CHAPTER 33

Using Digital Networking

Each Cisco Unity Connection server (or cluster) has a maximum number of users that it can serve. When the messaging needs of your organization require more than one Connection system, the systems can be networked together such that they replicate directory information among all the systems on the Connection Digital Network.

Users can send, reply to, and forward messages or place calls to users on other Connection systems as though they share the same system, while at the same time, each Connection installation in the network continues to serve only those users that were created on the server or cluster.

Users use the same Connection tools for messaging with users on other networked Connection systems that they use for messaging with users on their home system. Because of directory replication, each Connection system has the information that it needs to address messages to users who are associated with the other Connection systems.

When Connection servers are digitally networked, cross-server features can also 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 receives 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.)
- When calling from outside the organization to log on to Connection, all users can call the same number regardless of which Connection server they are homed on, and they are transferred to the applicable home Connection server to log on.

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

Note The Cisco Unity Connection Digital Networking feature is not supported in Cisco Unified Communications Manager Business Edition (CMBE).

Setting Up Cisco Unity Connection to Use Digital Networking

This section describes the prerequisites for setting up Digital Networking, and provides a high-level task list of all of the tasks that you need to complete for the setup, and the order in which they should be completed. If you are unfamiliar with Digital Networking, you should first read the "Digital Networking Concepts and Definitions" section on page 33-19 and then review the task list and procedures before beginning the setup.

Prerequisites

Revised May 2009

Before starting the setup, verify that the following prerequisites have been met on each server that will join the Digital Network (for clusters, verify these prerequisites for the publisher server):

- The server meets the requirements listed in the "Requirements for Digital Networking" section of the *System Requirements for Cisco Unity Connection Release 7.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html .
- Cisco Unity Connection is already installed in a standalone configuration.
- The servers that will be networked together are directly accessible through TCP/IP port 25 (SMTP), or SMTP messages are routable through an SMTP smart host.
- For Connection clusters, you must have a smart host available to resolve the SMTP domain of the cluster to both the publisher and subscriber servers in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down.

In addition, before setting up Digital Networking, you should be familiar with the concepts in the "Managing Partitions and Search Spaces" chapter.

Task List

Revised May 2009

Use this task list to set up Digital Networking between Cisco Unity Connection systems. The cross-references take you to detailed procedures.

If you have a Connection cluster, do the tasks only on the publisher server.

1. Make decisions about your networking deployment approach and gather information needed to configure Digital Networking. See the "Making Deployment Decisions and Gathering Needed Information" section on page 33-4.
2. Check the display name of each server that you are joining to the network, and modify it if it is not unique, or if you want to choose a more descriptive name. Also check the SMTP domain of each server that you are joining to the network, and modify it if it is not unique. See the "Verifying That Each Cisco Unity Connection Server Has a Unique Display Name and SMTP Domain" section on page 33-5.

Caution If the display name of a server matches the display name of another server on the Digital Network, the server will not be able to join the Digital Network. Likewise, if the SMTP domain matches the SMTP domain of another server on the network, the server will not be able to join the Digital Network.

3. If you are setting up Digital Networking for the first time, start by networking two Connection systems together. See the "Joining Two Cisco Unity Connection Servers to Create a Digital Network" section on page 33-6.
4. To add additional Connection servers to the network, see the "Adding a Cisco Unity Connection Server to an Existing Network" section on page 33-8.
5. Verify that replication is complete among locations. See the "Checking Replication Status" section on page 33-9.
6. If any servers on the network require a smart host to transmit and receive SMTP messages from other servers (for example, because a firewall separates the servers, or because the servers are part of a Connection cluster), configure the smart host, and configure the applicable locations to route through the host. See the "Configuring a Smart Host" section on page 33-10.

Note For each Connection cluster that you have added to the network, you must configure all other locations to route to the cluster through a smart host in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down. (You also configure the smart host to resolve the SMTP domain of the cluster to both the publisher and subscriber servers.)

7. For each cluster that you have added to the network, add the IP address of the subscriber server to the SMTP IP access list on every other location on the network; this ensures that other locations can receive message traffic from the subscriber server if the publisher server is down. See the "Configuring SMTP Access for Cluster Subscriber Servers" section on page 33-11.
8. Configure search spaces at each location to allow users who are homed at the location to reach users at other locations. See the "Configuring Search Spaces for Digital Networking" section on page 33-12.
9. Secure the Digital Networking setup. See the "Securing the Digital Networking Setup" section on page 33-13.
10. Optionally, set up cross-server logon and cross-server transfers. See the "Configuring Cross-Server Logon and Transfers" section on page 33-13.
11. Test the Digital Networking setup. See the "Testing the Digital Networking Setup" section on page 33-14.
12. Optionally, set up a network-wide All Users distribution list. See the "Creating a Network-Wide All Voice Mail Users Distribution List" section on page 33-16
13. If any servers on the Digital Network were previously configured as VPIM locations on other servers in the network, clean up the unused VPIM locations. See the "Cleaning Up Unused Cisco Unity Connection VPIM Locations and Contacts" section on page 33-17.
14. If you have not already done so, set up VPIM Networking to connect the Connection locations to any other VPIM-compatible voice messaging systems. See the "Setting Up Cisco Unity Connection to Use VPIM Networking" section on page 34-1.

Procedures for Setting Up Cisco Unity Connection to Use Digital Networking

See the following sections:

Making Deployment Decisions and Gathering Needed Information

Revised May 2009

Before you begin setting up Digital Networking, be sure to plan for the following, and gather the applicable information:

- If your network includes voice messaging servers that do not meet the prerequisites for Digital Networking but support the Voice Profile for Internet Mail (VPIM) protocol (for example, Cisco Unified Communications Manager Business Edition, Cisco Unity Connection 2.x servers, Cisco Unity 4.0 and later, or other VPIM-compatible systems), use VPIM Networking to connect them.

  We recommend the following approaches:

  - Unless your servers are already configured for VPIM, set up Digital Networking first, then set up VPIM Networking.
  - Choose a single Connection location on the Digital Network to handle the configuration of VPIM locations and contacts. This location is referred to as the “bridgehead.” The VPIM location and contact objects are replicated from the bridgehead to all digitally networked Connection locations so that those locations can address VPIM messages; the networked locations then forward the messages to the bridgehead for delivery to the remote voice messaging server. Managing these objects from a single location simplifies maintenance tasks and avoids potential overlaps in contact information that could cause confusion to users when they attempt to address messages.
  - If you have already configured VPIM locations on multiple systems that are joining a Digital Network, delete duplicate VPIM locations from all but one server before setting up Digital Networking. For instructions, see the “Removing a VPIM Location” section on page 34-15.
  - If you are migrating a VPIM location to Digital Networking (for example, because you used VPIM Networking to connect two or more Cisco Unity Connection 2.x servers and have upgraded the servers to Connection 7.x and Digital Networking) set up Digital Networking first. After the directory is fully replicated and you have tested message exchange between the Connection locations, remove the VPIM locations and VPIM contacts that represent the migrated servers and their users. The task list reminds you when to do this task.

- By default, every Connection server includes several predefined system distribution lists, which you can modify but not delete. If you have not renamed these lists so that the list names are unique on each server, or if you have added additional lists whose names are identical across servers, during initial replication each server automatically adds the remote server name to the display name of any remote lists whose names overlap with local list names. (The default lists are All Voice Mail Users, Undeliverable Messages, and All Voicemail-Enabled Contacts.) This can cause confusion when local users try to address to those remote lists.

  To solve this problem, you can use one of the following approaches:

  - If you want to maintain separate lists on each server, you can modify the name of each list on its home server so that it is unique (for example All Voice Mail Users on <Server Name>) and notify your users of the new list names for each server. If you choose this approach, you should also modify the recorded name of each list to indicate its source.
  - Alternatively, after setting up Digital Networking, you can create a master list that includes all users on all networked locations. The task list includes instructions on when and how to do this task.
- If you want to synchronize Connection user data with user data in an LDAP directory, we recommend that you configure Connection for integration with the LDAP directory prior to setting up Digital Networking, to simplify testing and troubleshooting.
- Make note of the following information about each server that is joining the network:
  - The IP address or fully qualified domain name (FQDN) of the server.
  - The user name and password of a user account that is assigned to the System Administrator role.
  - The dial strings that other servers will use to call this server, if cross-server logon or transfer will be configured on other servers to hand off calls to this server.

Verifying That Each Cisco Unity Connection Server Has a Unique Display Name and SMTP Domain

Revised May 2009

Each Cisco Unity Connection server that you join to a Digital Network must have a unique display name. If the display name is not unique, the server will not be able to join the Digital Network. For new Connection installations, the display name is typically the same as the host name of the server; however, if you changed the display name or upgraded the server from Connection 2.x (which uses “Local VMS” as the default display name), you may need to change the display name so that it does not overlap with other servers on the network.

Tip Choose a display name for each server that is descriptive and that will help you identify the location when it is listed among all locations in the Digital Network in Cisco Unity Connection Administration.

Each Connection server that you join to the Digital Network must also have a unique SMTP domain. By default, the SMTP domain is configured during installation to include the hostname of the server, in order to insure that it is unique. However, if the SMTP domains of multiple servers have been modified to the same value, you must change the domains to unique values before joining the servers in a Digital Network.

To Verify That Each Cisco Unity Connection Server Has a Unique Display Name and SMTP Domain

Step 1 To check the display name, in Cisco Unity Connection Administration on the first server, expand **Networking**, then click **Connection Locations**.

Step 2 On the Search Connection Locations page, if the Display Name of the local server is "Local VMS" or matches the display name of another server, or if you want to modify it to choose a more descriptive name, continue with Step 3.

If the Display Name value appears to be unique and you do not want to change it, skip to Step 5.

Step 3 Click the Display Name to edit it.

Step 4 On the Edit Connection Location page, modify the Display Name value, and click **Save**.

Step 5 To check the SMTP domain, expand **System Settings > SMTP Configuration**, then click **Server**.

Step 6 On the SMTP Server Configuration page, if the SMTP Domain of the server matches the SMTP Domain of another server, continue with Step 7.

If the SMTP Domain appears to be unique, skip to Step 9.

Step 7 Click **Change SMTP Domain**, change the value of the SMTP Domain field, and click **Save**.

Step 8 Click **OK** to confirm the change.

Step 9 Repeat Step 2 through Step 8 for each remaining Connection server that will be joined to the Digital Network.

Joining Two Cisco Unity Connection Servers to Create a Digital Network

This section contains two procedures. We recommend that you start by doing the first procedure; if Cisco Unity Connection Administration does not indicate that the servers have successfully joined the network in the first procedure, do the second procedure.

- To Automatically Join Two Cisco Unity Connection Servers, page 33-6
- To Manually Join Two Cisco Unity Connection Servers, page 33-7

To Automatically Join Two Cisco Unity Connection Servers

Step 1 In Cisco Unity Connection Administration (on either server), expand **Networking**, then click **Connection Locations**.

Step 2 Click **Join Connection Network**.

Step 3 On the Join Connection Network page, click **Automatically Join the Network**.

Step 4 In the Remote Location field, enter the IP address or fully-qualified domain name (FQDN) of the Connection server to connect to in order to join the server to the network.

Step 5 In the Remote User Name field, enter the user name of an administrator at the location specified in the Remote Location field. The administrator user account must be assigned to the System Administrator role.

Step 6 In the Remote Password field, enter the password for the administrator specified in the Remote User Name field.

Step 7 Click **Auto Join Network**.

Step 8 When prompted, click **OK** to confirm. If the status message indicates that you have successfully joined the network and need to activate and start the Connection Digital Networking Replication Agent, continue with Step 9. Otherwise, skip the rest of this procedure and continue with the "To Manually Join Two Cisco Unity Connection Servers" procedure on page 33-7.

Step 9 On either server, in Cisco Unity Connection Serviceability, click **Tools > Service Management**.

Step 10 In the Server list, click the Connection server, and click **Go**.

Step 11 Under Optional Services, locate the Connection Digital Networking Replication Agent and click **Activate**.

Step 12 Repeat Step 9 through Step 11 on the other server.

To Manually Join Two Cisco Unity Connection Servers

Step 1 In Cisco Unity Connection Administration (on either server), expand **Networking**, then click **Connection Locations**. (This server is referred to as the first server for the remainder of the procedure, and the other server is referred to as the second server.)

Step 2 Click **Join Connection Network**.

Step 3 On the Join Connection Network page, click **Manually Join the Network**.

Step 4 Click **Download** and save the first server configuration file to a location on your hard drive, or on media that you can use to copy the file to the second server.

Step 5 Browse to Connection Administration on the second server.

Step 6 In Connection Administration on the second server, expand **Networking**, then click **Connection Locations**.

Step 7 Click **Join Connection Network**.

Step 8 On the Join Connection Network page, click **Manually Join the Network**.

Step 9 In the Select the Remote Configuration File to Upload field, click **Browse** and browse to the copy of the configuration file that you downloaded from the first server in Step 4.

Step 10 Click **Upload**.

Step 11 When the upload completes, click **Download**, and save the second server configuration file to a location on your hard drive.

Step 12 In Connection Administration on the first server, in the Select the Remote Configuration File to Upload field, click **Browse** and browse to your local copy of the configuration file that you downloaded from the second server in Step 11.

Step 13 Click **Upload**.

Step 14 On either server, in Cisco Unity Connection Serviceability, click **Tools > Service Management**.

Step 15 In the Server list, click the Connection server, and click **Go**.

Step 16 Under Optional Services, locate the Connection Digital Networking Replication Agent and click **Activate**.

Step 17 Repeat Step 14 through Step 16 on the other server.

Adding a Cisco Unity Connection Server to an Existing Network

When you add a Cisco Unity Connection server to an existing Connection network of two or more locations, you join the server to a single location on the network; the server you are adding receives a list of all the other locations on the network, exchanges information with each location, and begins replicating directory information with each location.

This section contains two procedures. We recommend that you start by doing the first procedure; if Cisco Unity Connection Administration does not indicate that the server has successfully joined the network in the first procedure, do the second procedure.

- To Automatically Join a Cisco Unity Connection Server to a Networked Server, page 33-8
- To Manually Join a Cisco Unity Connection Server to a Networked Server, page 33-8

To Automatically Join a Cisco Unity Connection Server to a Networked Server

Step 1 In Cisco Unity Connection Administration (on either server), expand **Networking**, then click **Connection Locations**.

Step 2 Click **Join Connection Network**.

Step 3 On the Join Connection Network page, click **Automatically Join the Network**.

Step 4 In the Remote Location field, enter the IP address or fully-qualified domain name (FQDN) of the Connection server to connect to in order to join the server to the network.

Step 5 In the Remote User Name field, enter the user name of an administrator at the location specified in the Remote Location field. The administrator user account must be assigned to the System Administrator role.

Step 6 In the Remote Password field, enter the password for the administrator specified in the Remote User Name field.

Step 7 Click **Auto Join Network**.

Step 8 When prompted, click **OK** to confirm. If the status message indicates that you have successfully joined the network and need to activate and start the Connection Digital Networking Replication Agent, continue with Step 9. Otherwise, skip the rest of this procedure and continue with the "To Manually Join a Cisco Unity Connection Server to a Networked Server" procedure on page 33-8.

Step 9 On the server you just added to the network, in Cisco Unity Connection Serviceability, click **Tools > Service Management**.

Step 10 In the Server list, choose the Connection server, and click **Go**.

Step 11 Under Optional Services, locate the Connection Digital Networking Replication Agent and click **Activate**.

To Manually Join a Cisco Unity Connection Server to a Networked Server

Step 1 In Cisco Unity Connection Administration on the server that is already joined to the network, expand **Networking**, then click **Connection Locations**.

Step 2 Click **Join Connection Network**.

Step 3 On the Join Connection Network page, click **Manually Join the Network**.

Step 4 If you already have a local copy of the configuration file for the server that is already joined to the network, skip to Step 5.

If you do not have a local copy of the configuration file, click **Download**, and save the file to a location on your hard drive.

Step 5 In Cisco Unity Connection Administration on the server that you are adding to the network, expand **Networking**, then click **Connection Locations**.

Step 6 Click **Join Connection Network**.

Step 7 On the Join Connection Network page, click **Manually Join the Network**.

Step 8 In the Select the Remote Configuration File to Upload field, click **Browse** and browse to your local copy of the configuration file for the server that is already joined to the network.

Step 9 Click **Upload**.

Step 10 When the upload completes, click **Download**, and save the configuration file of the server that you are adding to the network to a location on your hard drive.

Step 11 In Connection Administration on the server that is already joined to the network, in the Select the Remote Configuration File to Upload field, click **Browse** and browse to your local copy of the configuration file that you downloaded in Step 10.

Step 12 Click **Upload**.

Step 13 On the server that you just added to the network, in Cisco Unity Connection Serviceability, click **Tools > Service Management**.

Step 14 In the Server list, click the Connection server, and click **Go**.

Step 15 Under Optional Services, locate the Connection Digital Networking Replication Agent and click **Activate**.

Checking Replication Status

When initial replication begins among locations, it can take a few minutes to a few hours for data to be fully replicated between all locations, depending on the size of your directory.

The Connection Locations pages in Cisco Unity Connection Administration provide information about the status of replication between locations.

To Check Replication Status

Step 1 In Cisco Unity Connection Administration on a server that is joined to the network, expand **Networking**, then click **Connection Locations**.

Step 2 On the Search Connection Locations page, in the Locations table, the Push Directory column indicates whether a directory push to the remote location from the location you are accessing is in progress. The Pull Directory column indicates whether a directory pull from the remote location is in progress.

For example, if an administrator initiates a Push Directory To request from ServerA to ServerB, the Connection Administration on ServerA shows that a directory push to ServerB is in progress, and the Connection Administration on ServerB shows that a directory pull from ServerA is in progress.

Caution Initial replication happens automatically. Do not initiate a directory push or pull while initial replication is in progress.

Step 3 To get more information about the status of replication with a particular remote location, click the **Display Name** of the remote location.

Step 4 On the Edit Connection Location page, 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. If the Last USN Sent value is higher than the Last USN Acknowledged value, this location is not currently fully synchronized with the remote location; in this case, the Last USN Acknowledged value should continue to increase periodically. (Note that the Last USN Sent value may also increase periodically.)

Configuring a Smart Host

Revised May 2009

Digital Networking uses SMTP to transmit both directory information and messages between Cisco Unity Connection locations.

If any pair of locations in the Digital Network cannot transmit and receive SMTP messages directly (for example, because a firewall separates the servers), you must configure these locations to route these messages through an SMTP smart host.

In addition, for each Connection cluster that you add to the network, you must configure all other network locations to route to the cluster through a smart host in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down, and configure the smart host to resolve the SMTP domain of the cluster to the IP addresses of both the publisher and subscriber servers. For example, a network has a single smart host and the following three locations:

- ServerA, which is not a cluster member
- Cluster 1, which is made up of ServerB, a publisher, and ServerC, a subscriber
- Cluster 2, which is made up of ServerD, a publisher, and ServerE, a subscriber

In order to create a Digital Network, you would join ServerA, ServerB and ServerD together to form the network. Note the following:

- On ServerA, you would configure the Connection locations for ServerB (which represents cluster 1) and ServerD (which represents cluster 2) to route through the smart host.
- On Server B (the cluster 1 publisher), you would configure the Connection location for ServerD (which represents cluster 2) to route through the smart host.
- On ServerD (the cluster 2 publisher), you would configure the Connection location for ServerB (which represents cluster 1) to route through the smart host.
- On the smart host, you would configure the SMTP domain name of cluster 1 to resolve to the IP addresses of both ServerB and ServerC (for example, by using DNS MX records). You would also configure the SMTP domain name of cluster 2 to resolve to both ServerD and ServerE.

Do the following tasks for each server that requires routing to other locations through a smart host:

1. Configure the SMTP smart host to accept messages from the Connection server. If your Digital Network includes Connection clusters, also configure the smart host to resolve the SMTP domain of the cluster to the IP addresses of both the publisher and subscriber servers. See the documentation for the SMTP server application that you are using.
2. Configure the Connection server to relay messages to the smart host. See the "To Configure the Cisco Unity Connection Server to Relay Messages to a Smart Host" procedure on page 33-11.
3. Configure the Connection server to route messages to the other Connection locations through the smart host. See the "To Configure the Cisco Unity Connection Server to Route Inter-Location Messages through the Smart Host" procedure on page 33-11.

To Configure the Cisco Unity Connection Server to Relay Messages to a Smart Host

Step 1 In Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then click **Smart Host**.

Step 2 In the **Smart Host** field, enter the IP address or fully qualified domain name of the SMTP smart host server. (Enter the fully qualified domain name of the server only if DNS is configured.)

Step 3 Click **Save**.

To Configure the Cisco Unity Connection Server to Route Inter-Location Messages through the Smart Host

Step 1 In Cisco Unity Connection Administration, expand **Networking**, then click **Connection Locations**.

Step 2 Click the name of a location that requires routing through a smart host.

Step 3 Check the **Route to This Remote Location Through SMTP Smart Host** check box.

Step 4 Click **Save**.

Step 5 Repeat Step 1 through Step 4 for each additional location that requires routing through the smart host.

Configuring SMTP Access for Cluster Subscriber Servers

Revised May 2009

When you create a Digital Network that includes a Cisco Unity Connection cluster server pair, you join only the publisher server of the pair to the network. In order for all locations on the network to communicate with the cluster subscriber server in the event that it has Primary status, you must configure all network locations (except for the publisher server that is clustered with the subscriber server) to allow SMTP connections from the subscriber server.

Directory updates are only replicated from the cluster publisher server. SMTP connectivity is needed so that locations can continue to receive user message traffic while the publisher server does not have Primary status. Replication resumes as soon as the publisher server has Primary status again.

For example, a network has the following three locations:

- ServerA, which is not a cluster member
- Cluster 1, which is made up of ServerB, a publisher, and ServerC, a subscriber
- Cluster 2, which is made up of ServerD, a publisher, and ServerE, a subscriber

In order to create a Digital Network, you would join ServerA, ServerB and ServerD together to form the network. Note the following:

- On ServerA, you would need to add the IP addresses of both ServerC and ServerE (the two subscriber servers) to the IP access list so that ServerA can communicate with either subscriber server if it has Primary status.
- On ServerB (the cluster 1 publisher), you would add the IP address of ServerE (the cluster 2 subscriber) to the IP access list; and on ServerD (the cluster 2 publisher), you would add the IP address of ServerC (the cluster 1 subscriber) to the IP access list.

To Configure SMTP Access for Cluster Subscriber Servers

Step 1 On a network location, in Cisco Unity Connection Administration, expand **System Settings > SMTP Configuration**, then click **Server**.

Step 2 On the Edit menu, click **Search IP Address Access List**.

Step 3 Click **Add New**.

Step 4 On the New Access IP Address page, enter the IP address of a cluster subscriber server at another location on the network.

Note Do not enter the IP address of the subscriber server on the publisher server that it is paired with.

Step 5 Click **Save**.

Step 6 On the Access IP Address page, check the **Allow Connection** check box.

Step 7 Click **Save**.

Step 8 Repeat Step 2 through Step 7 for each additional subscriber server on the network (other than the subscriber server that is paired with the server you are configuring).

Step 9 Repeat Step 1 through Step 8 on each network location.

Configuring Search Spaces for Digital Networking

When you initially set up Digital Networking between the servers, users who are homed on one location are not able to address messages to users at other locations, because the users on each location are in separate partitions and use search spaces that do not contain the partitions of users on the other locations. After initial replication completes between the locations, you can reconfigure your search spaces to include partitions that are homed on other servers, and you can change the search scope of users, routing rules, call handlers, directory handlers, and VPIM locations to use a search space that is homed on a remote location. (Note that while both partitions and search spaces are replicated between locations, you cannot assign users or other objects to a partition that is homed on another location.)

At a minimum, if you have not made any changes to the default partitions and search spaces on any server, at each location you can add the default partition of each remote Cisco Unity Connection location to the search space that local users are using. For example, in a network of three servers named ServerA, ServerB, and ServerC with no changes to the system defaults, in Cisco Unity Connection Administration on ServerA you would add the “ServerB Partition” and “ServerC Partition” default partitions as members of the “ServerA Search Space” default search space; in Connection Administration on ServerB you would add “ServerA Partition” and “ServerC Partition” to “ServerB Search Space,” and so on.

For instructions on adding partitions to search spaces see the "Managing Search Spaces" section on page 28-9.

Securing the Digital Networking Setup

No user credentials are transmitted as part of Digital Networking communications. However, in order to protect the security of SMTP addresses that are contained in the messages, make sure that any smart hosts that are involved in SMTP message transmission between Connection locations are configured to route messages properly, as it may be possible to extract SMTP addresses from the messages.

Configuring Cross-Server Logon and Transfers

The cross-server logon feature allows users to call the same number regardless of which Cisco Unity Connection server they are homed on, and they are transferred to the applicable home Connection server to log on. If you do not enable cross-server logon, users need to call the phone number of their home Connection server to log on.

The cross-server transfer feature enables calls from the automated attendant or from a directory handler of one Connection location to be transferred to a user on another networked Connection location, according to the call transfer and screening settings of the called user. When you enable cross-server transfers, cross-server live reply is automatically supported for users whose class of service allows live reply to other users. (Cross-server live reply allows users who listen to their messages by phone to reply to a message from a user on another Connection location by calling the user according to the call transfer and screening settings of the called user.) If you do not enable cross-server transfer, call transfers and live replies to users at other Connection locations are performed by using release-to-switch transfers to the Cross-Server Transfer Extension that is configured on the recipient User Basics page. If you do not enable cross-server transfers and you do not configure the Cross-Server Transfer Extension for a user, then callers who attempt to transfer to the user from another location hear the system default greeting and are able to leave a message for the user instead of being transferred.

By default, each Connection server is configured to ignore cross-server hand-off requests. You can enable cross-server logon and cross-server transfer individually between each pair of locations. In addition to enabling the hand-off and configuring a dial string on the originating location, you must configure the receiving location to accept hand-offs. Do the "To Enable Cross-Server Logon and Transfers Between Cisco Unity Connection Locations" procedure on page 33-14.

Search Space Considerations for Cross-Server Logon and Transfers

When setting up cross-server logon, note that 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. If a user calls from an extension that is in a partition that is not a member of the search space set as the initial search scope for the call, the call is not identified as coming from the user. If the extension of the user overlaps with an extension in another partition that also appears in this search space, the call is identified as coming from the first object that Connection finds when searching the partitions in the order in which they appear in the search space. Check the direct routing rules on each location that handles logon calls from remote users to determine the search space that 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.

Also note that a mismatch between the search space that is applied to the call on the originating location and the search space that is applied on the receiving location can cause problems for cross-server logins and cross-server transfers. A match could be made on the search scope on the originating location that cannot be made on a different search scope on the receiving location. For this reason, we recommend

that you verify that the same search scope is configured on both originating and receiving locations. For example, call routing rules can be used to direct cross-server calls on the receiving location to the appropriate search space based on the cross-server dial string that is used to reach that location.

To Enable Cross-Server Logon and Transfers Between Cisco Unity Connection Locations

Step 1 In Cisco Unity Connection Administration, on a location that handles logon calls from remote users or transfers calls to remote users (the originating location), expand **Networking**, then click **Connection Locations**.

Step 2 Click the Display Name of a remote location that will accept cross-server logon or transfer hand-offs for users who are homed on that location (the receiving location).

Step 3 On the Edit Connection Location page for the receiving location, do the following to initiate cross-server hand-offs to this receiving location:

a. To enable cross-server logon hand-offs to the remote location, check the **Allow Cross-Server Login to this Remote Location** check box.

b. To enable cross-server transfer hand-offs to the remote location, check the **Allow Cross-Server Transfer to this Remote Location** check box.

c. Enter the dial string that this location will use to call the remote location when performing the hand-off (for example, the pilot number of the home server).

Note You can enter only one dial string for each remote location that receives hand-offs. If the initiating server is configured for multiple phone system integrations, enter a dial string that all phone system integrations can use to reach the remote location.

Step 4 Repeat Step 1 through Step 3 on the originating location to configure each remote location that accepts cross-server logon or transfer hand-offs from this location.

Step 5 To configure the originating location to also accept cross-server logon or transfer requests from other locations (as a receiving location), do the following:

a. In Cisco Unity Connection Administration, expand **System Settings > Advanced**, then click **Conversations**.

b. Check the **Respond to Cross-Server Handoff Requests** check box.

Step 6 Repeat Step 1 through Step 4 on each location that performs cross-server logon and transfer hand-offs (as an originating location).

Step 7 Repeat Step 5 on each location that receives cross-server hand-offs (as a receiving location).

Testing the Digital Networking Setup

To test the Digital Networking setup, create test user accounts or use existing user accounts on each Cisco Unity Connection location. When setting up user accounts in Cisco Unity Connection Administration to be used in the tests, be sure to do the following for each account:

- Record a voice name.
- Record and enable an internal greeting.
- Assign the user to a search space that includes the partitions of remote users.

- On the User Basics page, check the List in Directory check box.
- On the Playback Message Settings page, check the Before Playing Each Message, Play the Sender's Information check box.

Do the following tests to confirm that Digital Networking is functioning properly:

- To Verify Messaging Between Users on Different Cisco Unity Connection Locations, page 33-15
- To Verify Call Transfers From the Automated Attendant to Users on Other Cisco Unity Connection Locations, page 33-15
- To Verify Call Transfers from a Directory Handler to Users on Other Cisco Unity Connection Locations, page 33-15
- To Verify Identified User Messaging Between Networked Users (When Identified User Messaging Is Enabled), page 33-16
- To Verify Live Reply Between Users on Different Cisco Unity Connection Locations, page 33-16

To Verify Messaging Between Users on Different Cisco Unity Connection Locations

Step 1 Log on to a Cisco Unity Connection location as a user.

Step 2 Follow the prompts to record and send messages to users who are associated with other Connection locations.

Step 3 Log on to the applicable Connection location as the recipient user 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 Users on Other Cisco Unity Connection Locations

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

Step 2 Verify that you reach the correct user phone.

To Verify Call Transfers from a Directory Handler to Users on Other Cisco Unity Connection Locations

Step 1 From a non-user phone, call the Connection location that has been configured to handle outside callers, and transfer to a directory handler.

Step 2 Verify that you can find a user who is associated with another Connection location in the phone directory, and that the directory handler transfers the call to the correct user phone.

To Verify Identified User Messaging Between Networked Users (When Identified User Messaging Is Enabled)

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

a. From a user phone, call a user who is associated with another Connection location, and allow the call to be forwarded to Connection.

b. Verify that the internal greeting plays.

c. Leave a test message.

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

a. Log on to the applicable Connection location as the recipient user and listen to the test message that you recorded in Step 1.

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

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

To Verify Live Reply Between Users on Different Cisco Unity Connection Locations

Step 1 From a user phone, call a user who is associated with another Connection location, and allow the call to be forwarded to voice mail.

Step 2 Leave a message.

Step 3 Log on to the applicable Connection location as the recipient user and listen to the test message that you recorded in Step 2.

Step 4 After listening to the message, verify that the user conversation allows you to live reply to the message by saying "Call sender" or by using the applicable key presses for the user conversation type. (To find the key presses for a particular conversation, see the "Cisco Unity Connection Phone Menus and Voice Commands" chapter of the *User Guide for the Cisco Unity Connection Phone Interface*.)

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

Creating a Network-Wide All Voice Mail Users Distribution List

If you would like to create a master distribution list that includes all users on all servers, do the following tasks:

1. On each location on the Digital Network, rename the All Voice Mail Users list with a unique name (for example All Voice Mail Users on <Server Name>). For instructions, see the "Modifying System Distribution Lists" section on page 27-3.
2. Create a new All Voice Mail Users system distribution list on one location to use as the master list.
3. Add the lists from all locations as members of the master list.
4. Put all lists except the master list in partitions that do not belong to a search space that users use, so that they cannot address to any list except the master. For example, on each location, create a new partition called Hidden DLs on <Server Name> and put the list homed at that location in that partition. (By default, new partitions are not a member of any search space.)

Tip To avoid having users generate large amounts of voice message traffic by using reply-all to reply to messages sent to the master list, we strongly recommend that you use search spaces to restrict access to the master list to a small subset of users. These users can use a search space that is essentially identical to the search space that other users use, except for the addition of the partition containing the master list.

Cleaning Up Unused Cisco Unity Connection VPIM Locations and Contacts

After migrating a Cisco Unity Connection server from VPIM Networking to Digital Networking, you should delete the VPIM location for the server on any other servers on the Digital Network that were previously using VPIM Networking to exchange messages with the server. Likewise, you should delete any VPIM locations on the server that represent other Connection locations on the Digital Network. In order to successfully delete the VPIM locations, you must first delete all contacts that are associated with the location.

Note that when you delete the VPIM contacts that represent Connection users, the contacts are removed from distribution lists; consider reviewing and updating distribution list membership on each server to include remote users as applicable. Also consider notifying users that they need to update the membership of any private lists that include contacts on the server being migrated.

For instructions on deleting a VPIM location and the associated VPIM contacts, see the "Removing a VPIM Location" section on page 34-15.

Manually Synchronizing Locations

If you notice that the directory does not seem to be synchronized between two network locations, do the following procedure.

To Check and Manually Synchronize Locations

Step 1 In Cisco Unity Connection Serviceability on each location, click **Tools > Service Management**. Verify that the Connection Digital Networking Replication Agent service is active on both locations. If it is not active, activate it.

Tip The status message on the Networking > Connection Locations page in Cisco Unity Connection Administration also alerts you if the replication agent is not active.

Step 2 In Cisco Unity Connection Administration on either location, expand **Networking**, then click **Connection Locations**.

Step 3 On the Search Connection Locations page, click the Display Name of the other location.

Step 4 On the Edit Connection Location page, check the values of the Last USN Sent and Last USN Acknowledged fields.

If the Last USN Sent value equals the Last USN Acknowledged value, skip to Step 5.

If the Last USN Sent value is higher than the Last USN Acknowledged value, and the Last USN Acknowledged value is not increasing after a minute or two, do the following:

a. Return to the Search Connection Locations page.

b. Check the check box next to the Display Name of the other location.

c. Click **Push Directory To**.

d. Wait until replication completes. The Networking > Connection Locations page indicates the status of replication (you must reload the page to update the status).

Step 5 Repeat Step 2 through Step 4 in Cisco Unity Connection Administration on the other location.

Removing a Location From the Network

Revised May 2009

When you remove a location from a Digital Network, it stops replicating directory information with other locations, and all objects that are homed on the server are removed from other locations. Conversely, all objects that are homed on other locations on the network are removed from the server you are removing.

We recommend that you carefully consider the impacts of removing a location from the Digital Network prior to doing so, particularly if you plan to add the location back to the network later. Consider the following impacts:

- Users on the server are removed from distribution lists that are homed on other locations in the Digital Network, and users on other locations are removed from distribution lists that are homed on the server you remove. If you later add the server back into the Digital Network, you need to update distribution list membership on the re-added server to include any remote users, and update distribution list membership on all other locations in the network to include users on the re-added server.
- System call handlers and interview handlers on other locations that are configured to send messages to a user or distribution list that is homed on the server you remove are reconfigured to send messages to the undeliverable messages list of the location. Likewise, system call handlers and interview handlers on the server you remove that are configured to send messages to a user or distribution list that is homed on another location are reconfigured to send messages to the local undeliverable messages list. If you later add the server back into the Digital Network, you need to update the recipients for these handlers to use the correct remote object. (Even if you do not plan to add the server back into the Digital Network, you should make sure that someone is checking messages that are sent to the undeliverable messages list, or reassign handlers that use it as a recipient.)
- Partitions that are homed on the server are removed from search spaces that are homed on other locations in the Digital Network, and partitions that are homed on other locations are removed from search spaces that are homed on the server you remove. A copy is made of search spaces that are homed on the server that are in use by other locations in the Digital Network (and likewise, the server makes a copy of remote search spaces that are homed on other locations). The copies replace the original search spaces on any objects that reference them. If you later add the server back into the Digital Network, you need to update the partition membership of search spaces on the re-added server to include any remote partitions, and update the partition membership of search spaces on all other locations in the network to include partitions on the re-added server.
- On each location in the Digital Network, there are configuration settings specific to other locations (for example, the fields related to cross-server transfers and SMTP routing). When you remove a server from the network, the settings for all locations in the network are deleted from the server that you remove, and the settings for the server that you remove are deleted from all other locations in

the network. If you later add the server back into the Digital Network, you need to update the settings for the re-added server on all other locations in the network, and configure the settings for all other locations on the re-added server.

Do the following procedure to remove a location from the Digital Network. You can remove only one Connection location from the network at a time.

Depending on the size of the directory, removing a Cisco Unity Connection location can take a few minutes to a few hours. Even though the operation may have completed on the local location, it may continue to be in progress on remote locations. We recommend that you wait for the removal operation to complete on all locations in the network before making additional changes to the network.

To Remove a Cisco Unity Connection Location From the Digital Network

Step 1 In Cisco Unity Connection Administration on any location in the Digital Network, expand **Networking**, then click **Connection Locations**.

Step 2 Check the check box to the left of the Display Name of the location that you want to remove.

Step 3 Click **Remove Selected**.

Step 4 Click **OK** to confirm the removal.

Caution Until Connection Administration returns a status message indicating that the removal is complete, avoid making other changes on the Digital Network (for example, removing another location, joining a new location to the network, or initiating a directory push or pull).

Digital Networking Concepts and Definitions

The following sections explain Digital Networking concepts in detail:

Cisco Unity Connection Locations and Digital Networking

Central to how Digital Networking works is an object referred to as a Cisco Unity Connection location. Each Connection server (or cluster) on the network is represented by a single Connection location, which is created locally during installation and which cannot be deleted from the server itself. When you join the server (or cluster) to a Digital Network, a Connection location is created for the server (or cluster) on all other locations in the network, and these locations automatically begin to perform directory

synchronization with the new location. If you remove the server (or cluster) from the Digital Network, the corresponding Connection location is removed from all other locations on the network, and its directory information is automatically removed from these locations (and vice versa). A Connection location can only belong to a single Digital Network. As soon as you join one server to a location on the Digital Network, any other locations on the network are notified of the new location and begin to exchange directory information with the new location.

All objects that you create on a particular location are said to be "homed" on that location. To modify the properties of an object or to delete the object, you must use the administration tools on the location that homes the object. Each location has its own directory of users and other objects, and replicates a subset of these objects and their properties to other locations; the collection of objects and object properties that are replicated among locations is referred to as the Connection directory.

In the context of Digital Networking, an object that is homed on a location is sometimes referred to as local for that location (for example, a local user) and an object that is homed on a different location is referred to as remote.

Object Replication

Each Cisco Unity Connection location replicates the objects and object properties shown in Table 33-1 from its directory to other locations:

Table 33-1 Replicated Objects in Cisco Unity Connection Digital Networks

Replicated Object	Replicated Properties
Users with mailboxes	• Alias • First name, last name, alternate names • Extension, cross-server transfer extension, and alternate extensions • Partition • Recorded voice name • SMTP proxy addresses
System contacts	All properties
System distribution lists	All properties, including list membership
Partitions	All properties
Search spaces	All properties
Connection location	• Display name • Host address • SMTP domain name • Connection version
VPIM locations	All properties except Contact Creation settings (contact creation is handled on the Connection location that homes the VPIM location)

In most cases, you can use replicated objects just as you would use local objects; for example, you can assign a remote user to be the message recipient of a system call handler, or configure the search scope of a user to use a remote search space. Note the following exceptions:

- System call handler owners must be local users.
- Objects that have partition membership (users, contacts, handlers, system distribution lists, and VPIM locations) can only belong to local partitions. You can, however, add a remote partition to a local search space.

When a replicated object that is homed on a Connection location is added, modified or deleted, the location sends an object change request containing details about the change to all other locations. The object change requests for a given location are ordered and tracked with a number known as the Universal Sequence Number (USN). For each change, the location increments the USN by one, and notes the change in its database. When a remote location receives an object change request with a USN value that is one higher than the previous request it received from the sender, it updates its copy of the Connection directory accordingly, and increments its tracked copy of the USN for the sender. If a remote location misses one or more changes and receives a change request with a USN that is more than one higher than the previous request it received from this location, it can request the missed changes by sending the USN values that it missed.

In addition to the USN, each location has another associated number known as the Replication Set. The Replication Set value is used to track the set of changes to which a USN belongs. The Replication Set value is automatically changed during an upgrade, restore, or rollback. This ensures that any changes to the database as a result of the operation are replicated to the network. For example, if Location A receives a message with replication set 10 and USN 5 from Location B, and then receives a message with replication set 9 and USN 5 from Location B, it knows to ignore the message with replication set 9 because it is a lower number and the message predates the message with replication set 10. If Location A receives another message from Location B with replication set 10 and USN 5 again, Location A knows this is a duplicate message and can ignore it.

Addressing Options for Non-Networked Phone Systems

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

When user extensions on one Connection location overlap with user extensions on another location, you can provide unique extensions for each user by setting up alternate extensions for each user account. For each user, enter a number for the alternate extension that is the same as the full phone number for the user, and make sure the alternate extension is in a partition that is a member of the search spaces that users at other locations use. In this way, when users log on to Connection to send messages, the number they enter when addressing messages is the same number that they use when calling.

When Connection numbering plans do not overlap across locations—that is, when user extensions are unique across locations—users can enter an extension when addressing a message to a user who is associated with another Connection server. As a convenience for users, you may choose to add alternate extensions to each user account, so that users do not need to remember two different numbers—one for calling a user directly, and one for addressing a message. If the numbering plans for each location do not overlap, setting up alternate extensions is optional because they are simply a convenience for users. However, if you do not set up alternate extensions, be sure to tell users to use the extension instead of the full phone number when addressing messages to users 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 user phones. For more information, see the "Alternate Extensions" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Identified User Messaging Between Networked Cisco Unity Connection Users

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

- Connection plays the internal greeting of the called user when the caller leaves a message.
- Connection plays the recorded voice name of the user who left the message when the recipient listens to the message.
- Connection allows the recipient to record a reply.

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

- A user logs on to Connection, and then records and sends a message. In this circumstance, when the user has logged on to Connection, Connection can identify the message as being from the user, regardless of which Connection 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.
- A user places a phone call to another user, and then leaves a message. This circumstance is the basis of identified user messaging. As long as identified user messaging is enabled on a Connection location, Connection is able to identify both local and remote users. Note, however, that for identified user messaging to work in both cases, the initial search scope of the call must be set to a search space that locates the correct user based on the calling extension, regardless of whether the caller is a local or remote user.

  If a user calls from an extension that is in a partition that is not a member of the search space set as the initial search scope for the call, the call is not identified as coming from the user. If the extension of the user overlaps with an extension in another partition that also appears in this search space, the call is identified as coming from the first object that Connection finds when searching the partitions in the order that they appear in the search space.

  In situations where numbering plans overlap across locations, it is therefore possible to have a user leave a message that is incorrectly identified as coming from another user with the same extension in a different partition. Because the initial search scope of the call is based on call routing rules, to avoid this situation, use the following configuration guidelines:

  - Maintain a separate search space for each location in which the partition containing its users appears first in the search space. (By default, each Connection server uses its own default partition and default search space, which are replicated to other locations when the server is networked.)
  - On each location, set up forwarded call routing rules specific to each other location by specifying a routing rule condition that applies only to calls from the location (for example, based on the port or phone system of the incoming call). Configure the rule to set the search scope of the call to the search space in which the partition containing users at the location appears first.

Cross-Server Logon and Transfers

In order to limit replication traffic and keep the directory size manageable, only a subset of user information is replicated from the home location of the user to other locations on the Digital Network. For this reason, only the user home location has information about call transfer settings, greetings, and other specific details for the user. In order for a Cisco Unity Connection location to properly handle calls destined for a user on a different location, Connection must hand off the call to the home location of the user.

When a Connection location initiates a cross-server logon, cross-server transfer, or cross-server live reply to hand off a call to another location, the hand-off details are negotiated by using DTMF tones, in the following process:

1. The Connection location on which the logon, transfer, or live reply originates puts the caller on hold and calls the home Connection location.
2. When the home location answers, the originating location sends a sequence of DTMF tones that identify the call as a hand-off request.
3. The home location responds with a sequence of DTMF tones, and the originating location hands off the call to the home location for processing along with a DTMF packet that contains the caller ID and the called ID.

At this point the functionality is the same as if the call had originated on the home location.

Systemwide advanced conversation settings allow you to modify the parameters of hand-off calls.

System Distribution Lists

Because system distribution lists are replicated among locations in the network, a user can address messages to any system distribution list at any location, as long as the list is reachable in the user search scope.

When a user addresses a message to a system distribution list, the local Cisco Unity Connection location parses the distribution list membership. The sending location first addresses messages to any VPIM users that are on the distribution list. Next, the sending location checks to see if there are any remote Connection users in the membership; if so, it sends a single message to each location that homes these remote users, addressed to the distribution list (the home locations each parse the message and deliver to their local users). Finally, the sending location checks for local users in the distribution list membership, and delivers the message to each of them.

Connection includes the following predefined system distribution lists: All Voice Mail Users, Undeliverable Messages, and All Voicemail-Enabled Contacts. Each Connection server in your organization has a distinct version of each of these lists. If you have not changed the names of these lists to be unique, during initial replication each server automatically adds the remote server name to the display name of any remote lists whose names overlap with local list names.

By default, the predefined lists on each Connection location have the same recorded voice name, and the All Voice Mail Users and All Voicemail-Enabled Contacts lists have the same extension at each location (the Undeliverable Messages list by default is not assigned an extension, because users do not typically address messages to this list). When setting up Digital Networking, you should consider modifying the recorded voice name of each All Voice Mail Users list and each All Voicemail-Enabled Contacts list; if you do not, users can hear a confusing list of choices when they address messages by name to one of these lists. When users address by extension to a list whose extension overlaps that of another list, they reach the first list that is located when Connection searches the partitions of the user search space in order.

Tip Distribution lists can be nested such that a distribution list contains other lists. You can create one master All Voice Mail Users distribution list that contains the All Voice Mail Users list of each Connection location.

Private Distribution Lists

When creating private lists, users can add members from other locations if allowed by their search scope, in which case the same set of users who are reachable when addressing a message or placing a call can also be added as members of a private list. Private lists are not replicated to other locations; when a user addresses a message to a private list, the home location of the user expands the distribution list and addresses messages to each individual recipient on the list.

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

- When you delete a Cisco Unity Connection location, remote users at that location are removed from all private lists.
- When a VPIM contact becomes a Connection user, the contact is removed from all private lists.

VPIM Locations and Digital Networking

When you use the recommended approach of configuring a single Cisco Unity Connection location on the Digital Network as a bridgehead to handle all VPIM locations, the VPIM location data and all contacts at the VPIM location (including automatically created contacts) are replicated to other locations in the network. When a VPIM message is sent to or from a user at another Connection location, the message first passes to the bridgehead, which handles forwarding the message to the destination server.

If necessary to handle your topology, you can check the Route to this Remote Location Through SMTP Smart Host check box on the VPIM location page in Cisco Unity Connection Administration on the bridgehead server. You may need to do this if, for example, a firewall separates the Connection location from the VPIM location. (Note that in order to route to a location through the smart host you must also configure the smart host on the System Settings > SMTP Configuration > Smart Host page in Connection Administration on the bridgehead server.)

Notable Behavior

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

See the following sections:

- Broadcast Messages, page 33-25
- Client Access to Digitally Networked Cisco Unity Connection Servers, page 33-25
- Mapping Users to Cisco Unity Connection Systems, page 33-25
- Replication During Bulk Operations, page 33-25
- Replication with Cisco Unity Connection Clusters, page 33-25

Broadcast Messages

Broadcast messages cannot be sent to multiple locations on a Cisco Unity Connection network.

Client Access to Digitally Networked Cisco Unity Connection Servers

Users on each server must access their home server (or cluster) when using the Cisco Personal Communications Assistant (PCA) and IMAP clients. The phone interface is the only client that provides cross-server logon capability.

Mapping Users to Cisco Unity Connection Systems

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

- User phones must forward calls to the Connection system on which the users are homed.
- If user phones have a "Messages" or a speed-dial button that dials the number to access Connection, the buttons must be configured to call the Connection system on which the users are homed.
- If you do not configure cross-server logon, users must dial the Connection system that they are associated with to check their messages; in this case, you need to tell users the correct number to dial when calling into Connection.

To create a record of the mapping, run the Users report on each Connection system. The information in this report includes the user name and primary location. See the "Generating Reports" chapter for more information.

Replication During Bulk Operations

Replication is paused during bulk operations, and resumes as soon as the operation completes.

Replication with Cisco Unity Connection Clusters

When you create a Digital Network that includes a Cisco Unity Connection cluster server pair, you join only the publisher server of the pair to the network; directory updates made on a cluster subscriber server are replicated only from the cluster publisher server. If the Digital Network is properly configured, messages continue to be sent to and from the cluster even when the subscriber server has Primary status. However, in order to keep the directory current on the publisher server, the secondary server should not have Primary status for an extended period of time.