CHAPTER 16

# Networking

See the following sections:

## Message Addressing

Message addressing involves the ability to select recipients when creating a new message.

Use the troubleshooting information in this section if users report that they are unable to address messages to recipients on another voice messaging system. See the following sections:

- Users Cannot Address Messages to Remote Cisco Unity Connection Users, Contacts, or Public Distribution Lists, page 16-1
- Users Cannot Address Messages to Recipients at a VPIM Location, page 16-2
- Users Cannot Blind Address Messages to a Mailbox at a VPIM Location, page 16-2

If a message is successfully created and sent to a remote recipient but is not received by the recipient, see the "Message Transport" section on page 16-3. For addressing issues involving only local recipients on the same Cisco Unity Connection server, see the "Searching and Addressing" chapter.

### Users Cannot Address Messages to Remote Cisco Unity Connection Users, Contacts, or Public Distribution Lists

If users are unable to address messages to remote objects on a Digital Network, do the following tasks in the order presented:

1. Check for the presence of the remote object in Cisco Unity Connection Administration on the location on which users are experiencing the problem. This indicates whether the remote object has been replicated. If the object is not found, see the "Directory Synchronization in a Digital Network" section on page 16-5 for further troubleshooting steps.
2. Check the partition and search space configuration. The remote object to which the message is being addressed must belong to a partition that is a member of the search space configured as the search scope for the user.

3. Turn on the CDE micro trace (level 12 CDL Access). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces" chapter.

## Users Cannot Address Messages to Recipients at a VPIM Location

Addressing to a particular recipient at a VPIM location can fail for one of the following reasons:

- Blind addressing is disabled for the VPIM location, and no VPIM contact exists for the recipient. If you are relying on automatic VPIM contact creation to populate VPIM contacts based on incoming messages, it is possible that contact creation is not set up properly for this location, or that no messages have been received from the remote user. Check the settings on the Contact Creation page for the VPIM location in Cisco Unity Connection Administration.
- A VPIM contact exists, but users are unable to locate it because the extension is incorrect or the contact name does not match user searches. Check the VPIM contact configuration in Connection Administration.
- Users are attempting to blind address to VPIM recipients, but the DTMF Access ID of the VPIM location is incorrect or does not match the pattern users are attempting to enter when addressing. Check the value of the DTMF Access ID setting on the Edit VPIM Location page in Connection Administration, and confirm that users are aware of the correct value.
- The user search scope does not include the partition of the VPIM contact or VPIM location. If the VPIM contact partition does not match the partition of the VPIM location to which the contact belongs, the search results depend on the method used to address the message as well as the partition and search space configuration. When users address messages to a VPIM mailbox by entering a VPIM location DTMF Access ID plus a remote user mailbox number, or when voice-recognition users say a name and location (for example, "John Smith in Seattle"), the action is allowed or denied based on the partition of the VPIM location. However, when users address to a VPIM contact by using spell-by-name or by entering the local extension of the contact, or when voice-recognition users say the name of a contact without the location (for example, "John Smith"), the action is allowed or denied based on the partition of the VPIM contact, regardless of whether the partition of the VPIM location is out of scope for the user. In Connection Administration, on the Edit User Basics page for the user, check which search space is configured as the search scope. Then check which partition is configured for the VPIM contact (on the Edit Contact Basics page) or for the VPIM location (on the Edit VPIM Location page), as applicable. Finally, check the Edit Search Space page for the user search space to determine whether the partition appears in the Assigned Partitions list.

## Users Cannot Blind Address Messages to a Mailbox at a VPIM Location

Blind addressing allows users to send messages to recipients at the VPIM location even if the recipients are not defined as contacts in the Cisco Unity Connection directory. If blind addressing is not working, confirm that you have enabled it for an individual VPIM location by checking the Allow Blind Addressing check box on the VPIM Location page in Cisco Unity Connection Administration. When this check box is checked for a location, users can address messages to recipients at this location by entering a number that is made up of the VPIM location DTMF Access ID and the mailbox number of the recipient, or by saying the digits of the mailbox number and the display name of the VPIM location (for example, "five five at Seattle office").

# Message Transport

Cisco Unity Connection uses SMTP to exchange voice messages with other systems. This includes VPIM messages, messages between users on digitally networked Connection servers, and messages sent to Connection by IMAP clients or forwarded by Connection to the relay address configured on the Message Actions page for a user.

In order for a Connection system to exchange SMTP messages with other voice messaging systems or Connection locations, the system must either be able to directly access TCP/IP port 25 on the remote system, or be configured to deliver messages to an SMTP smart host that can relay messages to the system. When both Digital Networking and VPIM Networking are in use, typically you create each VPIM location on only one Connection server in the Digital Network; the digitally networked locations then forward messages that are addressed to users at the VPIM location to the Connection server that homes the VPIM location for delivery. In this case, only this Connection server needs SMTP connectivity (either directly or through a smart host) with the remote messaging system.

When a message is recorded by a Connection user for delivery to a remote system, the message is first processed by the Message Transfer Agent (MTA). This service formats the message. For example, for a VPIM message, the MTA formats the To: and From: fields on the message, sets the content-type of the message to multipart/Voice-Message, and sets other header properties. It then places the message in a pickup folder on the Connection server. The SMTP service periodically checks the pickup folder for messages, removes a message from the folder, determines the destination server from the message header, establishes an SMTP connection to the correct server, and sends the message. The process is reversed when Connection receives an incoming message via SMTP—the message is first processed by the SMTP service, then the MTA service.

Use the troubleshooting information in this section if you are experiencing difficulties with message transport. See the following sections:

- Messages Sent from a VPIM Location Are Not Received by Cisco Unity Connection Users, page 16-3
- Messages Sent from Cisco Unity Connection Are Not Received by Users at a VPIM Location, page 16-4
- Messages Sent from Users on One Cisco Unity Connection Location Are Not Received by Users on Another Cisco Unity Connection Location, page 16-4

## Messages Sent from a VPIM Location Are Not Received by Cisco Unity Connection Users

In order for incoming VPIM messages to be received and processed correctly, the following are required:

- SMTP connectivity must be available between the originating voice messaging system and Cisco Unity Connection.
- If messages from the originating voice messaging server are routed through a smart host that is different from the one that is configured on the System Settings > SMTP Configuration > Smart Host page in Cisco Unity Connection Administration, the IP address of this smart host must be added to the IP Address Access List as an allowed connection. (On the System Settings > SMTP Configuration > Server page, click Edit > Search IP Address Access List to view or modify the access list.)
- The domain name in the incoming message “From” field must match the Remote VPIM Domain Name value that is defined for the VPIM location in Connection Administration.

- If a Remote Phone Prefix value is defined for the VPIM location, the mailbox number in the incoming message "From" field must begin with the prefix digits.
- If a Cisco Connection Phone Prefix is defined for the VPIM location, the mailbox number in the incoming message "To" field must begin with the prefix digits.
- The Connection users receiving the message must be in a partition that is a member of the search space that is defined as the search scope of the VPIM location on the receiving server.

You can verify SMTP connectivity and check the format of the "From" and "To" fields by turning on all levels of SMTP micro traces. ("MAIL FROM" and "RCPT TO" appear in the SMTP trace logs.) In addition, when you turn on all levels of MTA micro traces, the MTA log contains information about the processing of the message, including messages describing prefix processing errors. You can use the message ID listed at the end of the output file path name in the SMTP logs (for example, csUnitySmtp-30-1223425087697), to locate a message in the MTA log, or search by the recipient address (for example, 5551212@receiving-server-domain.com). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces" chapter.

## Messages Sent from Cisco Unity Connection Are Not Received by Users at a VPIM Location

In order for outgoing VPIM messages to be received and processed correctly, the following are required:

- SMTP connectivity must be available between Cisco Unity Connection and the receiving voice messaging system, either through direct TCP/IP connectivity to port 25, or through an SMTP smart host. (You can configure the SMTP smart host on the System Settings > SMTP Configuration > Smart Host page in Cisco Unity Connection Administration.)
- The audio attachment on the VPIM message must be in a format that is playable on the remote system. If the remote voice messaging system is not Connection or Cisco Unity, you may need to configure the Outbound Messages setting for the VPIM location in Cisco Unity Connection Administration to use the G.726 codec to transcode the audio format.

As with incoming VPIM messages, when troubleshooting outgoing messages, we recommend that you start by turning on all MTA and SMTP micro traces. When examining the logs for outgoing message issues, start with the MTA log first, then review the SMTP log. For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces" chapter.

## Messages Sent from Users on One Cisco Unity Connection Location Are Not Received by Users on Another Cisco Unity Connection Location

In general, messages that are successfully addressed to a remote user by using the phone interface should be delivered as long as SMTP connectivity is established between the Cisco Unity Connection locations. A notable exception occurs when a user replies to all recipients of a received message, and some of those recipients are not in the search scope of the replying user. In this case, the replying user receives a non-delivery receipt for any recipient who is not in the search scope.

Messages sent by using an IMAP client to a remote user can fail if the profile information for the remote user (specifically, the SMTP proxy address information of the remote user) has not fully replicated to the Connection location of the sending user. You can diagnose this condition by checking the unique sequence numbers for each location in Cisco Unity Connection Administration. For more information, see the "Unique Sequence Numbers (USNs) Are Mismatched Between Locations" section on page 16-5.

If the issue does not appear to be related to the partition and search space configuration or directory replication, you may be able to further diagnose the problem by turning on all levels of SMTP and MTA micro traces. For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces" chapter.

# Directory Synchronization in a Digital Network

Use the troubleshooting information in this section if you are experiencing difficulties with directory synchronization in a Digital Network. See the following sections:

- Unique Sequence Numbers (USNs) Are Mismatched Between Locations, page 16-5
- Automatic Directory Replication Is Stalled, page 16-5
- Manual Directory Replication Is Stalled, page 16-6
- Push and Pull Status Are Mismatched Between Locations, page 16-6

## Unique Sequence Numbers (USNs) Are Mismatched Between Locations

The Connection Locations pages in Cisco Unity Connection Administration provide information about the status of replication between locations. On the Edit Connection Location page for a remote location, the Last USN Sent, Last USN Received, and Last USN Acknowledged fields indicate the sequence numbers of replication messages sent to and from the remote location. When two locations are fully synchronized, the Last USN Sent and Last USN Acknowledged values on the location that is sending replication updates should equal the Last USN Received on the location that is receiving updates.

During replication, it is normal for the Last USN Acknowledged value to lag behind the Last USN Sent value.

During a push synchronization, the Last USN Sent may display a very large value while the Last USN Acknowledged shows a much smaller value. This is normal. Monitor the Last USN Acknowledged to make sure it continues increasing toward the Last USN Sent value. If it does not, see the "Manual Directory Replication Is Stalled" section on page 16-6.

## Automatic Directory Replication Is Stalled

Directory changes on one Cisco Unity Connection server are automatically propagated to other locations in the Digital Network. If either the Last USN Acknowledged value that is displayed on the sending location or the Last USN Received value that is displayed on the receiving location stops incrementing toward the Last USN Sent value that is displayed on the sending location, replication may be stalled. This can happen when a Connection location receives an update to an object that depends on another object about which it has not received information. For example, the addition of a member to a distribution list depends on the presence of a user record for the member being added. If the location has not received the information about the user record, it waits for a default of five minutes to see if the directory message containing the user record information arrives to satisfy the dependency.

In most cases, the problem should resolve itself after the five minute time-out, at which point the receiving Connection system requests that the record be re-sent. If the problem is not resolved, use the Real-Time Monitoring Tool (RTMT) or the command line interface (CLI) to check the Application System log to see if any errors have been reported by the CuReplicator application. For information on using RTMT to view system logs, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

You may also want to turn on Digital Networking macro traces to diagnose a replication issue. For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces" chapter.

## Manual Directory Replication Is Stalled

When an administrator initiates a manual push or pull of the directory between two Cisco Unity Connection locations, the Push Directory or Pull Directory status displayed on the Networking > Connection Locations page for the remote location in Cisco Unity Connection Administration may indicate that replication is in progress, but the Last USN Acknowledged or Last USN Received values on the Edit Connection Location page may not be changing. If this problem occurs, try stopping the push or pull operation by checking the check box next to the display name of the remote location on the Connection Locations page and clicking Stop Push (if the Push Directory status for that location indicates a push is in progress) or Stop Pull (if the Pull Directory status for that location indicates a pull is in progress). You can then restart the manual replication.

## Push and Pull Status Are Mismatched Between Locations

When an administrator initiates a manual push or pull of the directory between two Cisco Unity Connection locations, the Push Directory status displayed on the Networking > Connection Locations page in Cisco Unity Connection Administration on the sending location should match the Pull Directory status displayed in Connection Administration on the receiving location (for example, both should display In Progress during replication).

If the status does not match, wait at least five minutes. If it still does not match, you may be able to correct the mismatch by doing the following procedure.

### To Resynchronize Push and Pull Status Between Locations

**Step 1** In Cisco Unity Connection Administration on the location that displays Idle status for the push or pull, check the check box next to the display name of the mismatched location, and click **Push Directory To** or **Pull Directory From** to start the operation that should display In Progress.

For example, if location one shows a push is in progress and location two shows a pull is idle, on location two, check the check box next to the location one display name and click Pull Directory From.

**Step 2** When the operation status displays as In Progress, wait a minute, then recheck the check box for the remote location and stop the operation by clicking either **Stop Push** or **Stop Pull**, as applicable.

# Cross-Server Logon and Transfers in a Digital Network

When Cisco Unity Connection servers are digitally networked, cross-server features can be configured such that:

- Calls are transferred to users who are not associated with the local server, according to the call transfer and screening settings of the user who is receiving the transfer. (This includes calls that are transferred from the automated attendant or directory assistance, and live reply calls that are transferred when a user listens to a message and chooses to reply by calling the sender.) This functionality is referred to as a cross-server transfer.

- When calling from outside the organization to log on to Connection, users—no matter which is their home Connection server—can call the same number and are transferred to the applicable home Connection server to log on. This functionality is referred to as a cross-server logon.

Use the troubleshooting information in this section if you are experiencing difficulties with cross-server logon or transfers. See the following sections:

- Users Hear the Opening Greeting Instead of the Password Prompt When Attempting to Log On, page 16-7
- Users Hear a Prompt Indicating That Their Home Server Cannot Be Reached During Cross-Server Logon, page 16-7
- User ID and Password Are Not Accepted During Cross-Server Logon, page 16-8
- Callers Are Prompted to Leave a Message Rather Than Being Transferred to the Remote User, page 16-8
- Callers Are Transferred to the Wrong User at the Destination Location, page 16-9
- Callers Hear a Prompt Indicating That Their Call Cannot Be Completed When Attempting to Transfer to a Remote User, page 16-9

## Users Hear the Opening Greeting Instead of the Password Prompt When Attempting to Log On

If a user attempts a cross-server logon and hears the opening greeting, the problem may be caused by one of the following:

- The originating location is not configured for cross-server logon hand-offs to the destination location. In Cisco Unity Connection Administration on the originating location, confirm that the Allow Cross-Server Login to this Remote Location check box is checked on the Edit Connection Location page for the destination location.
- The user is not found in the search scope on the originating location. Connection uses the search scope of the call when it reaches the Attempt Sign-In conversation to identify which user is trying to log on. In Cisco Unity Connection Administration on the originating location, check the direct call routing rules to determine which search space is set by the rule that sends calls to the Attempt Sign-In conversation. If the partitions that contain remote users are not a part of this search space, cross-server logon does not work, even if it is enabled.

## Users Hear a Prompt Indicating That Their Home Server Cannot Be Reached During Cross-Server Logon

When a cross-server logon hand-off fails to complete successfully, users hear a prompt indicating that their home server cannot be reached at this time. This may happen for one of the following reasons:

- The destination location is not configured to accept cross-server hand-offs. In Cisco Unity Connection Administration on the destination location, confirm that the Respond to Cross-Server Handoff Requests check box is checked on the System Settings > Advanced > Conversations page.
- The Cross-Server Dial String that is defined for the destination location on the originating location is incorrect, or the originating location is unable to place a call to this string by using the phone system integration that is used to dial out. In Connection Administration on the originating location, check the Cross-Server Dial String value on the Edit Connection Location page.

- No ports are available to dial out on the originating location or to answer the call on the destination location. You can use the Connection Port Usage Analyzer to help determine if port usage is becoming a problem for cross-server transfers. You can download the tool and view the Port Usage Analyzer Help at http://www.ciscounitytools.com/App_CUC_PortUsageAnalyzerLL.htm.

## User ID and Password Are Not Accepted During Cross-Server Logon

If a user attempts a cross-server logon and the call appears to be handed off correctly to the destination location but the user cannot log on, the most likely cause is that the user is not found in the search scope on the destination location, or another user with an overlapping extension is found first in the search scope.

Cisco Unity Connection uses the search scope of the call when it reaches the Attempt Sign-In conversation to identify which user is trying to log on, both on the originating and destination locations. In general, we recommend that the same search scope be used by the routing rules that handle cross-server logon on both the originating and destination locations. If necessary, you can add a routing rule on the destination location that specifically handles cross-server calls (for example, based on the calling number matching the extension of a port at the originating location).

To determine which search space is in use as the search scope during the call, turn on the CDE micro trace (level 4 Search Space). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces" chapter.

For information on configuring call routing rules and managing partitions and search spaces, see the "Managing Call Routing Tables" and "Managing Partitions and Search Spaces" chapters of the *System Administration Guide for Cisco Unity Connection Release 7.x*.

## Callers Are Prompted to Leave a Message Rather Than Being Transferred to the Remote User

If callers are prompted to leave a message for a user at the destination location even though the active transfer rule for that user is configured to transfer calls to an extension, this is may be a sign that the cross-server transfer hand-off has failed. This can happen for one of the following reasons:

- The originating location is not configured to perform cross-server transfers to the destination location. In Cisco Unity Connection Administration on the originating location, confirm that the Allow Cross-Server Transfer to this Remote Location check box is checked on the Edit Connection Location page for the destination location.
- The destination location is not configured to accept cross-server hand-offs. In Connection Administration on the destination location, confirm that the Respond to Cross-Server Handoff Requests check box is checked on the System Settings > Advanced > Conversations page.
- The Cross-Server Dial String that is defined for the destination location on the originating location is incorrect, or the originating location is unable to place a call to this string by using the phone system integration that is used to dial out. In Connection Administration on the originating location, check the Cross-Server Dial String value on the Edit Connection Location page.
- No ports are available to dial out on the originating location or to answer the call on the destination location. You can use the Connection Port Usage Analyzer to help determine if port usage is becoming a problem for cross-server transfers. You can download the tool and view the Port Usage Analyzer Help at http://www.ciscounitytools.com/App_CUC_PortUsageAnalyzerLL.htm.

Note that if the currently active transfer extension for the user is configured to perform a supervised transfer to an extension that is busy, callers are transferred to voice mail to leave a message when the If Extension Is Busy field is configured to do so, even if the cross-server transfer was successful.

## Callers Are Transferred to the Wrong User at the Destination Location

If a caller attempts a cross-server transfer and the call appears to be handed off correctly to the destination location but the caller reaches the wrong user at the destination, the most likely cause is that another user with an overlapping extension is found first in the search scope when the call is passed to the destination.

To determine which search space is in use as the search scope during the call, turn on the CDE micro trace (level 4 Search Space). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces" chapter.

## Callers Hear a Prompt Indicating That Their Call Cannot Be Completed When Attempting to Transfer to a Remote User

If a caller attempts a cross-server transfer and the call appears to be handed off correctly to the destination location, but the caller hears a prompt indicating that the call cannot be completed and Cisco Unity Connection hangs up, the most likely cause is that the remote user is not found in the search scope when the call is passed to the destination.

To determine which search space is in use as the search scope during the call, turn on the CDE micro trace (level 4 Search Space). For detailed instructions on enabling the traces and viewing the trace logs, see the "Diagnostic Traces" chapter.