ConfigMgr.exe in order to create the UVPIM account. See the "Creating the UVPIM Account by Using ConfigMgr.exe (Optional)" section on page 7-16.

11. Customize the primary location profile settings. See the "Customizing the Primary Location" section on page 7-18.

12. Convert SMTP delivery locations to VPIM delivery locations, and Internet subscribers to VPIM subscribers, either by running the stored procedure, or by doing the conversion manually:

   – To run the stored procedure, see the "Running the Stored Procedure to Convert VPIM Delivery Locations and Subscribers" section on page 11-3.

   – To convert the VPIM delivery locations and subscribers manually, see the "Manually Converting VPIM Delivery Locations and Subscribers" section on page 11-4.

13. Optionally, customize the delivery location settings that control automatic VPIM directory updates. See the "Customizing VPIM Subscriber Directory Update Settings" section on page 7-28.

14. Optionally, extend identified subscriber messaging to include VPIM subscribers. See the "Extending Identified Subscriber Messaging to Include VPIM Subscribers" section on page 7-34.

Running the Stored Procedure to Convert VPIM Delivery Locations and Subscribers

If there are a large number of Internet subscribers to be converted to VPIM subscribers, we recommend that you run the stored procedure during off hours when the Cisco Unity server is not processing very many calls or messages.

To Run the VpimMigrateSMTP Stored Procedure

As a best practice, you should back up the Cisco Unity server before running the stored procedure.

Step 1   Log on to the Cisco Unity Bridgehead server by using the administration account that was selected when Cisco Unity was installed.

Step 2   Open a command prompt window.

Step 3   At the command prompt, enter the following:

osql /d UnityDB /E /Q csp_VpimMigrateSMTP

Note   For more information about any of the osql options, enter **osql /?**

Step 4   After the stored procedure has finished running, close the command prompt window.

Note that the stored procedure adds the VPIM subscribers to the SQL Server database on the Cisco Unity server and then finishes running. However, Cisco Unity still must synchronize the subscriber data with Active Directory. If there are a large number of VPIM subscribers, this synchronization could take up to several hours.

Step 5 Finish the migration by continuing with the procedures in the "Setting Up the Voice Connector for VPIM Networking" section on page 7-10.

Manually Converting VPIM Delivery Locations and Subscribers

If you prefer not to use the VpimMigrateSMTP stored procedure to convert SMTP delivery locations to VPIM delivery locations and Internet subscribers to VPIM subscribers, use the following task list and procedures to do the conversion manually. You do these tasks on the Cisco Unity Bridgehead server.

1. Write down the data on each SMTP delivery location, and then delete the delivery location. See the "To Record SMTP Delivery Location Data and Then Delete the Delivery Location" procedure on page 11-4.

2. Create VPIM delivery locations by using the SMTP delivery location data. See the "To Create VPIM Delivery Locations" procedure on page 11-4.

3. Export Internet subscriber data to a CSV file by using the Subscriber Information Dump tool, available in Tools Depot. See the "To Export Internet Subscriber Data to a CSV File" procedure on page 11-5.

4. Modify the CSV file so that it can be used as the input CSV file for the Cisco Unity Bulk Import wizard. See the "To Modify the CSV File for Use with the Cisco Unity Bulk Import Wizard" procedure on page 11-6.

5. Delete the Internet subscribers and the associated contacts. See the "To Delete the Internet Subscribers and Associated Contacts" procedure on page 11-6.

6. Create VPIM subscribers by using the Cisco Unity Bulk Import wizard with the modified CSV file. See the "To Create VPIM Subscriber Accounts by Using the Cisco Unity Bulk Import Wizard" procedure on page 11-7.

To Record SMTP Delivery Location Data and Then Delete the Delivery Location

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

Step 2 Click the **Find** icon to search for and display an SMTP delivery location.

Step 3 Make note of the Display Name, Dial ID, and Domain Name on the Delivery Location Profile page.

Step 4 Click the **Delete** icon to delete the SMTP delivery location.

Step 5 Repeat Step 2 through Step 4 for each SMTP delivery location.

To Create VPIM Delivery Locations

Add the VPIM delivery locations by using the Display Names, Dial IDs, and Domain Names that you had made note of in Step 3 of the previous "To Record SMTP Delivery Location Data and Then Delete the Delivery Location" procedure.

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

Step 2 Click the **Add** icon.

Step 3 Enter the Display Name and Dial ID for the location.

Step 4 Select **VPIM** as the Destination Type for the location.

Step 5   Click **Add**.

Step 6   Record a voice name for the location.

Step 7   Enter the SMTP domain name of the remote Cisco Unity server.

Step 8   If needed to accommodate your numbering plan, or if there is more than one VPIM delivery location with the same domain name, enter a number in the Remote Phone Prefix field.

Subscribers do not enter this prefix when addressing messages. However, on outgoing messages, the Voice Connector adds the prefix to the beginning of the recipient mailbox number to form the To address. On incoming messages, the Voice Connector expects this same prefix to be the leading digits of the From mailbox number and removes these digits before determining the sending mailbox number.

Step 9   If needed to accommodate your numbering plan, enter a number in the Cisco Unity Phone Prefix field.

On outgoing messages, the Voice Connector adds this prefix to the beginning of the sender mailbox number to form the From address. On incoming messages, the Voice Connector expects this same prefix to be the leading digits of the To mailbox number and removes these digits prior to determining the matching Cisco Unity recipient ID.

Step 10   Indicate whether incoming messages from this VPIM location should be converted to another audio format.

Step 11   Indicate whether outbound messages to this VPIM location should be converted to another audio format. Typically, you choose **Do Convert Outgoing Messages**.

Step 12   Optionally, check the **Sender's Recorded Name** and/or **Sender's vCard** check box(es). The data may be used for creating or updating directory entries, if the remote system is configured to allow automatic creation, modification, and deletion of VPIM subscribers for the delivery location corresponding to this system.

Step 13   Click the **Save** icon.

Step 14   Repeat Step 2 through Step 13 for each delivery location.

To Export Internet 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 **SMTP 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 **RemoteAddress** 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 VPIM subscribers will be associated with the same VPIM 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. See the Cisco Unity Bulk Import wizard Help for details.

Step 5   In the CSV file, do a search and replace to change **VOICE:** to **VPIM:** in each remote address.

Step 6   If the Dial IDs of the VPIM delivery locations are different from the Dial IDs that were in the SMTP delivery locations, change the Dial ID in each remote address. Remote addresses are in the format:

VPIM:<Dial ID>_<Remote Mailbox Number>

Step 7   Save and close the CSV file.

To Delete the Internet Subscribers and Associated Contacts

Step 1   Start Active Directory Users and Computers. (On the Windows Start menu, click **Programs > Administrative Tools > Active Directory Users and Computers**.)

Step 2   In the tree in the left pane, expand the container in which users are created.

Step 3   In the right pane, click the **Type** column header so that all of the contacts are listed together.

Step 4   Select the contacts that are associated with the Internet subscribers.

Step 5   Right-click the highlighted selection and click **Delete**.

The Cisco Unity directory monitor service will detect the change the next time it synchronizes with the directory, and the associated Internet subscribers will be deleted from Cisco Unity.

Step 6   Exit Active Directory Users and Computers.

Step 7   Verify that the Internet subscribers have been deleted from Cisco Unity by doing the following sub-steps:

a.   In the Cisco Unity Administrator, go to any page in the **Subscribers > Subscribers** section.

b.   Click the **Find** icon and search for an Internet subscriber whose associated contact was deleted in Active Directory Users and Computers. You may need to wait for the deletion of the contacts to be propagated to Cisco Unity.

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

Step 1   Prepare a subscriber template that will be used for creating the VPIM subscribers.

Step 2   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. See the Cisco Unity Bulk Import wizard Help for instructions.

Step 3   On the bridgehead Cisco Unity server, on the Windows Start menu, click **Programs > Cisco Unity > Cisco Unity Bulk Import**.

Step 4   Accept the default, **CSV File**, and click **Next**.

Step 5   Specify where the log files should be saved, and click **Next**.

Step 6   On the Choose Subscriber Type dialog box, click **VPIM**, and click **Next**.

Step 7   Click **Next**, and proceed through the wizard. When you get to the Select the CSV File dialog box, use the CSV file that you modified in the "To Modify the CSV File for Use with the Cisco Unity Bulk Import Wizard" procedure on page 11-6.

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 "To Correct Errors That Occurred When Importing Data from a CSV File" procedure on page 11-7.

Step 8   When the VPIM subscriber accounts are created, click **Finish**.

Step 9   If you had import errors, but in Step 7 you chose to correct them later, see the "To Correct Errors That Occurred When Importing Data from a CSV File" procedure on page 11-7.

If you had no import errors, or if all errors have now been corrected, finish the migration by going to the "Setting Up the Voice Connector for VPIM Networking" section on page 7-10.

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

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).

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.

GLOSSARY

A

Active Directory
The Microsoft Windows directory service that stores information about objects on the network. Active Directory consists of a forest, domains, organizational units, containers, and objects. Different classes of objects can be represented in Active Directory including users, contacts, groups, computers and printers. The Active Directory schema can be extended to add attributes to existing object classes and to create new object classes.

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 and are stored as contacts in Active Directory. Mailbox greetings and voice names can be individually recorded for each subscriber. Messages that are 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 and are stored as contacts in Active Directory. Mailbox greetings and voice names can be individually recorded for each Bridge subscriber. Messages that are 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.

C

contact   An Active Directory object that represents a subscriber who does not have an Active Directory logon account or an Exchange mailbox.

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 that are 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. The Exchange partner servers must be in the same Active Directory forest. Message routing is done by Exchange.

directory   The data store used by Cisco Unity, which contains information about subscribers, distribution lists, and locations. Cisco Unity stores data in Active Directory. During setup, you specify one Exchange server (the partner Exchange server) through which Cisco Unity communicates with other Exchange servers in the network. If the partner server is Exchange 2000 or Exchange 2003, Cisco Unity uses Active Directory.

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. In VPIM Networking, depending on the settings for each delivery location, the Voice Connector may generate directory messages based on incoming VPIM messages and non-delivery receipts (NDRs). The Voice Connector sends the directory messages to the Cisco Unity Bridgehead server, where the CsVPIMConnector service processes them and creates, modifies, or deletes VPIM subscribers and the associated Active Directory contacts.

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>]
where type can be AMIS, OMNI, VOICE, or VPIM. The Voice Connector 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 Exchange 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 Exchange 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 are stored as contacts in Active Directory. Mailbox greetings and voice names can be individually recorded for each Internet subscriber. Messages that are sent to an Internet subscriber are sent via SMTP over the Internet or any TCP/IP network.

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 who are associated with one Cisco Unity server can use the phone to send voice messages to subscribers who are associated with another Cisco Unity server; to individuals with access to a computer connected to the Internet; and to 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 that is 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) that are 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

schema   Defines the structure of a database, including classes of data objects and the type of information that each data object can contain. When setting up Cisco Unity for use with Exchange 2000 or Exchange 2003, the Active Directory schema must be extended.

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.

transport event sink	A transport event sink is code that is activated through a defined trigger, such as the receipt of a new message. When the Voice Connector is installed, it registers a transport event sink with the Windows SMTP server. Transport events occur when messages flow through the SMTP core transport system.
	The transport event sink is registered by the Voice Connector and monitors all incoming messages. Messages that have the content type Multipart/Voice-Message and that are addressed to the SMTP domain defined during the Voice Connector installation are readdressed to the Voice Connector by the transport event sink. The transport event sink ensures that incoming VPIM messages are routed to the Voice Connector for processing.
Trusted Internet subscriber	Trusted Internet subscribers are Internet subscribers that are trusted with decrypted secure messages. Trusted Internet subscribers must be associated with a Trusted Internet Location. Based on the security settings of the Trusted Internet location, secure messages to Trusted Internet subscribers are decrypted by the Cisco Unity Voice Connector for Microsoft Exchange before they are sent by the Exchange server. (Messages to regular Internet subscribers are sent directly by the Exchange server and cannot be decrypted and therefore cannot be played by the recipient.)
Trusted Internet location	A delivery location that is used to configure decryption options for secure messages that are sent to Trusted Internet subscribers.

U

UAmis account	Outgoing AMIS messages are placed in a special Exchange mailbox that has the display name 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 Exchange mailbox that has the display name UOmni_<Servername>. The Bridge Connector (a Cisco Unity component that runs as a Windows service called CsBridgeConnector) monitors the UOmni mailbox. 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.
UVPIM mailbox	Administrative messages from the Voice Connector to create, modify, or delete VPIM subscribers are placed in a special Exchange mailbox that has the display name UVPIM_<Servername>. The CsVPIMConnector service that runs on the Cisco Unity VPIM bridgehead server monitors the UVPIM mailbox. 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 VPIM 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. If a vCard is attached to an incoming message from a VPIM system, the recipient can look at the vCard data in Cisco Unity ViewMail for Microsoft Outlook. Cisco Unity can also be configured to update the directory with information from the header or vCard data from incoming VPIM messages.

Voice Connector   Formerly known as "Internet Voice Connector," "IVC," or "Voice Gateway." The Cisco Unity Voice Connector for Exchange is a Cisco Unity networking component that enables messaging between Cisco Unity servers that access separate directories, and between Cisco Unity servers and other voice messaging systems. The Voice Connector registers with Exchange to handle certain message address types (AMIS, OMNI, VOICE, and VPIM). The Voice Connector takes different actions depending on the address type. For example, with the VPIM address type, the Voice Connector encodes the message according to the VPIM specification and adjusts the "To" and "From" addresses. The Voice Connector for Exchange 2000 also works with Exchange 2003; there is not a separate Voice Connector for Exchange 2003.

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 and are stored as contacts in Active Directory. 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).

Networking Guide for Cisco Unity Release 5.x (With Microsoft Exchange)

Networking Guide for Cisco Unity Release 5.x (With Microsoft Exchange)

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com