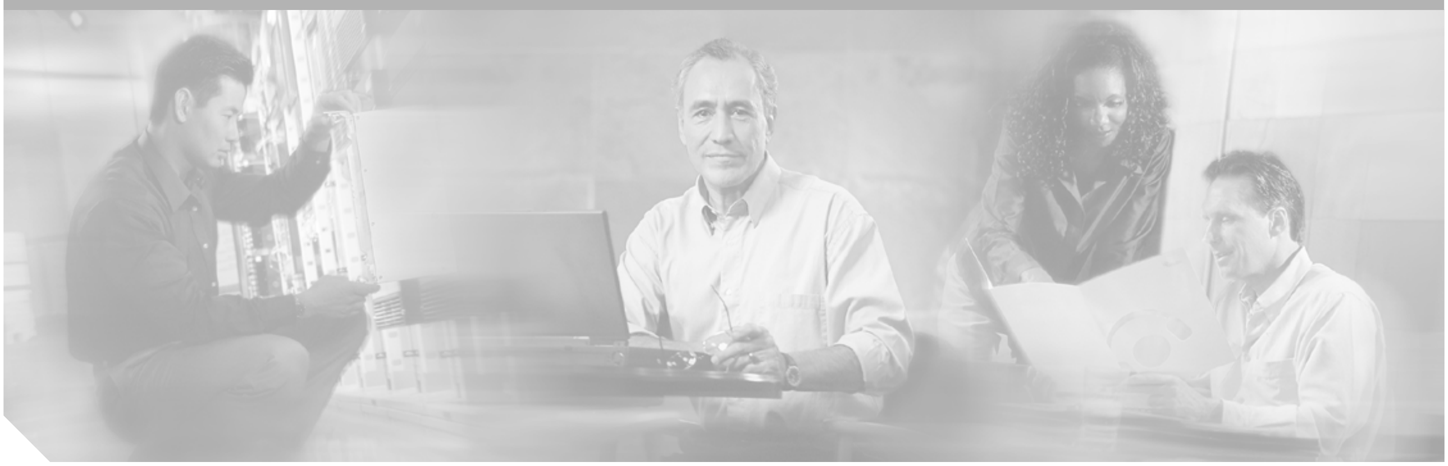


Cisco Unity Express Design Guide

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

CONTENTS

Preface

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

Purpose

This version of *Cisco Unity Express Design Guide* presents some basic network design content and best-practice recommendations, but it is not yet complete. The technical staff responsible for the content provided in this publication plans to incorporate additional network design material as it becomes available.

Note The content in this publication applies to Cisco Unity Express 2.1 unless specifically noted in the text.

Topis addressed with this version of the design guide include:

- Cisco Unity Express deployment models
- Basic network infrastructure design for Cisco Unity Express
- Cisco Unity Express system design
- Auto-attendant (AA) design considerations for Cisco Unity Express
- Voice-mail considerations for Cisco Unity Express

The *Cisco Unity Express Design Guide* does not provide implementation, configuration or troubleshooting information.

Audience

The *Cisco Unity Express Design Guide* is intended for system administrators and others responsible for designing a network in which Cisco Unity Express provides auto attendant (AA) or voice mail to users at one or more sites. To apply the design content presented, you must have a working knowledge of the configuration, features and operation of the systems that coexist with Cisco Unity Express in your network. Applicable systems include Cisco Call Manager Express, (CME), Cisco CallManager, and Cisco Unity.

Document Conventions

This guide uses the conventions in Table 1.

Table 1 Cisco Unity Express Design Guide Document Conventions

Convention	Description
bold text	Boldfaced text is used for: • Key and button names. (Example: Click **OK**.) • Information that you enter. (Example: Enter **Administrator** in the User Name box.) • In command-line interface (CLI) configuration examples, specific command statements are highlighted for emphasis in the context of the accompanyng description.
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter **ping** <IP address>.)
- (hyphen)	Hyphens separate keys that you must press simultaneously. (Example: Press **Ctrl-Alt-Delete**.)
> (right angle bracket)	A right angle bracket is used to separate selections that you make: • On menus. (Example: On the Windows Start menu, click **Settings** > **Control Panel** > **Phone and Modem Options**.) • In the navigation bar of the Cisco Unity Administrator. (Example: **Go to the System** > **Configuration** > **Settings** page.)
The letter *a* is used in the high-order address range for an IP V4-formatted address. Example: a.10.224	Represents a public Class A Internet address or network.
The letter *b* is used in the high-order address range for an IP V4-formatted address. Example: b.121.10.22	Represents a public Class B Internet address or network.
The letter *x* and *y* used in a phone number Example: xxx.yyy.1234	Represents the area code and prefix for a telephone number.
The letter *n* used in a phone number. Example: xxx.yyy.nnnn	Represents a generalized telephone extension.

The *Cisco Unity Express Design Guide* also uses the following conventions:

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

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

Chapter 1: Cisco Unity Express Deployment Models

Cisco Unity Express is an entry-level auto-attendant (AA) and voice-mail system that is integrated with a Cisco IOS router for small-to-medium business or enterprise branch offices requiring up to 100 mailboxes.

Cisco Unity Express provides a distributed AA and voice-mail application to an IP Telephony solution where the large offices may have a high-end voice mail solution (such as Cisco Unity) and one or more of the smaller remote offices may use a local or distributed Cisco Unity Express for voice mail. Cisco Unity Express is deployed with one of two call-processing models that are based on either Cisco CME or Cisco CallManager.

The call processing engine (Cisco CME or Cisco CallManager) manages the IP phones and features such as call-forward-busy (CFB) and call-forward-no-answer (CFNA) to the voice mail pilot number, while Cisco Unity Express provides the AA menus, scripts and voice mail telephony user interface (TUI) sessions for callers retrieving or leaving voice messages. Cisco Unity Express stores the AA scripts and prompts, voice mail subscriber spoken names, greetings and voice mail messages.

Cisco Unity Express interfaces with Cisco CME call control via a Session Initiation Protocol (SIP) interface and to Cisco CallManager via a Java Telephony Applications Programming Interface (JTAPI) interface.

Cisco Unity Express Overview

Cisco Unity Express is offered in two forms: a Network Module (NM) and an Advanced Integration Module (AIM) that is added to the router in the office. Cisco Unity Express hardware includes a CPU to offload AA and voice-mail processing from the router CPU such that Cisco Unity Express has minimal impact on the router CPU, as well as storage (hard disk on the NM and compact flash on the AIM) for the AA menus, prompts, voice-mail greetings, and messages.

The NM-CUE offers up to 100 hours of voice mail storage and is available as of Cisco Unity Express 1.0. The AIM-CUE offers up to 8 or 14 hours of storage (depending on which flash card is equipped) and is available as of Cisco Unity Express 1.1. Cisco Unity Express is available in four different product tiers (or licenses), including a 12-mailbox, 25-mailbox, 50-mailbox and 100-mailbox license.

The key benefits of Cisco Unity Express include the following:

- Provides a cost-effective, Cisco-integrated voice mail solution for IP phones in the branch or remote office as part of the full-service branch (FSB) evolution.
- Delivers a router-integrated AA and voice-mail application for Cisco CME.

- Enables a decentralized voice-mail solution in a centralized Cisco CallManager network. It keeps voice-mail traffic off the WAN (does not require the WAN to have the bandwidth and quality of service (QoS) to carry real-time traffic). As a result, voice-mail availability continues during WAN failures—via Cisco Survivable Remote Site Telephony (SRST).

Standalone Office

The deployment model shown in Figure 1 is a single site representing a standalone (autonomous) small-medium business office, such as a medical or legal office. While it is possible to create this deployment with either Cisco CME or Cisco CallManager as the call controller, it is almost certain to be Cisco CME (shown in Figure 1) as Cisco CallManager is not cost-effective for a standalone environment where there are fewer than 250 people in the office.

This type of office has very limited or no IT expertise. A Cisco partner, reseller, or systems integrator (SI) is likely to install, configure, and maintain the system. An Internet Service Provider (ISP) or local exchange carrier (LEC) is likely to provide the Internet and PSTN service. It is possible that this organization may also sell, install, and maintain the system for the small-medium business. If the end customer performs configuration changes on the Cisco Unity Express system, end-customer network administration staff will access the system via the GUI (not the CLI). The SI or ISP may well access the system via the CLI.

Figure 1 Standalone Office

The office environment depicted in Figure 1 includes the following characteristics:

- All offnet voice connectivity is via the PSTN to customers or clients of the business.
- Onnet voice calls are made between IP phones connected in the office.
- The data connectivity from the site is purely for Internet access and is connected to a local ISP service.

Multisite Networks

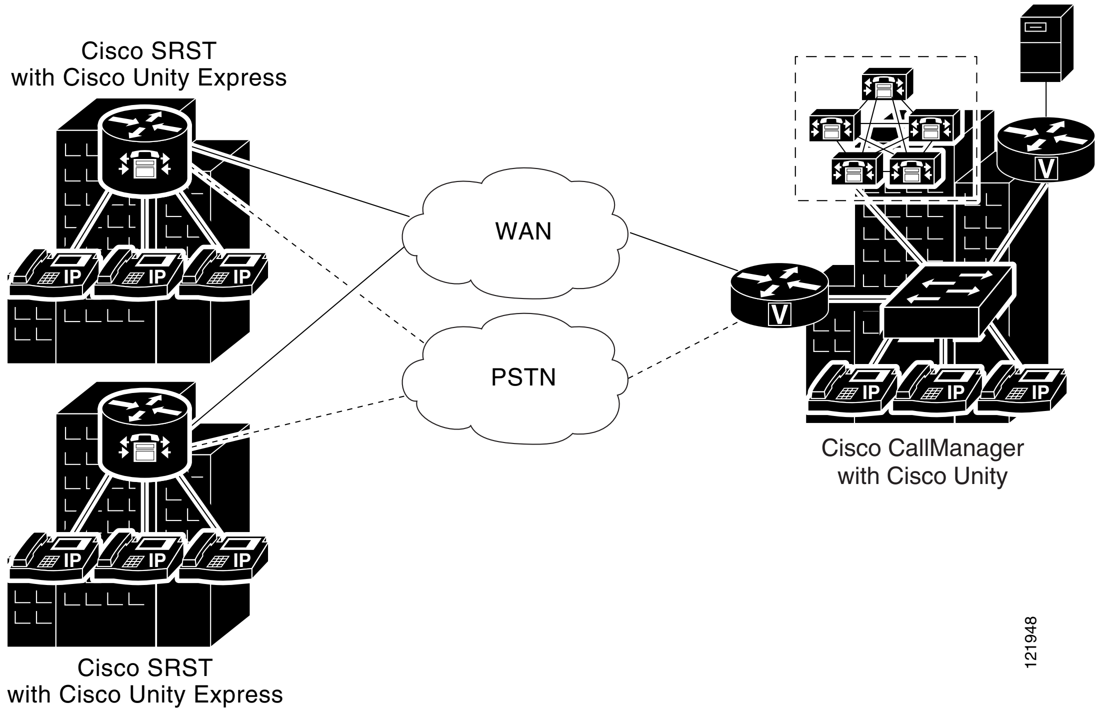
In this deployment model, there are multiple sites of the same business or enterprise networked together. The networking may be very loose (very little inter-site business is conducted, such as restaurants of the same chain) or fairly tight (a branch office of a larger enterprise where there is significant business traffic between sites).

The sites in the network may be of two forms:

- All Cisco CME sites (a distributed call-control model) with a Cisco Unity Express providing local AA and voice-mail service at each site (shown in Figure 2).
- The IP phones and PSTN calls at all sites in the network are controlled by a centralized Cisco CallManager while Cisco Unity Express in the router (with Cisco SRST configured) at each remote site provides distributed voice mail (shown in Figure 3).

Figure 2 Multisite Network with Cisco CME

Figure 3 Multisite Network with Cisco CallManager



The network may also be a hybrid of the two preceding deployment models and contain a mix of sites of any of the types summarized in Table 2.

Table 2 Site Configurations in a Multisite Network

	Call Control	
Voice Mail	**Centralized**	**Distributed**
Centralized	Cisco CallManager and Cisco Unity	Cisco CME and Cisco Unity
Distributed	Cisco CallManager and Cisco Unity Express	Cisco CME and Cisco Unity Express

The decision points in choosing between distributed and centralized call control are very often the same as those that govern choosing between distributed and centralized voice mail. These include the following:

- Management philosophy of your company
  - Who makes decisions on the technology used at which sites?
  - Is this a centralized IT decision or, are these more often left up to the sites themselves in a “remote ownership” or “franchise” model?
- Redundancy and availability considerations determine whether a distributed solution is the right fit when AA and voice-mail access must be available during WAN failures.
- WAN bandwidth availability and WAN QoS provisioning— A centralized voice mail model requires that all calls into voice mail traverse the WAN. This requirement might not be optimal for your application or your WAN architecture might not yet be ready for this traffic.

Sites Networked with PSTN

The first type of multisite deployment is where the coupling between the sites is either loose (based on your business model), or the WAN is not QoS-enabled and therefore not capable of carrying VoIP traffic. It might not be in your best interest to upgrade the WAN at this time. For sites fitting this model, the WAN between the sites is used purely for low-bandwidth data access. Any voice calling between sites is via the PSTN.

This type of network has the following characteristics:

- All offnet voice connectivity is via the PSTN to customers or clients of the business.
- Onnet voice between sites are made between IP phones connected to the Cisco CME or Cisco CallManager system resident at the site and the PSTN. All other sites are reached via PSTN dialing.
- WAN connectivity between sites is used purely for data traffic.

Each site in this deployment model operates essentially as a standalone site. Small sites will tend to be Cisco CME and Cisco Unity Express (cost-effective at the low end) while large sites are likely to be Cisco CallManager and Cisco Unity (high-end solutions).

A variation of this deployment occurs when the WAN is QoS-enabled but has limited bandwidth for VoIP traffic. Perhaps inter-site onnet calls can be carried via VoIP, but AA and voice-mail calls cannot. This is another situation where a distributed AA and voice-mail solution is a a good fit.

Sites Networked with H.323 VoIP

A second type of multisite deployment features a tighter coupling between sites and a VoIP-capable WAN between sites. For sites fitting this model, the WAN between the sites is used for both voice and data access, and the PSTN is used only for off-net calls.

This type of office has the following characteristics:

- All offnet voice connectivity is via the PSTN to customers or clients.
- Onnet voice between sites are made between IP phones connected to the Cisco CME or Cisco CallManager system resident at the site via VoIP to all other sites in the enterprise.
- The WAN connectivity between sites is used for voice and data traffic.

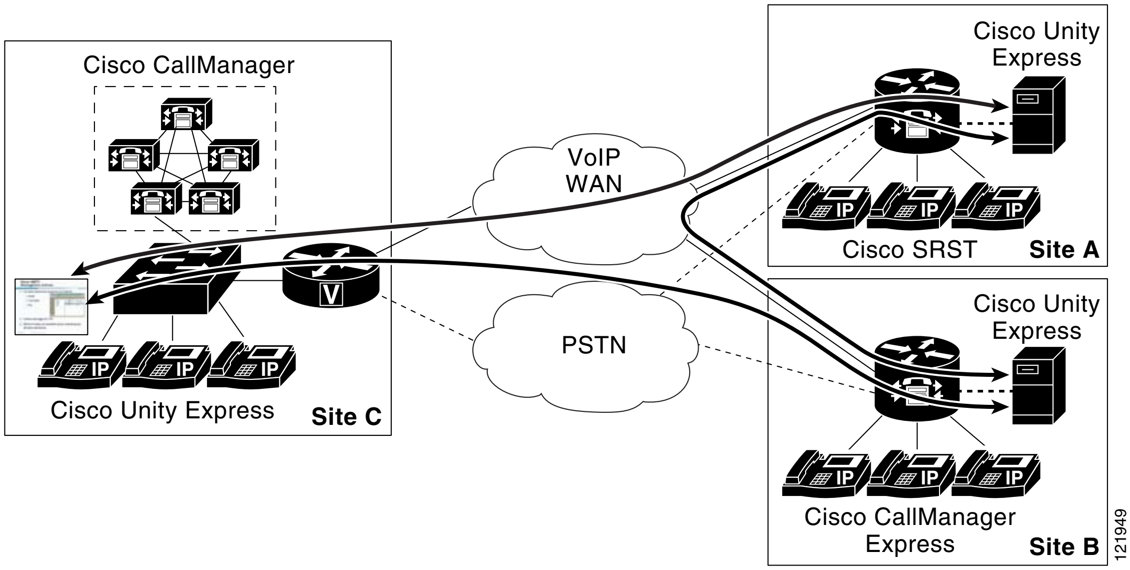
When networking together, mixed Cisco CME and Cisco CallManager sites with VoIP, deploy Cisco CME 3.1 (or later releases) and ensure the H.450 and other internetworking dependencies between these call controllers are addressed in your network.

Cisco Unity Express Voice Mail Networking

Cisco Unity Express 2.0 and later releases support voice-mail networking via Voice Profile for Internet Mail (VPIM) Version 2. While this protocol is widely supported by voice mail systems in general, Cisco Unity Express supports networking only with other sites running Cisco Unity Express and Cisco Unity Release 4.03 or later releases.

As in the previous sections, a network can be deployed with various configurations for each site, including Cisco CME with Cisco Unity Express, Cisco CallManager with Cisco Unity Express and Cisco CallManager with Cisco Unity. In such a network, all the Cisco Unity Express and Cisco Unity sites can be networked together via VPIM, as shown in Figure 4.

Figure 4 Cisco Unity Express Voice Mail Networking



Unsupported Deployments

The following deployment scenarios are not supported (up to Cisco CME 3.2 and Cisco Unity Express 2.1):

- Sites networked with SIP as the VoIP protocol. While Cisco CME by itself supports SIP trunking, these deployments are not yet supported if Cisco Unity Express is used in conjunction with Cisco CME. Only H.323 VoIP trunking is supported.
- For implementations prior to Cisco CME 3.2 and Cisco Unity Express 2.0, these two components must be collocated in the same router chassis. As of Cisco CME 3.2 and Cisco Unity Express 2.0, this is no longer a requirement. While you should have LAN connectivity between Cisco CME and Cisco Unity Express (and not low-speed WAN links), these two components may now reside in physically different routers.
- Cisco SRST, Cisco Unity Express and the PSTN gateway at the site must be collocated in the same router chassis up to and including Cisco SRST Release 3.1. As of Cisco SRST Release 3.2, the PSTN gateway portion can be separated out onto a different router.
- Multiple Cisco Unity Express systems in the same router chassis.
- A “centralized” Cisco Unity Express model where a single Cisco Unity Express system provides voice mail to IP phones at more than one Cisco CME or Cisco SRST site.
- SIP phones as Cisco Unity Express voice mail subscribers—only SCCP IP phones are supported.
- Analog phones as Cisco Unity Express voice mail subscribers. Analog phones (FXS ports) can connect to Cisco Unity Express as “outside” callers into the AA and voice-mail systems, but cannot receive subscriber features such as call-forward busy (CFB), call-forward no answer (CFNA), or message waiting indicator (MWI.)

Chapter 2: Network Infrastructure Considerations for Cisco Unity Express

Cisco Unity Express is an IP application that physically integrates into a router chassis and that takes advantage of the infrastructure provided by the host router and the associated IP network connected to the router.

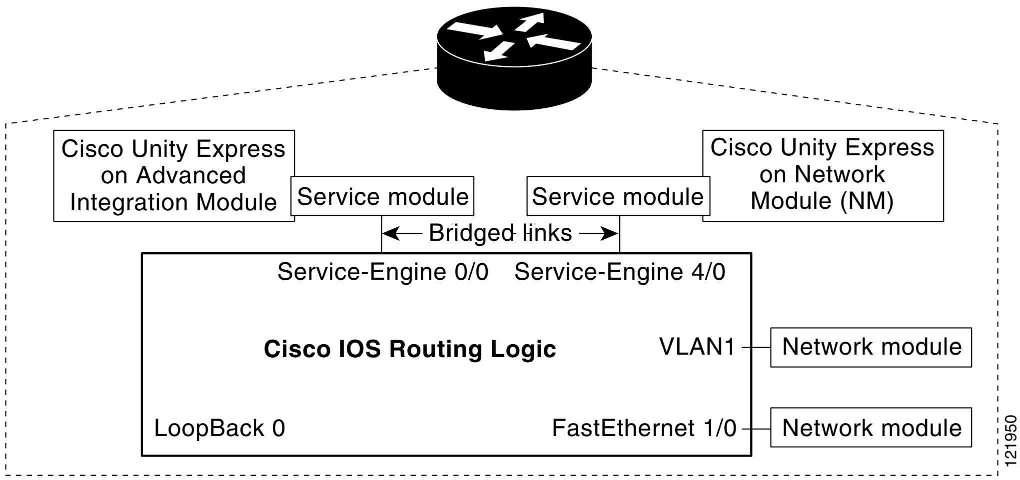
The specific sections in this chapter address the following aspects of your IP network that can affect Cisco Unity Express implementations:

IP Connectivity

The Cisco Unity Express module connects to its host router via a back-to-back Ethernet configuration that physically travels across the backplane of the router. The Cisco Unity Express module has an internal IP address and a default gateway configuration. The service-engine interface on the router has its own IP address which may be configured as unnumbered. The following sections illustrate the IP connectivity configuration options for the Cisco Unity Express module.

Topics addressed in this section include the following:

Figure 5 IP Connectivity Configuration



IP Unnumbered

The most common way to configure the Cisco Unity Express module is to use the unnumbered IP address method. An **ip unnumbered** command configuration, shown in the following configuration fragment, allows the Cisco Unity Express module to consume an IP address in the subnet of the network associated with a particular router egress port, such as FastEthernet 0/0. The router interface with which the Cisco Unity Express interface is associated must be in an "up" state at all times for Cisco Unity Express to communicate.

Note This method requires the configuration of a static route to the service-engine interface.

IP unnumbered configuration example:

```
interface FastEthernet0/0
 ip address b.68.10.1 255.255.255.0
!
interface Service-Engine4/0
 ip unnumbered FastEthernet0/0
 service-module ip address b.68.10.10 255.255.255.0
 service-module ip default-gateway b.68.10.1
!
ip route b.68.10.10 255.255.255.255 Service-Engine4/0
```

The IP address of the Cisco Unity Express module in the example is b.68.10.10. The default-gateway on the Service Engine must be set to the IP address of the Ethernet interface on the router that the unnumbered statement refers to (b.68.10.1 in the example). If this is a Cisco CME deployment, then this default-gateway setting must be the Cisco CME router.

It is also possible to use a subinterface or a loopback interface as the **ip unnumbered** command parameter (such as **`ip unnumbered fastethernet0.1`**).

Stub Network

Stub network configuration requires Cisco Unity Express to have its own IP subnet assigned, but does not require a static route. Using a stub network is one recommended approach for configuring Cisco Unit Express when using a private address space. When implementing a stub network configuration, the IP address must be routable, so that the TFTP/FTP server used for software installation or backup-and-restore knows how to reach the Cisco Unity Express module. This is shown in the following configuration example:

Stub network configuration example:

```
router# show running-config
interface FastEthernet0/0
 ip address b.68.10.1 255.255.255.0
!
interface Service-Engine4/0
 ip address b.68.20.1 255.255.255.0
 service-module ip address b.68.20.10 255.255.255.0
 service-module ip default-gateway b.68.20.1
```

VLAN

This configuration illustrates a situation in which an Etherswitch module is present in the router for which a VLAN interface is most commonly used. A VLAN-specific configuration is shown in the following configuration fragment and is very similar to the **ip unnumbered** configuration given in the "IP Unnumbered" section on page 8. A VLAN implementation also requires a static route.

VLAN configuration example:

```
interface VLAN1
 ip address b.68.10.1 255.255.255.0
!
interface Service-Engine4/0
 ip unnumbered VLAN1
 service-module ip address b.68.10.10 255.255.255.0
 service-module ip default-gateway b.68.10.1
!
ip route b.68.10.10 255.255.255.255 Service-Engine4/0
```

Private and Public Addressing

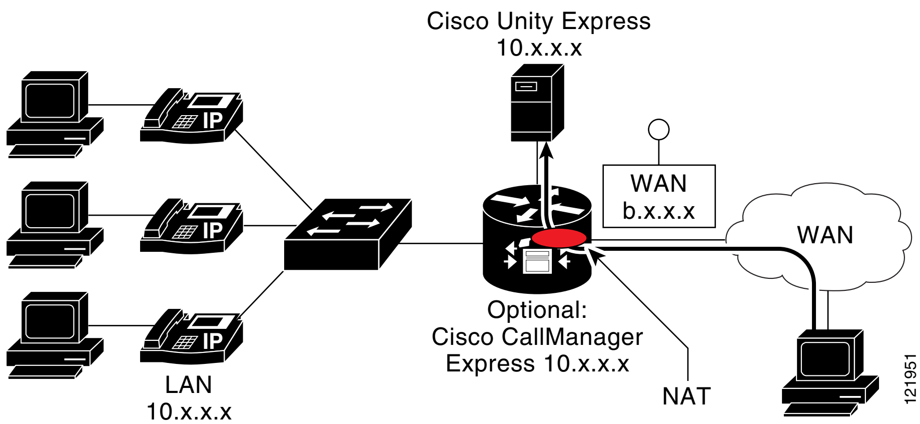
If you decide to configure an actual IP address for Cisco Unity Express (as opposed to using unnumbered), the next decision is to determine the type of IP address that should be assigned. The IP address can be public or private.

Topics addressed in this section include the following:

Private Addressing

In many voice networks, the voice devices have private addresses (indicated by 10.x.x.x), while the WAN link may have a public address (indicated by b.x.x.x). You can assign private addresses to both Cisco CME (if present in the deployment) and Cisco Unity Express in order to fit in a large network and also for voice security reasons. This design is shown in Figure 6.

Figure 6 Cisco Unity Express with a Private Address

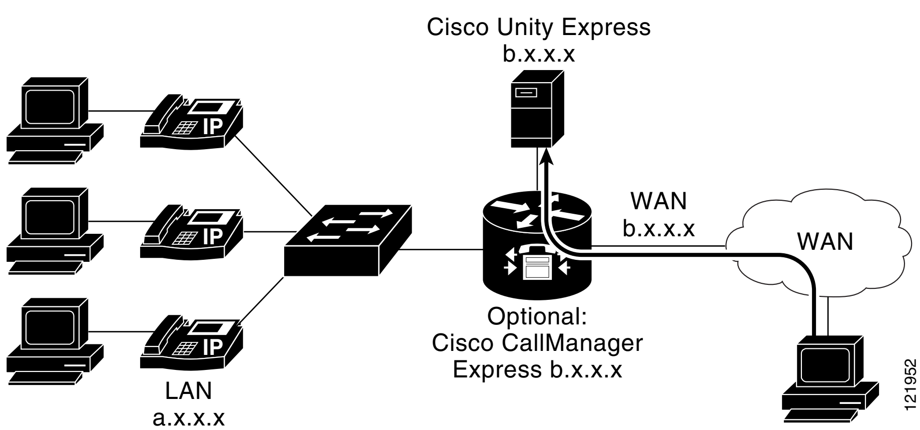


If you choose this design, then remote management access via HTTP—for the Cisco Unity Express or Cisco CME graphical user interface (GUI)—must pass through Network Address Translation (NAT) to be able to reach the Cisco Unity Express module. The GUI uses both the Cisco IOS HTTP server as well as an HTTP server on the Cisco Unity Express module.

Public Addressing

In this configuration, Cisco Unity Express has a public addresses (indicated by b.x.x.x). If Cisco CME is present, it too has a public address that is assigned to it. This makes sense in networks where voice devices in general have public addresses, or where remote management access to Cisco Unity Express or Cisco CME must work without requiring NAT. This design is shown in Figure 7.

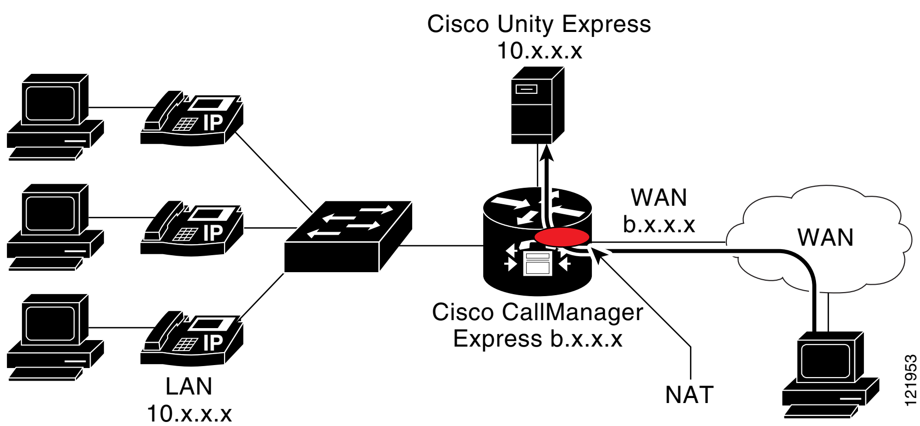
Figure 7 Cisco Unity Express with a Public Address



Cisco Unity Express with Private Addressing and Cisco CME with Public Addressing

In a Cisco CME deployment, it is possible to configure Cisco Unity Express with a private address (indicated by 10.x.x.x), like the phones and other telephony devices, while Cisco CME has a public address (indicated by b.x.x.x) assigned. This is a common scenario in a cable- or DSL-attached branch office location where a single public address is allocated to the site. All outbound H.323 traffic would use the Cisco CME public address for voice traffic while the IP Phones and Cisco Unity Express addresses remain "hidden" from the network. This design is shown in Figure 8.

Figure 8 Cisco Unity Express with Private Addressing and Cisco CME with Public Addressing



The side effect of the configuration is that while Cisco CME is remotely accessible (HTTP for GUI), the Cisco Unity Express GUI—which is integrated with the Cisco CME GUI—still requires NAT to work with the configuration, as described in "Private Addressing" section on page 10.

NAT

Network Address Translation (NAT) affects Cisco Unity Express implementation. These considerations are discussed in the following sections.

GUI Access

If NAT is required for remote GUI (HTTP) access, use the following configuration process:

Step 1 Assign a private address to the Cisco Unity Express interface.

Step 2 Create a static source NAT IP translation.

Step 3 Make the service-engine interface the inside interface.

Step 4 Make the FastEthernet interface the outside interface.

A NAT configuration is shown in the following:

```
router# show running-config
interface FastEthernet0/0
```

```
 ip address b.19.153.38 255.255.255.0
 ip nat outside
!
interface Service-Engine2/0
  ip address 10.10.10.1 255.255.255.0
  ip nat inside
  service-module ip address 10.10.10.2 255.255.255.0
  service-module ip default-gateway 10.10.10.1
!
ip nat inside source static tcp 10.10.10.2 80 b.19.153.38 80
```

This configuration allows access to the Cisco Unity Express GUI (at http://b.19.153.38/, not 10.10.10.2), as well as Telnet access to the router.

Note If this is a Cisco CME deployment, access to the integrated Cisco Unity Express and Cisco CME GUI works correctly, but access to the Cisco CME-specific GUI (http://b.19.153.38/telephony-service.html) does not work as port 80 is being accessed via NAT. To restore operation to the Cisco CME-specific GUI (if access to this is required in the deployment), the HTTP port for Cisco CME must be changed to something other than 80. Use the **ip http port** *port* configuration command.

This ensures that the Cisco CME HTTP server uses a different port. To access the Cisco CME GUI, use a port-specific URL, such as http://b.19.153.38:<port>/telephony_service.html. Any other HTTP access to the servers on the private LAN also requires configuration to use a port other than 80.

A static NAT statement for port 21 might also be needed to enable remote FTP software installation or upgrade for Cisco Unity Express.

Java Telephony Application Programming Interface

Java Telephony Application Programming Interface (JTAPI) communications does not currently work via NAT or firewall, so you cannot configue Cisco Unity Express on the other side of NAT from a Cisco CallManager controlling calls via JTAPI.

Voice Mail Networking

Cisco Unity Express voice mail networking (VPIM) configurations with NAT will be addressed in subsequent releases of this document.

Network Infrastructure Configuration Trade-Offs for Cisco Unity Express

The previous sections covered different types of configurations. Some trade-offs to consider when deciding between these options include the following:

- Address availability—If spare subnets are available, the best way to configure the Cisco Unity Express module is to put it on its stub network. If IP addressing is tight, the unnumbered approach is best, and you can use a loopback interface if one is available.
- Reliable reachability of Cisco Unity Express AA and voice mail—A key consideration is to ensure that the Cisco Unity Express module is always reachable. If an interface fails and the Cisco Unity Express module is using the failed module as its unnumbered interface, then AA and voice mail applications are not reachable. If the unnumbered approach is used for IP addressing, use a loopback interface and not a physical interface.

- Remote management—For a Cisco CME deployment, GUI access uses an HTTP server in Cisco IOS as well as an HTTP server on the Cisco Unity Express module. For the GUI to work, HTTP traffic to both Cisco CME and Cisco Unity Express must be routable. If Cisco Unity Express is given a private network address, use NAT to route HTTP traffic to the private address. CLI access is not affected by the IP addressing (private, public or unnumbered) scheme used by Cisco Unity Express, as CLI access always uses Telnet to the router, but not to the Cisco Unity Express IP address.
- Security—Reachability of network addresses may be a concern in some networks, and for this reason you may decide to use a private address for Cisco Unity Express. One view is that Cisco Unity Express is a host device (server) on the network that just happens to be integrated in the router chassis; therefore, it should have a routable and reachable address from your internal network. An opposite view is that the casual user on your internal network should not be able to reach the Cisco Unity Express IP address in any direct manner (such as ping) for security reasons; therefore, Cisco Unity Express should be a “hidden” device with a private address, and traffic specifically destined to Cisco Unity Express (like the GUI HTTP) should go through NAT.

Best Practises

The preceding sections describe the different options and tradeoffs for configuring the IP addresses for Cisco Unity Express. In general, the recommended way to configure Cisco Unity Express IP addressing is shown in the following configuration example, which shows an IP unnumbered interface referencing a loopback interface to guard against LAN and WAN interface failures affecting the availability of Cisco Unity Express.

```
interface Loopback0
 ip address a.32.152.9 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip bind srcaddr a.32.152.9
!
interface Loopback2
 ip address a.32.152.241 255.255.255.252
 ip ospf network point-to-point
!
interface Service-Engine4/0
 ip unnumbered Loopback2
 service-module ip address a.32.152.242 255.255.255.252
 service-module ip default-gateway a.32.152.241
!
ip route a.32.152.242 255.255.255.255 Service-Engine4/0

GigabitEthernet3/0       unassigned      YES unset  administratively down down
Service-Engine4/0        a.32.152.241   YES TFTP   up                    up
Loopback2                a.32.152.241   YES NVRAM  up                    up
```

Note Enable IP routing on the router for packets to be forwarded to the Cisco Unity Express application.

Date and Time

Date and time for Cisco Unity Express are controlled via two configurations of the system:

- Timezone and geographic area configuration
- Network Time Protocol (NTP) source

Topics addressed in this section include the following considerations:

- Operation, page 14
- Best Practices, page 14

Operation

While the Cisco Unity Express module has its own onboard clock, you cannot set the clock via the GUI or the CLI. The clock is controlled entirely via NTP, which is in Coordinated Universal Time (UTC), and the timezone setting (the offset from UTC to local time). The clock is synchronized with the NTP source during Cisco Unity Express software startup. While Cisco Unity Express is running, small clock drifts are corrected, but no large (greater than 1 second) clock changes take place until the software is rebooted.

Note On a Cisco CME system with Cisco Unity Express, the GUI clock-set capability in the **Configure** > **System Parameters** > **System Time** GUI window displays and controls the Cisco CME (router) clock, not the Cisco Unity Express module clock. Setting the router's clock has no effect on Cisco Unity Express, unless the router is also defined as the NTP server for Cisco Unity Express (not a recommended configuration).

The following is an example Cisco Unity Express module configuration that is required to set the NTP source for the clock:

ntp server b.19.153.31

When you initially insert the Cisco Unity Express module into a router and apply power, the software (installed by the factory), has already started up by the time the IP addressing and other basic configuration is done. After the NTP configuration is completed on both the router and the Cisco Unity Express module, you must restart the application to synchronize the clocks.

Cisco Unity Express 2.0 and later releases contain an NTP auto-sync feature that automatically resets the Cisco Unity Express clock if a discrepancy of more than 0.5 second is detected. In older Cisco Unity Express releases, resetting the clock for discrepancies of larger than 1 second required a software reboot.

Best Practices

The following practices are recommend for optimal date and time control:

- Use a robust NTP server in your network for maximum clock stability.
- Use the Cisco Unity Express host router (or any other low-end router) as the NTP server only as a last resort. A host router can easily incur clock drift and does not contain batteries to maintain clock settings over a power cycle.
- Use multiple NTP servers to enhance the reliability of clock synchronization and server availability. Up to three NTP servers can be configured for Cisco Unity Express. The NTP protocol's algorithm determines which NTP server is the most stable and draws its clock from that server.

TFTP and FTP Servers

The Cisco Unity Express bootloader uses TFTP to load the RAM-based Linux kernel (cue_installer) from a network location as the first step of a software installation or upgrade. This is the only use of TFTP in the Cisco Unity Express system. FTP is used for the remainder of the software installation and upgrade, as well as for backup and restore communication.

Topics addressed in this section include the following:

FTP Server Location and Access

Setup the FTP server so that all Cisco Unity Express sites using it have reliable, high-speed, and secure access to the FTP server. The following are considerations to take into account:

- Backup and restore bandwidth required—The size of the backup depends on the Cisco Unity Express license (number of mailboxes) and storage capacity of each site. If only the Cisco Unity Express system's configuration is backed up, very little bandwidth is needed. If the system's voice mail message content is also backed up, then much higher bandwidth is needed.
- Security of the FTP connection—A Cisco Unity Express backup or restore operation transmits the voice message content over the FTP connection. If ensuring the privacy of this information is important, use IPSec technology between the Cisco Unity Express site and the FTP server.
- Security of information on the FTP server—A Cisco Unity Express backup is stored unencrypted in files on the FTP server. Ensure that access to the FTP server's accounts and disk drives are secured from tampering and unintended access. Choose strong passwords for FTP server account access.
- Cisco Unity Express system access to the FTP server—Ensure that Cisco Unity Express can access the FTP server by either name or IP address. If the FTP server is accessed by name, then ensure that Cisco Unity Express is DNS enabled. Any firewall between the FTP server and Cisco Unity Express must allow FTP traffic to go through.

FTP Packages

This section does not provide any Cisco endorsement or recommendation of FTP packages. It simply lists some FTP packages that have been tested with Cisco Unity Express.

- Linux
  - ProFTPD 1.2.8 Server
  - PureFTPd
  - WU-FTPD
- Windows
  - FileZilla FTP Server 0.8.8
  - GuildFTPd
  - Serv-U
  - Microsoft IIS FTP

Note An FTP package that is known to be incompatible with Cisco Unity Express is the TYPSoft FTP server. When a file does not exist on the FTP server, the TYPSoft FTP server returns 501 (Syntax error in parameters or arguments) instead of 550 (Requested action not taken. File unavailable).

FTP Server Configuration Guidelines

There are numerous FTP servers and they all have different configurations. This section provides only general guidelines for the types of features and characteristics your FTP server should have to work with Cisco Unity Express:

- The FTP server must support PASV mode (PASSIVE FTP). Ensure that PASV mode is enabled on the FTP server (if there is an option for this).
- Don't use anonymous FTP for Cisco Unity Express Backup and Restore.
- Use the default port (Port 21) for the FTP server.
- When creating user accounts, ensure that each user account is assigned a different home directory.
- Give full permissions to the user over the home directory. Ensure that the user account can upload and download files. Also ensure that the user can create, modify, delete, and rename files and directories from the home directory.
- Ensure that there is enough disk space on the FTP server. Regularly monitor the disk space on the FTP server.
- If a particular directory is configured as the backup directory for Cisco Unity Express, do not manually delete any files or directories from the directory that is configured on Cisco Unity Express. The Backup and Restore service on Cisco Unity Express manages the contents of the directory, cross-references files from different subdirectories, and indexes files into the log files. For example, if Cisco Unity Express is using ftp://server.com/backupdir as the configured backup URL, and "bkpuser" as the user account, then the backup files go into the directory "~bkpuser/backupdir". Cisco Unity Express automatically creates this directory. Do not delete any files/directories under the "backupdir" directory.
- If a single FTP server is used to store backups from multiple Cisco Unity Express sites, ensure that the directory for each site is different. For example, if there are five sites, configure the backup URL for the sites as ftp://server.com/backupdir/site1, ftp://server.com/backupdir/site2 etc.

TTY Port Numbers

The TTY port numbers for the Cisco Unity Express module varies based on the router platform model and router slot where the Cisco Unity Express hardware is inserted. Generally this TTY number is not needed, except to do the following

- Enter a password on the TTY line for security reasons (to prohibit unauthorized telnet access to Cisco Unity Express).
- Clear the line in the event the previous session was disconnected without clearing the line properly.
- Force a security session inactivity disconnect for Cisco Unity Express CLI session.

The TTY port number formulas for different router platforms and Cisco Unity Express hardware is given in Table 3.

Table 3 Cisco Unity Express TTY Formulas

Router Platform	NM-CUE	AIM-CUE
Cisco 2600XM and Cisco 3700	2000 + ((NM-slot-num * 32) + 1)	2000 + ((number-of-NM-slots in router + 1) * 32) + AIM-slot-num + 1
Cisco 2811, Cisco 2821, Cisco 2851	2 + (NM-slot-num * 64)	2 + ((number-of-NM-slots-in-router + 2 + AIM-slot-num) * 64)
Cisco 3800	2 + (NM-slot-num * 64)	2 + ((number-of-NM-slots-in-router + 1 + AIM-slot-num) * 64)

The Cisco 2600XM series routers have one AIM slot (0/0) while the Cisco 2691, Cisco 2800 series, Cisco 3700 series and Cisco 3800 series all have two AIM slots (0/0 and 0/1).

The TTY ports for Cisco Unity Express NMs are given in Table 4, while AIM numbering is given in Table 5.

Table 4 NM-CUE TTY Port Numbers

Platform	NM-CUE Slot	TTY Port Number
Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745	1/0	2033
Cisco 3725, Cisco 3745	2/0	2065
Cisco 3745	3/0	2097
Cisco 3745	4/0	2129
Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, Cisco 3845	1/0	66
Cisco 3825, Cisco 3845	2/0	130
Cisco 3845	3/0	194
Cisco 3845	4/0	258

Table 5 AIM-CUE TTY Port Numbers

Platform	Number of NM Slots	AIM-CUE Slot	TTY Port Number
Cisco 2600XM, Cisco 2691	1	0/0	2065
Cisco 2691	1	0/1	2066
Cisco 3725	2	0/0	2097
Cisco 3725	2	0/1	2098
Cisco 3745	4	0/0	2161
Cisco 3745	4	0/1	2162

Table 5 AIM-CUE TTY Port Numbers

Platform	Number of NM Slots	AIM-CUE Slot	TTY Port Number
Cisco 2801	0	0/0	66
Cisco 2801	0	0/1	130
Cisco 2811, Cisco 2821, Cisco 2851	1	0/0	194
Cisco 2811, Cisco 2821, Cisco 2851	1	0/1	258
Cisco 3825	2	0/0	194
Cisco 3825	2	0/1	258
Cisco 3845	4	0/0	322
Cisco 3845	4	0/1	386

Security

The following topics summarize network security strategies that aid in preventing unauthorized access to Cisco Unity Express:

- System and Remote Access, page 18
- Application Environment, page 21
- User Interfaces and Login Types, page 25
- Security Best Practices, page 29

System and Remote Access

There are no external interfaces on the Cisco Unity Express hardware (physically there is an FE interface port, but it is disabled in software and unusable). All access must pass through the host router and across the backplane to the NM-CUE or AIM-CUE.

Local Access

The only local access to a Cisco Unity Express system is via the host router's console interface into the router CLI and then opening a "session" to the Cisco Unity Express CLI by using the following command:

service-module service-Engine x/y session

Entering this command requires you to be in enable mode on the router which is protected by the router's enable login and password settings. Although there is also an enable mode in the Cisco Unity Express module CLI, Cisco Unity Express has no password capability. Any network administrator with access to enable mode on the router, also can access the Cisco Unity Express CLI. There is no user ID or password control on the Cisco Unity Express CLI. Access is controlled via the router, and if logging is required, set up the router with AAA/RADIUS monitoring of login access.

GUI access via a browser to Cisco Unity Express is always considered remote access as it is across an IP segment from the router.

Remote Access via Telnet

The following IP configuration is used as the baseline configuration in this section:

```
interface FastEthernet0/0
 ip address b.19.153.41 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface Service-Engine1/0
 ip unnumbered FastEthernet0/0
 service-module ip address b.19.153.37 255.255.255.0
 service-module ip default-gateway b.19.153.41
```

Direct telnet access to the Cisco Unity Express IP address is disabled by default as shown in the following example:

```
pc> telnet b.19.153.37
Trying b.19.153.37...
telnet: Unable to connect to remote host: Connection refused
```

Remote CLI access to Cisco Unity Express is therefore only possible via telnet to the router (b.19.153.41) and then by the using the session command to get access to the Cisco Unity Express CLI. That way, all the security protections that are built into telnet access to your router automatically also protect access to Cisco Unity Express. A Telnet session to the router, followed by a session into Cisco Unity Express is shown in the following example:

```
pc> telnet b.19.153.41
Trying b.19.153.41...
Connected to b.19.153.41.
Escape character is '^]'.

User Access Verification

Password:
lab-2691>enable
Password:
lab-2691#service-module service-Engine 1/0 session
Trying b.19.153.41, 2033 ... Open
```

Telnet to the router address, followed by the explicit TTY port number that is allocated to Cisco Unity Express (which depends on the slot where it is inserted as per Table 4 and Table 5) is not blocked and can provide undesirable "direct" access to Cisco Unity Express as shown in the following example:

```
pc> telnet b.19.153.41 2033
Trying b.19.153.41...
Connected to b.19.153.41.
Escape character is '^]'.

User Access Verification

Password:
Password OK
```

To protect against this kind of access, insert a login and password configuration on the TTY port. In this example, the Cisco Unity Express module is in slot 1/0 on a Cisco 2691 and has a TTY port of 2033 leading to Cisco Unity Express as shown in the following configuration example:

Configuration example for login/password on telnet access:

```
line 33
 password cisco
 flush-at-activation
 no activation-character
 login
 no exec
 transport preferred none
 transport input all
```

Access Timeout

Cisco Unity Express CLI access via the TTY port in the router (as described in the "Local Access" section on page 18 and the "Remote Access via Telnet" section on page 19) does not time out by default. The connection stays up until it is disconnected by the user who initiated it. If an inactivity timeout on access to Cisco Unity Express CLI is required, use the the **session-timeout** command on the router TTY configuration to disconnect the session after a configured number of minutes. The following example configuration of an inactivity timeout on Cisco Unity Express CLI access.

```
line 33
 session-timeout 5
 password 7 02050D480809
 login
```

Remote Access via SSH

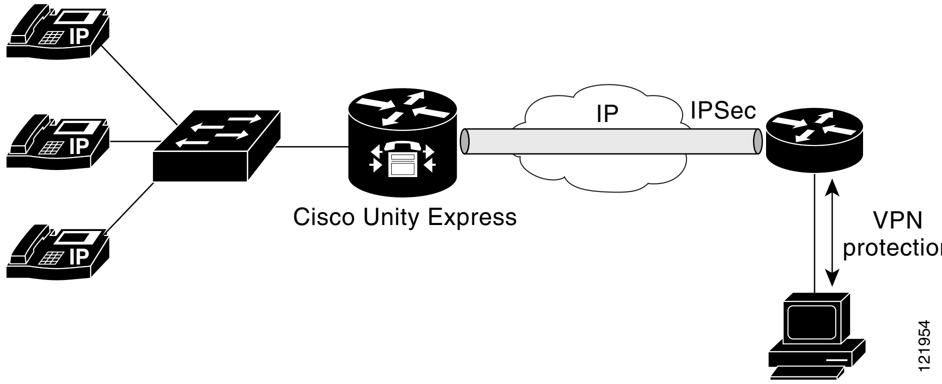
For secure CLI access to Cisco Unity Express, enable secure shell (SSH) on the router and use an SSH-enabled remote access application, such as the Secure Shell windows application.
Cisco Unity Express itself does not support SSH (but neither does it support telnet access), but communication between the router and Cisco Unity Express is via the router backplane.
Cisco Unity Express is not exposed to any external interfaces or IP segments. SSH access to the router is sufficient to protect telnet access to Cisco Unity Express.

Remote Access via HTTPS

Cisco Unity Express does not support HTTPS for browser access. This capability is on the roadmap of security features to be added. While login to the GUI is password protected, the login ID and password currently travel in clear text across the IP network.

You can protect GUI access in Cisco Unity Express by using IPSec tunnels on the routers between the nearest router to where the browser is located and the router hosting the Cisco Unity Express module. You can use VPN technology to protect the segment between the client PC and the nearest router where IPSec is available, as shown in Figure 9. As an alternative, you can use VPN technology all the way from the client PC to the host router.

Figure 9 Secure HTTP Access



HTTPS is supported on Cisco CME, and requires at least the Cisco IOS 12.3.4T Advanced IP Services IOS image. HTTP access for Cisco Unity Express and the IP Phones (which do not support HTPPS/SSL) continue to use port 80, while the Cisco CME GUI access uses HTTPS on port 443. For this to work, include the following commands on the router:

ip http server

ip http secure-server

Application Environment

Cisco Unity Express is an IP application and therefore communicates with its environment via various TCP and UDP protocols and ports.

Protocols and Port Numbers

The protocols and port numbers used by Cisco Unity Express are listed in Table 6.

Table 6 Cisco Unity Express Protocols and Port Numbers

Protocol	Remote Source Port	Cisco Unity Express Destination Port	Cisco Unity Express Source Port	Remote Device Destination Port	Remote Device	Notes
SSH					Secure Shell Client	Not supported on Cisco Unity Express. Use SSH to the host router.
Telnet					Telnet Client	Not supported on Cisco Unity Express. Use telnet to the host router.
DNS			TCP/UDP 53		DNS Servers	

Table 6 Cisco Unity Express Protocols and Port Numbers

Protocol	Remote Source Port	Cisco Unity Express Destination Port	Cisco Unity Express Source Port	Remote Device Destination Port	Remote Device	Notes
TFTP			UDP 69		TFTP Server	Used for loading RAM kernel.
FTP			TCP 20 (data), TCP 21 (control)		FTP Server	Used for software install; backup and restore.
HTTP		TCP 80			Administrator / User Web browsers	Cisco Unity Express and Cisco CME Admin and User browser access.
NTP		UDP 123			NTP server	Date/Time server.
SNMP					Network Management station	SNMP hardware inventory for Cisco Unity Express is supported out of the host router. Cisco Unity Express itself does not support SNMP.
Syslog		TCP 514			Syslog service	
SIP		UDP 5060			Cisco CME or SRST Host router	No SIP trunking is supported.
RTP	UDP 16384-32767	UDP 16384-32767	UDP 16384-32767	UDP 16384-32767	Voice Media	IP Phone and gateway ports.
JTAPI				TCP 2748	Cisco CallManager	Used for call control in Cisco CallManager deployments.
SMTP		TCP 25	TCP 25		Cisco Unity Express or Cisco Unity	Voice mail networking between sites.

Suggested Access Control Lists

The following IP configuration example applies to the description provided in this section:

Note As you customize the access control lists (ACLs) for your environment, substitute your network's configuration information into the appropriate places in the ACLs presented in this section.

```
service-module ip default-gateway b.19.153.41
Address of Cisco UE service module: b.19.153.37
FTP Server for software backup and download: a.10.1.150
Admin Subnet: a.10.1.0/24
IP Phone/GW Subnet: a.10.2.0/24
Syslog Server: a.10.1.160
```

```
DNS: a.10.1.170
Call manager server 1: b.84.23.10
Call manager server 2: b.84.23.11
```

The ACL in the following configuration examples are recommended to be used with Cisco Unity Express. The ACLs specific to Cisco CallManager should be included only if Cisco Unity Express is deployed with a Cisco CallManager. The following ACLs should be applied on the Cisco Unity Express service-engine interface on the router, as shown in Cisco Unity Express service-engine examples that follow.

Recommended inbound ACLs:

```
access-list 101 remark Filter Outbound Traffic from CUE - Apply Inbound on Interface
ServiceEngine
access-list 101 remark Restrict DNS to only a.10.1.170, add additional dns servers as
required
access-list 101 permit udp host b.19.153.37 host a.10.1.170 eq domain
access-list 101 permit tcp host b.19.153.37 host a.10.1.170 eq domain

access-list 101 remark Restrict TFTP to only the host router
access-list 101 permit udp host b.19.153.37 host b.19.153.41 eq tftp

access-list 101 remark Restrict FTP traffic to only a single server
access-list 101 permit tcp host b.19.153.37 host a.10.1.150 eq ftp
access-list 101 permit tcp host b.19.153.37 host a.10.1.150 eq ftp-data

access-list 101 remark Restrict NTP traffic to only the host router
access-list 101 permit udp host b.19.153.37 host b.19.153.41 eq ntp

access-list 101 remark Restrict Syslog traffic to single server
access-list 101 permit tcp host b.19.153.37 host a.10.1.160 eq syslog

access-list 101 remark Restrict SIP signaling to host router
access-list 101 permit tcp host b.19.153.37 host b.19.153.41 eq 5060
access-list 101 permit udp host b.19.153.37 host b.19.153.41 eq 5060

access-list 101 remark Restrict RTP to IP phone and GW segment plus router
access-list 101 permit udp host b.19.153.37 a.10.1.0 0.0.0.255 range 16384 32767
access-list 101 permit udp host b.19.153.37 host b.19.153.41 range 16384 32767

access-list 101 remark Restrict SMTP communication to host router
access-list 101 permit tcp host b.19.153.37 any eq smtp

access-list 101 remark Restrict CCM communication to host router
access-list 101 permit tcp host b.19.153.37 host b.84.22.11 eq 2748
access-list 101 permit tcp host b.19.153.37 host b.84.23.10 eq 2748
```

Recommended outbound ACLs:

```
access-list 102 remark Filter Traffic to CUE - Apply Outbound on Interface ServiceEngine
access-list 102 remark Restrict http access to management and phone segment
access-list 102 permit tcp a.10.1.0 0.0.0.255 host b.19.153.37 eq www
access-list 102 permit tcp a.10.2.0 0.0.0.255 host b.19.153.37 eq www

access-list 102 remark Restrict SIP signaling to host router
access-list 102 permit tcp host b.19.153.41 host b.19.153.37 eq 5060
access-list 102 permit udp host b.19.153.41 host b.19.153.37 eq 5060

access-list 102 remark Restrict RTP to IP phone and GW segment plus router
access-list 102 permit udp a.10.1.0 0.0.0.255 host b.19.153.37 range16384 32767
access-list 102 permit udp host b.19.153.41 host b.19.153.37 range 16384 32767

access-list 102 remark Restrict SMTP communication to host router
```

```
access-list 102 permit tcp host A.B.C.D host b.19.153.37 eq smtp

access-list 102 remark Restrict CCM communication to host router
access-list 102 permit tcp host b.84.22.11 eq 2748 host b.19.153.37
access-list 102 permit tcp host b.84.23.10 eq 2748 host b.19.153.37
```

The inbound ACL for SMTP `access-list 101 permit tcp host b.19.153.37 any eq smtp` allows Cisco Unity Express to send SMTP messages to any other host in the network. If you want to restrict this operation to allow Cisco Unity Express to send STMP traffic only to specific hosts in the network, then expand this ACL to list those hosts explicitly.

Similarly, in the outbound ACL for SMTP `access-list 102 permit tcp host A.B.C.D host b.19.153.37 eq smtp`, replace A.B.C.D with the explicit addresses of the hosts that you want to allow to send SMTP traffic to Cisco Unity Express.

Attach ACLs to the service-engine interface as follows:

```
interface Service-Engine1/0
 ip unnumbered FastEthernet0/0
 ip access-group 101 in
 ip access-group 102 out
 service-module ip address b.19.153.37 255.255.0.0
 service-module ip default-gateway b.19.153.41
```

Operating System (Linux)

Cisco Unity Express is an embedded Linux-based application. There is no access via CLI, telnet, or any other interface into the Linux operating system.

LDAP

While Cisco Unity Express includes an Lightweight Directory Access Protocol (LDAP) directory as part of the application, there is no access via CLI, telnet, or any other interface or protocol into LDAP— it is an entirely embedded system.

SQL

While Cisco Unity Express includes an Structured Query Language (SQL) database as part of the application, there is no access via CLI, telnet, or any other interface or protocol into the database—it is an entirely embedded system.

Software Installation

Cisco Unity Express 1.0 and 1.1 use TFTP for the initial installation step of loading the cue_installer image from a server. Cisco Unity Express 2.0 introduces an onboard installer that eliminates this step from the install process, except when the installer must be upgraded.

In all cases, the actual software installation uses FTP because of the following:

- TFTP is insecure and has no login/password control.
- FTP access can be secured with a login/password combination, even though the actual file transfer is not secure unless it travels over an IPSec-protected route between the FTP server and the Cisco Unity Express host router.

During the software installation, a command that is similar to the following is required to start loading software from the FTP server:

```
se-1-3-235-101installer#> s i p u ftp://a.3.61.16/cue-vm.1.1.1.pkg user ftpuser
```

In this example, “user” is the FTP account user ID, and “ftpuser” is the password. If the command is entered exactly as shown, then the password is echoed in clear text on the screen. If this operation is undesirable, omit the password from the “s i p u” command and the installer will prompt for a password (which is not echoed to the screen or stored anywhere).

Software Image and File Checking

All the files that are used during a software or license installation on Cisco Unity Express contain digital signatures that are cross checked during software installation and start-up. You can view an example list of files at http://www.cisco.com/cgi-bin/tablebuild.pl/cue-netmodule11. This digital signature precludes rogue software from being installed or started on the Cisco Unity Express platform.

Backup and Restore

Cisco Unity Express uses an FTP server for backup and restore. The FTP server’s password configuration in Cisco Unity Express is protected in the GUI (the field is blanked out) as well as in the CLI as shown in the following backup configuration show output examples:

```
cue# show backup
Server URL:                         ftp://127.0.0.1/ftp
User Account on Server:             test
Number of Backups to Retain:        20

cue# show running-config
backup server url "ftp://127.0.0.1/ftp" credentials hidden
"EWlTygcMhYmjazXhE/VNXHCkplVV4KjescbDaLa4fl4WLSPFvv1rWUnfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35jwAAA
AA="
```

There are several other considerations for securing backups. These include the following:

- The data transfer of the backup (or restore) uses FTP between Cisco Unity Express and the FTP server; therefore, only secured if this connection is protected by an IPSec tunnel between the router and the FTP server (or a router close to the FTP server).
- The storage of backup files is as secure as the access to the FTP server. The files are not encrypted unless you use an offline utility to encrypt these files after Cisco Unity Express has completed its backup (and decrypt them again before attempting a restore operation).
- All Cisco Unity Express user password fields (part of the user account information) inside the backed up files are encrypted. The backed up files are also encrypted on the Cisco Unity Express local storage and cannot be read directly or reverse engineered.

User Interfaces and Login Types

Cisco Unity Express supports three separate user interfaces: GUI, CLI, and TUI, and two types of users:

- Administrators—An administrator is a member of a group that has Super User privileges enabled. The system-default Administrators group has super-user privileges that are enabled by default, but you can also define your own groups that have this privilege.

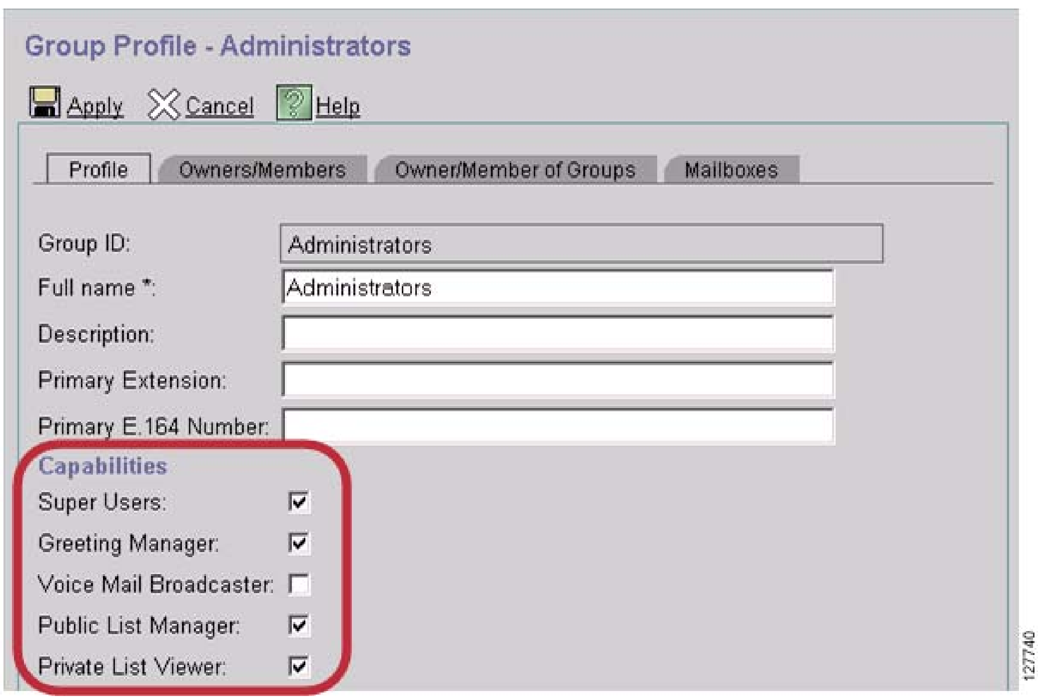
- End users (subscribers)—A subscriber is defined as any user account that does not have Super User privileges enabled (in other words, any user account that is not a member of any group that has these privileges).

The following configuration example shows the CLI of a system with the system-default Administrators group as the only group in the system with super-user privileges. Two user accounts (administrator and admin) are members of this group and can therefore log in to the GUI with full access. Figure 10 shows a screenshot of the GUI configuration for the same parameters.

Administrator definition configuration example:

```
groupname Administrators member admin
groupname customer-service member bob
groupname customer-service member cary
groupname customer-service member ggarrett
groupname Administrators privilege superuser
groupname Administrators privilege ManagePrompts
groupname Administrators privilege ManagePublicList
groupname Administrators privilege ViewPrivateList
groupname Broadcasters privilege broadcast
```

Figure 10 IP Connectivity Configuration



Up to Cisco Unity Express 2.0, only the Super User and Greeting Manager were defined in the system. As of Cisco Unity Express 2.1, five privileges are defined:

- Super User—This privilege grants access to the full GUI window of the system and can do any configuration task.
- Greeting Manager—This privilege grants Administration via Telephony (AVT) TUI access to administer AA prompts.
- Voice Mail Broadcaster—This privilege grants AVT TUI access to send broadcast messages.

- Public List Manager—This privilege grants GUI access to define and administer public distribution lists.
- Private List Viewer: This privilege grants GUI access to view the existence and membership of other users' private distribution lists. No changes can be made.

The preceding privileges can be assigned (in any combination) to any group defined in the system. User accounts who are members of that group then inherit the group's privileges.

Up to Cisco Unity Express 2.0, a single default system group (Administrators) existed. It included the Super User and Greeting Manager privileges. As of Cisco Unity Express 2.1, two default system groups are defined with privileges as follows:

- Administrators—Super User, Greeting Manager, Public List Manager, and Private List Viewer
- Broadcasters—Voice Mail Broadcaster

Access to a Cisco Unity Express system is summarized in Table 7.

Table 7 Cisco Unity Express Administrator and Subscriber Access Privileges

	Administrator	Subscriber
GUI access	Full GUI (all menus and fields).	View access to users and groups defined in the system. Modify access only to personal profile password, personal identification number (PIN), mailbox greeting, and mailbox 0-out destination.
Password and PIN reset	Access to password and PINs for all users on the system. Passwords cannot be viewed (unless the default assigned by the system is still active and the password has never been changed), but can be changed.	Access to own password only. Passwords cannot be viewed, but can be changed.
CLI	Via router access only. The Cisco Unity Express administrator or user account information is not used for this access.	None.
Voice-mail TUI	For own mailbox. Same as Subscriber access.	For own mailbox.
AVT TUI—AA alternate greeting and customer prompts	Yes.	No.
AVT TUI—Broadcast messaging	No.	Members of "Broadcasters" group only.
AVT TUI—Remote User Administration	Yes.	No.

Passwords and PINs

All Cisco Unity Express user accounts (administrator and subscriber) defined on the system are password controlled on login. Passwords are used for Web login access, while PINs are used for TUI mailbox and AVT login access.

Rules that govern passwords and PINs include the following:

- Passwords are mandatory, can be 3 to 32 characters long, are case sensitive, and allow alphabetic and numeric characters.
- PINs are mandatory, can be up to 3 to 16 digits long, and are numeric only.
- Passwords and PINs do not expire up to Cisco Unity Express 2.0. As of Cisco Unity Express 2.1, you can configure passwords and PINs to expire (with a default system setting of 30 days).
- Passwords and PINs are not checked against a history of recently used passwords. As of Cisco Unity Express 2.1, when a password or PIN expires, the most recently used password and PIN cannot be selected again.
- Passwords and PINs can never be viewed, displayed, or extracted from the system, passwords and pins are encrypted and stored with a one-way hash algorithm.
- Default passwords and PINs are assigned by the system when new user accounts are created—these can be blank or randomly generated (the latter is recommended). Randomly generated system default passwords and PINs appear in the GUI to a user with Administrator privileges, until the you change the password and PIN; then, they are never visible again. Passwords and PINs are never visible in the CLI.

When a password or PIN is changed, checks done include the following:

- Password and PIN grammar (valid characters)
- The new password or PIN is a minimum of 3 characters long (as of Cisco Unity Express 2.1, the minimum length of a password or PIN can be configured if the system default does not comply with your security policy)
- The new password or PIN is different from the current password

There is an idle timeout of 10 minutes on any GUI login. Mouse movements do not count as activity; you must click menu items and open or close windows to reset the inactivity timer. The user is forced off after the inactivity timer expires.

Password and PIN Recovery

A forgotten password or PIN cannot be recovered by a subscriber; contact the system administrator to do this. An administrator can never extract an existing password or PIN from the system, but can reset any user account password or PIN to a known string, and then advise the user of the new setting. The user can then log back in and change the password or PIN to a private setting.

If the Administrator cannot log in (due to a forgotten or incorrect password), and another administrator is defined on the system, the other administrator can log in and reset the password. If there is no other administrator defined on the system, your only recovery path is to log in to the Cisco Unity Express CLI, and either reset the password by using the CLI, or add another administrator to the system who can log in to the GUI to reset the password. To do this, you need the router enable password.

By using the user account definitions given previously in the "Suggested Access Control Lists" section on page 22, you can reset the administrator's password or the user account PIN. You can reset account's PIN to 1234, by using the Cisco Unity Express CLI command **username admin password** *xxxx* or **username admin pin 1234**. As an example, you can add a new administrator with a known password to the system as shown in the following:

```
cue> username new-admin create
cue> username new-admin password xxxx
cue> username new-admin group Administrators
```

Default System Password Policy

Any new user account created on the Cisco Unity Express system is automatically assigned a password and a PIN. The default policy can be set to blank or to randomly generate a password and a PIN. The latter policy is recommended and is the system default. If you want to assign blank passwords as the default policy, use the **Defaults** > **User** window to set the policy.

The first time any user logs in to the GUI (password) or into a mailbox (TUI), the user is forced to change the password and PIN before any access to the system is granted. At this time, the password can no longer be blank, it must be a valid password and PIN of the minimum number of characters that are configured on the system (system default is 3).

There is a retry limit of three attempts on a PIN (not applicable to passwords). When you exceed the limit, an error message is logged and the user is returned to the top-level prompt ("if you have a mailbox on the system, enter it, otherwise please hold for an operator"). The mailbox is not disabled.

CLI

There is no CLI password on the Cisco Unity Express system itself. But the Cisco IOS session command on the router is required to gain access to the Cisco Unity Express CLI, and Cisco Unity Express is therefore protected by the router CLI password protections. The Cisco IOS session command requires enable mode on the router.

Security Best Practices

The following recommendations summarize suggested actions required to secure access to your Cisco Unity Express system:

- Assign an enable password to the router hosting the Cisco Unity Express module.
- Restrict telnet access to the router.
- Enable login and password control on the router TTY port connecting to Cisco Unity Express.
- Configure an inactivity timeout on the router TTY port connecting to Cisco Unity Express.
- Enable SSH on the router to protect telnet traffic; use only SSH-capable telnet client software.
- Use VPN/IPSec router technology to protect HTTP web access into Cisco Unity Express HTTPS is supported in a later release.
- Use ACLs to close access to any ports that are not actively in use by Cisco Unity Express.
- Use ACLs to restrict traffic into and from Cisco Unity Express.
- Protect the FTP server that is used for software installation with a login/password control.
- Protect the FTP server that is used for backup and restore with login/password control.
- During a Cisco Unity Express software install/upgrade, do not provide the FTP password on the install command line; let the installer prompt you for it.
- Maintain the Cisco Unity Express system with the "generate random password and PIN" user access policy. This is the default policy in a newly installed system.
- If you're using Cisco Unity Express 2.1 or a later release, enable the password and PIN expiry feature.
- Set the minimum length for passwords and PINs on Cisco Unity Express to be in line with your security policies.

System Management Considerations

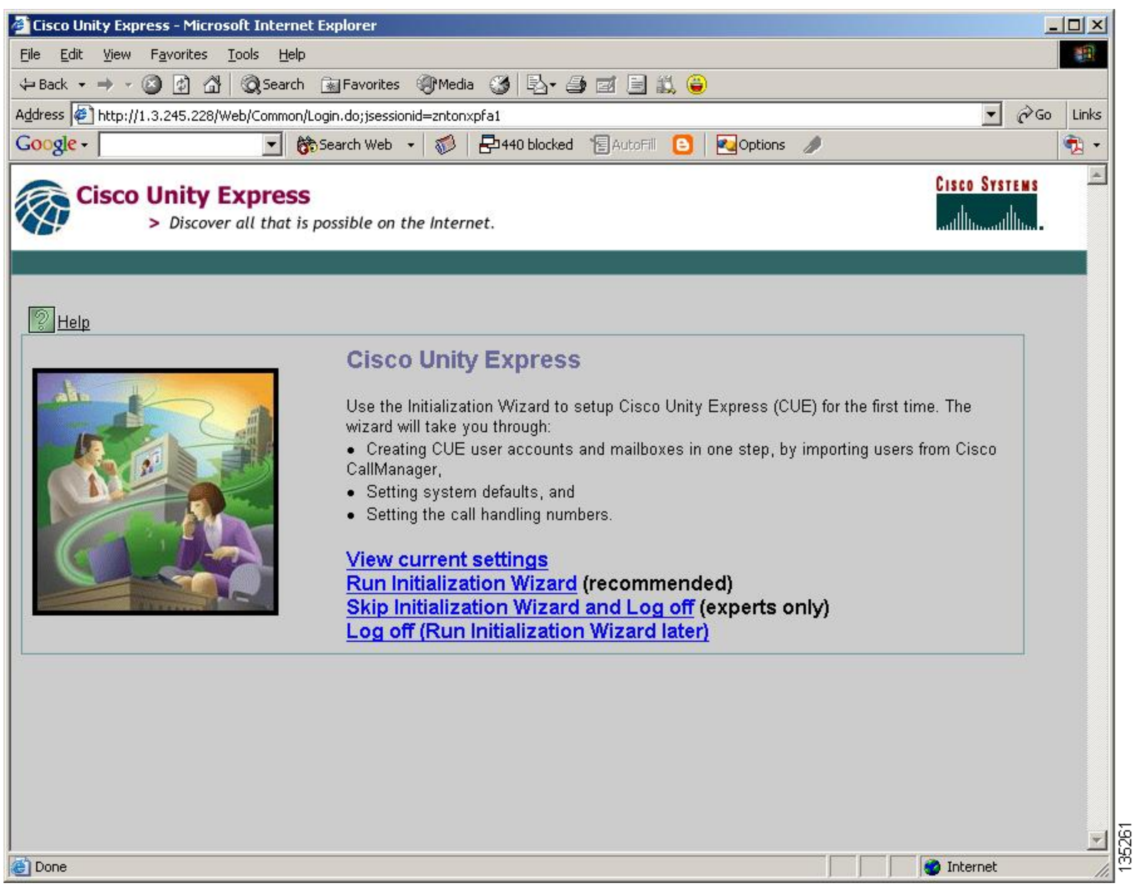
System management considerations for Cisco Unity Express deployment are bulk provisioning and call-detail record maintenance.

Bulk Provisioning

Cisco Unity Express offers a CLI and can therefore be provisioned via scripting from a central Network Management station.

If the Cisco Unity Express system is provisioned entirely via CLI, the Initialization Wizard flag is never reset. This has no operational impact on the system other than when administrators log in to the GUI.AT that point, adminstrators are presented with the Initialization Wizard banner window, even though the system is by now fully configured and operational. In this situation, the administrator should choose the "Skip Initialization Wizard" link shown in Figure 11, as it is not applicable to a system that is already fully configured.

Figure 11 Bypass the Initialization Wizard for a Fully Configured System



Call Detail Records

There is no information specific to Cisco Unity Express captured in call detail records (CDRs). CDRs are produced by the call control engine, either Cisco CME or Cisco CallManager.

Power Backup

A Linux platform should be disconnected from its power source without going through an orderly shutdown. Not doing so risks corruption of the file system. However, on a router platform, you can power cycle the chassis without regard to what is plugged into it. Also, there are unexpected power failures that no one can control. While every precaution has been taken to harden Cisco Unity Express's file system against corruption when power is removed unexpectedly from the system, there is a risk of data corruption associated with power failures.

Best Practices

The following "best practices" are recommended for Cisco Unity Express implementation:

- Follow the Cisco Unity Express system shutdown procedures at all times before disconnecting power from the router that hosts Cisco Unity Express.
- For any router that has telephony features of any kind, an uninterrupted power supply (UPS) is recommended.

Chapter 3: Cisco Unity Express System Design Considerations

The "Chapter 2: Network Infrastructure Considerations for Cisco Unity Express" chapter addressed network infrastructure considerations such as IP addressing, date and time synchronization, and security features when deploying Cisco Unity Express in your network. Cisco Unity Express offers both an autoattendant (AA) and a voice mail application. Before describing these topics individually in subsequent chapters, this chapter addresses general Cisco Unity Express design considerations that apply at a system level is to both AA and voice mail. Topics in this chapter include how the "ports" on the system are set up and used by the applications, how language is customized, and system backup considerations.

Sections in this chapter address the following topics:

AA and Voice-Mail Ports

Cisco Unity Express does not have any physical ports as it is a purely IP-based system. However, as is common for AA and voice mail systems, there is a limit on the maximum number of simultaneous calls that can be active in the system at any one time. This limit is referred to as *ports* or *sessions*.

Up to Cisco Unity Express 2.0, a combination of the mailbox license and the hardware that was purchased with a Cisco Unity Express system determined the number of ports the system had. You could not via the configuration. The number of ports included all calls into any of the system's pilot numbers (that is, the AA, the AVT as well as voice mail). Table 8 summarizes the ports for different hardware and licensing on Cisco Unity Express for releases up to Cisco Unity Express 2.0.

Table 8 Cisco Unity Express Ports for 1.0, 1.1 and 2.0

Cisco Unity Express Hardware	License	Ports
NM-CUE	12 mailbox	4
	25 mailbox	4
	50 mailbox	8
	100 mailbox	8
AIM-CUE (512M and 1G CF)	12 mailbox	4
	25 mailbox	4
	50 mailbox	4

With Cisco Unity Express 2.1, the number of ports are decoupled from the license that is installed on the system, and instead has a dependency only on the Cisco Unity Express hardware form factor and the router platforms on which Cisco Unity Express is installed. Table 9 summarizes the ports for different hardware platforms on Cisco Unity Express for Cisco Unity Express 2.1 and later releases.

Table 9 Cisco Unity Express Ports for s 2.1 and Higher

Cisco Unity Express Hardware	License	Platform	Ports
NM-CUE	All	All	8
NM-CUE_EC	All	All	16
AIM-CUE (512M and 1G CF)	All	Cisco 2600XM, Cisco 2691	4
AIM-CUE (512M and 1G CF)	All	Cisco 2800, Cisco 3700 and Cisco 3800	6

Ports cannot be dedicated to either the AA or voice mail; the ports are shared by default. There is, however, separate configuration control of the maximum number of calls into each AA and the maximum number of calls in voice mail. You can have multiple AAs defined, each with its own pilot number.

Note For optimal system performance, retain the default system configuration, which is to share all system ports among all the AA and voice mail pilot numbers (that is, to have all the AA and voice mail session parameters set to the maximum number).

Use the following GUI windows if you want to change the default configuration and limit the maximum number of ports used by the following:

- AA—**Voice Mail** > **Auto Attendant** > select the appropriate AA > **Next** (Script Parameters) > **Next** (Call Handling) and change the maximum sessions field. The *maximum sessions* field is applicable to each individual AA pilot number and, as with the sharing arrangement with voice mail, the default operation here is also to share the system ports equally among all the different AA pilot numbers that are defined on the system (there can be up to five AAs defined).
- Voice mail—**Voice Mail** > **Call Handling** and change the maximum sessions field.

AA and Voice Mail Operators

You can configure Cisco Unity Express at least two different operators on the system, that of the system AA and the voice mail operator. Additionally, you can define operators in your custom AA scripts.

Set the system "operator" fields, so that calls that encounter error conditions or do not make valid dual-tone multifrequency (DTMF) choices from the prompts and menus that are provided by the system (AA or voice mail), are redirected to an "operator" (likely a receptionist or an administrative assistant) who can help direct the caller.

Topics addressed in this section include the following:

- Voice Mail Operator, page 35
- System AA Operator, page 35
- Custom AA Operator, page 35

Voice Mail Operator

Cisco Unity Express defines a system voice mail operator where calls are redirected if a caller does not respond to voice mail menus, or does not hang up after leaving a voice mail for a subscriber. The voice mail "operator" is triggered when the following voice mail prompt is reached:

> "If you have a mailbox on the system, please press #, or you will be transferred to the operator."

By default, the voice mail operator is set to the AA pilot number. Alternately, you can set this to the extension of any employee in your office. To change this attribute, choose **Voice Mail** > **Call Handling** and change the "Voice Mail Operator Number" field.

System AA Operator

The Cisco Unity Express system AA (the "autoattendant" script on the **Voice Mail** > **Auto Attendant** GUI window) has an operator extension to which calls are directed when you select "0" from the system AA menu to transfer to the operator. You can set this extension to any dialable digit string using the **Voice Mail** > **Auto Attendant** > **autoattendant (aa.aef)** > **Next** (Script Parameters) "operExtn" field. By default the "openExtn" field is set to 0 which might not be a meaningful or dialable string in your configuration. Ensure that either 0 is dialable and results in a call being routed to desired destination, or set this parameter to the extension number of a phone in your office.

Custom AA Operator

Any of your customized AA scripts can optionally provide menus or prompts to the caller to choose an operator (or receptionist). This operator setting is specific to each custom AA script and is independent of the system AA and voice mail operator system settings described in the "Voice Mail Operator" section on page 35 and the preceding "System AA Operator" section.

Operator extensions in your custom AA scripts show up as parameters in the script and you can set the values of these fields by using the **Voice Mail** > **Auto Attendant** > [choose your custom AA script] > **Next** (Script Parameters) and change the field that corresponds to the script variable you chose for this field.

Codecs and Transcoding

Cisco Unity Express supports only G.711 voice streams, so all calls made into the system (including those from IP phones, PSTN gateway ports and any other VoIP equipment in your network) must use G.711 if they enter the AA or voice mail pilot numbers that terminate on Cisco Unity Express.

If you require that G.729A calls traverse IP segments of your network between sites, and that these calls forward or dial direct into Cisco Unity Express AA or voice mail, then you must use a transcoding resource collocated with Cisco Unity Express to change the voice stream from G.729A to G.711 before the voice stream enters the AA or voice mail pilot numbers.

Topics addressed in this section include the following:

- Voice Activity Detection, page 36
- Dual-Tone Multifrequency Relay Method Support, page 36

Voice Activity Detection

When calls terminate into Cisco Unity Express AA or voice mail, voice activity detection (VAD) must be disabled.

For Cisco CME and Cisco SRST configurations, this is a setting controlled by the Session Initiation Protocol (SIP) dial-peer defining the routing for calls into Cisco Unity Express, as shown in the following configuration example. The configuration of the far-end device or dial-peer does not matter in this case because Cisco CME or Cisco SRST terminates the voice stream and re-originates it towards Cisco Unity Express.

The following example depicts VAD disabled on dial-peer with Cisco CME or Cisco SRST.

```
dial-peer voice 3100 voip
 description VM-AA
 destination-pattern 31..
 session protocol sipv2
 session target ipv4:172.19.153.37
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
```

For Cisco CallManager deployments with Cisco Unity Express, the VAD parameter is controlled by either Cisco CallManager (IP phones) or by the far-end PSTN gateway. If this is an H.323 gateway, then set the dial-peer on that gateway that is pointing the call towards Cisco CallManager to so that VAD is disabled.

Dual-Tone Multifrequency Relay Method Support

Cisco Unity Express supports only the SIP-notify out-of-band, dual-tone multifrequency (DTMF) relay method. Inband DTMF cannot be processed by Cisco Unity Express, regardless of whether this is inband tones via the speechpath, or inband DTMF relay using RFC 2833. While Cisco Unity Express uses a SIP interface to communicate with Cisco CME or Cisco SRST, SIP trunking calls and SIP phones are not currently supported by Cisco Unity Express—due to the lack of RFC 2833 support. A future release is planned to support RFC 2833-based features, but such support is not available in any release up to Cisco Unity Express 2.1.

VoIP trunking calls into Cisco Unity Express must be H.323, and IP phones with mailboxes on Cisco Unity Express must be controlled via Skinny Client Control Protocol (SCCP) by the call agent (Cisco CME, Cisco SRST or Cisco CallManager).

Subscriber Names and Directories

Cisco Unity Express has an embedded, local Lightweight Directory Access Protocol (LDAP) directory where user definitions are stored. There is no external access to this LDAP directory (from an outside application to Cisco Unity Express's directory), nor does Cisco Unity Express offer any means to coordinate its internal user information with an external directory such as Active Directory (from Cisco Unity Express to an external application).

There is a user import function in Cisco Unity Express where it can access either the Cisco CME router configuration, or the Cisco CallManager database to draw out new user definitions that do not exist in Cisco Unity Express's directory. As a result, you do not need to retype this information. The import function is a one-time, manually initiated activity. The import function is not a directory synchronization feature.

Cisco Unity Express's internal LDAP directory drives the dial-by-name feature available in the AA. Users that are not defined on the Cisco Unity Express system configuration do not show up in the dial-by-name directory. You can insert user definitions on Cisco Unity Express that do not have mailboxes on the system if you want them to be accessible via the AA dial-by-name feature. The user name defined in Cisco Unity Express is independent of any user names defined for phone display purposes or directories of other IP telephony systems in your network.

Language Customization

Releases prior to Cisco Unity Express 2.0 support only U.S English. As of Cisco Unity Express 2.0, three additional languages are supported:

- European French
- German
- European Spanish

A Cisco Unity Express system can only support one language at a time, so if you install one of the alternate languages (U.S. English is the default), that language replaces the current language on the system.

Language customization in Cisco Unity Express affects the system AA and voice mail prompts. Language customization does not affect the CLI, GUI, custom prompts, user spoken names, or user greetings. The administrative interfaces (CLI and GUI) are always English only. Custom AA prompts, user spoken names, and user greetings can be in any language you like and are not controlled by the language customization of the system.

While the strategy of individual product roadmaps strive to support the same languages for different Cisco products in your IP telephony network, there is no technical dependency or coordination between the languages that are supported by the different systems, including Cisco Unity Express, Cisco Unity, Cisco CME, and Cisco CallManager. Each of these systems is independently configured and customized with languages.

Backup and Restore

Backup and restore operations use FTP to an FTP server. Flash or other types of media cannot be used for backup and restore.

Cisco Unity Express backup must be initiated manually; there is no mechanism within the system itself to schedule unattended backups. As the backup functionality is available via the CLI (as well as the GUI), it is possible for you to develop a script on another server that will automatically (such as based on time-of-day) log in to the Cisco Unity Express system's CLI and initiate a backup. If you do scheduled backups in this manner, take the following into consideration:

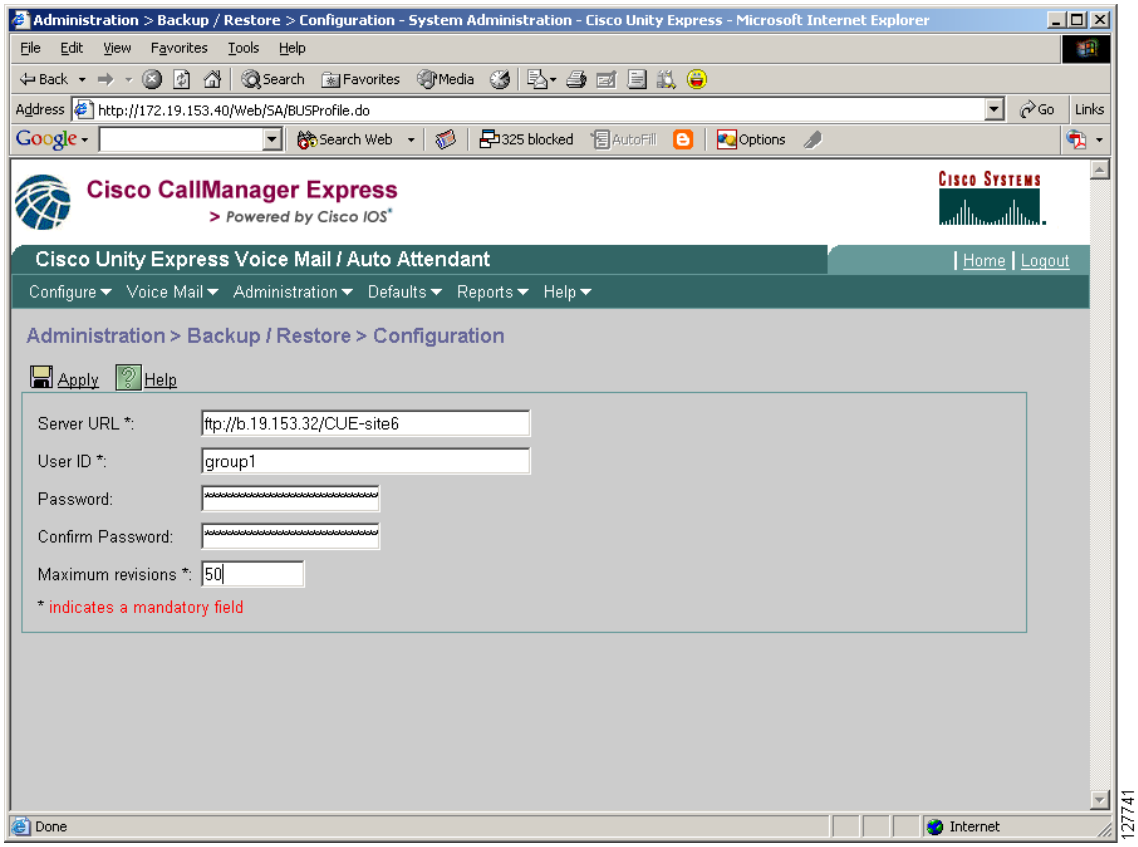
- Doing a backup requires the system to be offline, and taking the system offline disconnects all calls in progress. So if the backup is triggered by a script where the warnings about call disconnection are not seen (due to a scripted interface), this may cause you to do backups during normal day-time use of the system and thereby disrupting the operation of the system. Write your script to initiate backup during a time of day when no calls are expected to be active.
- If any errors occur, ensure that your script provides a notification to an administrator to investigate.

Topics addressed in this section include the following:

Directory Path for Backup

A backup from a Cisco Unity Express system is done to a configured FTP server, and the directory location specified in the configuration cannot be the root path of the FTP system. Figure 12 shows an example configuration where ftp://b.19.153.33/CUE-site6 is the backup path. A value of ftp://b.19.153.33/ is unacceptable. To enter the backup server path, the FTP server must be in contact with Cisco Unity Express. As a result, the FTP location must exist, and Cisco Unity Express validates the location during configuration entry.

Figure 12 Backup FTP Server Configuration



The preceding configuration is shown in the following CLI example.

Note Note that the password is not printed in either the GUI or the CLI – this is done for security purposes. It is strongly recommended that the FTP server user account you use for backups is password protected. The backup files are not encrypted by Cisco Unity Express.

The following is CLI output example depicting backup FTP server configuration:

```
cue# show backup
Server URL:                        ftp://b.19.153.33/CUE-site6
User Account on Server:            group1
Number of Backups to Retain:       50
```

Cisco Unity Express logs into the FTP server with the account user ID specified in the configuration. In the preceding example, this is `group1`. The backup directory specified in the configuration (CUE-site6) is therefore a subdirectory from the "home" location of the user ID on the server. In this example it is:

```
/home/group1/CUE-site6
```

Backing Up Multiple, Networked Cisco Unity Express Systems

Backup processes done from one Cisco Unity Express system have no knowledge of backups or server paths used by other Cisco Unity Express systems in the same network. If multiple Cisco Unity Express sites are configured to back up to the same FTP server, ensure that a separate directory is used for each site and that the directories are named in a recognizable manner, for example by use of site numbers (as shown below) or geographical tags of sites:

- ftp://b.19.153.33/CUE-site6
- ftp://b.19.153.33/CUE-site7
- ftp://b.19.153.33/CUE-site8

There is nothing in the actual backup file naming that indicates what site this backup belongs to—all site file names are the same as shown in the following example. If multiple Cisco Unity Express systems point their backups to the same directory location on the FTP server, the Cisco Unity Express systems will interfere with each other and the backup will not be successful. Also, the administrator will be unable to tell which backup belongs to which Cisco Unity Express system, making restore operations unsuccessful.

The following output example depicts backup file names:

```
[backup-server]$ cd /home/group1/CUE-site6
[backup-server]$ ls -l
total 40
drwxr-xr-x    2 cue    cue    4096 Mar 11 19:42 Configuration_1
drwxr-xr-x    2 cue    cue    4096 Mar  6 19:00 Configuration_2
drwxr-xr-x    2 cue    cue    4096 Mar 19 11:38 Configuration_3
drwxr-xr-x    2 cue    cue    4096 Mar 19 12:52 Configuration_4
drwxr-xr-x    2 cue    cue    4096 Mar  5 17:00 Data_1
drwxr-xr-x    2 cue    cue    4096 Mar  6 18:58 Data_2
drwxr-xr-x    2 cue    cue    4096 Mar 13 21:15 Data_3
drwxr-xr-x    2 cue    cue    4096 Mar 19 11:38 Data_4
-rw-r--r--    1 cue    cue    5178 Mar 19 13:15 history.log
```

Configuration and Data in the Backup

The router configuration is not backed up or restored—only the Cisco Unity Express application configuration and data are backed up and restorable. A Cisco Unity Express backup provides a choice of configuration or data categories, or both.

Configuration information includes:

- System configuration
- Voice Mail configuration
- User Information and Spoken Names
- AA scripts and prompts

Data information includes:

- Voice Mail greetings
- Voice Mail message content

For a large system (many mailboxes with many messages), the data information is the bulk of the size of the information to be backed up, and the configuration is small in comparison. For example, in a test on a 40 user system with 40 minutes of voice mail, 22 megabyte of the 24 MB backup was in the voice message (data) part of the backup. The data is also what changes most frequently and what must be backed up daily. There is little incentive to back up one set of information without the other, and the recommendation is to back up configuration and data daily during a time when no voice calls are likely to be active in the system. Backing up configuration and data at all times also simplifies restore operations—ensuring that the configuration (of mailboxes) and the voice messages (content of the mailboxes) coincide.

As the configuration of the system is part of the backup, it is important to back up from, and restore to the same system. If a backup is done from Site-1 and this is restored onto Site-2, the Site-2 system will assume the identity and all the characteristics of Site-1, including DNS settings, hostname, and IP address settings, which is almost certainly undesirable. Such a system could be recovered (identity changed back to Site-2) by retaining the user and mailbox definitions and message content of the Site-1 system, but considerable manual configuration will be required to do so and this is not recommended.

Selective Backup

While there is a choice to back up configuration or data or both as discussed in the "Configuration and Data in the Backup" section on page 40, the particular feature does not provide a selective backup capability. Instead, the backup and restore feature in Cisco Unity Express is designed as a disaster protection mechanism. A backup or restore operation is per system; it is not per mailbox and not per message. It is not designed to facilitate moving user mailboxes from one system to another as they move between sites and there is no way to accomplish this in Cisco Unity Express 2.0 software. Nor is there any way to restore a message that a user accidentally deleted.

Multiple Generations of Backups

Up to 50 generations of backups are kept (if configured to do so) by the Cisco Unity Express Backup and Restore facility. The default is 10. When a backup exceeds the configured maximum number of generations, the oldest backup is automatically deleted—the backup attempt does not fail. So the number of generations of backups kept by the system, such as 15, is a moving window of the most recent 15 backups done on the system.

There is no date/time stamp in the backup itself or in the file names that are used, so ensure that the clock is set correctly on the FTP server where the backups are stored, so that file timestamps are an accurate indication of the last backup date. The Backup History on the Cisco Unity Express system does contain a time and date stamp for when the backup was done. Sample output of the CLI backup history command is shown in the following example. The same information is available via the GUI and navigating to **Administration** > **Backup/Restore** > **Configuration**.

The following show an example backup history:

```
cue# show backup history

#Start Operation
Category:       Configuration
Backup Server:  ftp://b.19.153.33/CUE-site6
Operation:      Backup
Backupid:       1
Description:    Site 6
Date:           Sun Apr 21 06:42:34 PDT 2004
Result:         Success
Reason:
#End Operation

#Start Operation
```

```
Category:       Data
Backup Server:  ftp://b.19.153.33/CUE-site6
backups
Operation:      Backup
Backupid:       1
Description:    Site 6
Date:           Sun Apr 21 06:42:41 PDT 2004
Result:         Success
Reason:
#End Operation
```

If more than 50 generations of backups must be kept (or 50 days assuming backups are run daily), this can be accomplished by using a succession of different directories for backups. For example, ftp://b.19.153.33/CUE-site6 could be the backup directory that is configured for the first 50 backup days, and then change the configuration to ftp://b.19.153.33/CUE-site6-2, and this will cause another 50 backups to be stored in the second directory without affecting the ones in the initial directory. The backup generations is controlled by the history.log file stored in the backup directory, shown earlier in the "Backing Up Multiple, Networked Cisco Unity Express Systems" section on page 40. This file controls the number of backups and is used to determine which backup should be deleted if the maximum number of generations is exceeded. This file also controls the restore view (in the GUI navigate to **Administration** > **Backup / Restore** > **Start Restore**) should you select to do a restore. The restore view is built from the current directory configured for backups, so by changing the configuration (temporarily) you can get a view of an older directory and select a restore from there.

Note Do not move or change individual files within a backup directory (such as CUE-site6). Doing so invalidates the history.log control file and therefore the ability to restore any of the backups from this directory. You can move or copy (or encrypt with an offline utility) the entire directory, but do not perform such operations on individual files within the directory.

Backup File Sizes

The largest contribution in size to a Cisco Unity Express backup is the actual voice mail message content. Messages are stored in G.711, which is a 64 kilobit codec, so the size can be calculated at 64000/8=8000 bytes per second, therefore 8 kilobyte file size per second of recorded voice. This factor applies to mailbox greetings, spoken names, and voice message content.

The components of a Cisco Unity Express system that determines the backups file size include:

- The base system configuration
- User and mailbox definitions, including spoken names and greetings
- Voice message content
- Custom AA scripts and prompts

If the following attributes of the system are known, you can estimate the backup size:

- AA script and prompt sizes
- Greeting time per user (in seconds)
- Spoken name time per user (in seconds)
- Number of users
- Total voice mail minutes

All the non-AA information, with the exception of spoken name time, is available from the Cisco Unity Express system as shown in the following example. The same information can be seen in the GUI by navigating to **Reports** > **Voice Mail**. Spoken name time can be estimated at 3 seconds per mailbox.

The following output example illustrates system summary:

```
cue# show voicemail usage
personal mailboxes:                     40
general delivery mailboxes:             0
orphaned mailboxes:                     0
capacity of voicemail (minutes):        6000
allocated capacity (minutes):           3310.0
message time used (seconds):            2400
message count:                          33
average message length (seconds):       72.72727272727273
greeting time used (seconds):           308
greeting count:                         40
average greeting length (seconds):      7.7
total time used (seconds):              2708
total time used (minutes):              45.13333511352539
percentage used time (%):               1
```

You can derive the size of AA information from the file sizes given in the **Voice Mail** > **Prompts** and **Voice Mail** > **Scripts** GUI windows. Similarly, the **show ccn** prompts and **show ccn scripts** CLI commands can be used to see the same information.

An estimate of the backup file size for a particular Cisco Unity Express system can be made with the following calculation (the figures given here are based on Cisco Unity Express 1.2) and adding together all the components:

- Base system configuration: assume 400-to-500 KB
- Users and mailboxes: (average greeting time(s) * 8 KB) + (average spoken name time(s) * 8 KB) * number of mailboxes
- Voice messages: (voice message time(s) * 8 KB) + 5 percent overhead factor
- AA: (script + prompt files sizes) + 5 percent overhead factor

Backup Bandwidth

FTP is a protocol that uses all the bandwidth it can get to communicate between two systems. The more bandwidth is available, the quicker the FTP session will be. It is recommended that you insert a QoS policy on the WAN link of the router that carries the Cisco Unity Express backup traffic to regulate the bandwidth available to FTP traffic. Once this available bandwidth is determined and you have an estimate of the backup size for a particular site (using the information given in the "Backup Bandwidth" section on page 43), you can estimate how long a typical backup will take. Cisco Unity Express does not perform incremental backups; it completes a full backup of all information every time.

If you have LAN connectivity between the Cisco Unity Express system and the FTP server, a typical backup takes two to three minutes.

Best Practices

The folowing list gives the best practises to follow when configuring and performing backups on a Cisco Unity Express system:

- Ensure that the running configuration is written out to the start-up configuration before a backup is done. From the Cisco Unity Express CLI, enter the **write** command, or from the GUI, go to the **Administration** > **Control Panel** and click the **Save Unity Express Configuration** button.
- Restore onto the same system that was backed up. However, if you must restore onto a different system, then it is best to do so on a system that has been newly installed (that is, it has no preexisting configuration) with a license that matches that of the system that created the backup. License mismatches are encountered when restoring onto a different system than the one from which data was backed up—which can cause unpredictable results.
- Do a backup at the end of the business day when users are no longer using the system and incoming calls are zero at a minimum.
- Back up both Configuration and Data daily.
- Back up each system in a network to a uniquely named directory on the FTP server.
- Ensure that the clock is set correctly on the FTP server.
- Ensure that there is enough disk space on the FTP server for the backups to complete successfully.
- Do not modify or delete individual files within a backup directory.

Shutdown, Linux and OIR

Cisco Unity Express is a Linux-based system and therefore, like all Unix and Linux systems, must be shut down before you turn off the system. Not doing so runs the risk of corrupting the file system which will require a software install and restore from a backup to recover.

Of the platforms supporting Cisco Unity Express, only the Cisco 3745 and Cisco 3845 have online insertion and removal (OIR) capability. OIR is an attribute of the platform, not of the NM, so the NM-CUE or NM-CUE-EC can be removed and replaced during OIR, as can any other NM on an OIR-capable platform.

If OIR is done on the NM-CUE or NM-CUE-EC:

- Manually shut down Cisco Unity Express application prior to removing the NM from the chassis.
- Replace only like-for-like modules (that is if you remove an NM-CUE module, insert another NM-CUE module into the same slot). This is a requirement for all NMs replaced via OIR.

Do not use OIR to insert an NM-CUE module into a system that has never had an NM-CUE resident and configured in that same slot before. For example, if slot 2/0 is open on an existing running router, the NM-CUE cannot be added without requiring a reboot of the router. The router does not recognize unconfigured hardware during an OIR operation, only replacement of the existing hardware.

Upgrades and Downgrades

Two types of upgrades can be done on a Cisco Unity Express system:

- Software upgrade where the software release level is changed.
- License upgrade where the capacity of the system (the number of mailboxes) is changed.

A downgrade is defined as going backwards in either software release (such as Cisco Unity Express 2.0.2 to 2.0.1) or license level (such as 25 mailboxes to 12 mailboxes) while maintaining the system configuration and data on the disk.

Topics addressed in this section include the following:

Software Upgrades

There is no particular software upgrade procedure as such in Cisco Unity Express. Software upgrades are accomplished by:

- Doing a backup procedure.
- Installing a new release of software.
- Doing a restore procedure.

If only the software release level changes during an upgrade, then no action with regard to license installation has to be taken. The existing license survives a software release change.

Note A software install cleans the disk, so no configuration or voice message data survives a software install or upgrade; it is imperative to do a system backup before you start the upgrade.

In Cisco Unity Express releases prior to 2.0, a full installation was done every time, which means the entire software image file (of about 70 MB) was downloaded from the FTP server to the Cisco Unity Express system during the install/upgrade procedure. Cisco Unity Express 2.0 and later releases support an incremental upgrade capability where file and component checks are done, and only the incremental changes are downloaded from the FTP server.

For upgrades of minor releases, for example Cisco Unity Express 2.0.1 to Cisco Unity Express 2.0.2, this should save a significant amount of downloading time, especially if your FTP server is accessible only via a WAN link. A major release upgrade (for example, from 2.0 to 2.1) will likely contain much more incremental changes and therefore be closer in size to the full download time. The actual download time varies, depending on the current and target release of the upgrade and the exact file changes between the two releases.

License Upgrades

If the capacity of the system is changed, for example from a 12-mailbox system to a 25 mailbox system, then install a new license file on the Cisco Unity Express system. If a license installation is done in isolation (that is, the software level remains the same), then the disk contents survive and the system is operational after the license install.

Note It is always good practice to do a backup before any installation or upgrade, so while it may not be needed, it is recommended to do a backup before a license install.

If the capacity of the system (license) is changed at the same time that the software level is also changed, then a backup is mandatory, and the disk will be cleaned during the software upgrade operation.

Downgrades

Limited software downgrade capability is supported as of Cisco Unity Express 2.0. A downgrade of the license level (while preserving the configuration and data of the system) of a Cisco Unity Express system is not supported and doing so may cause unpredictable results.

Chapter 4: Auto-Attendant Design Considerations

Cisco Unity Express offers auto-attendant (AA) and voice-mail applications. You can choose to use one or both together. Cisco Unity Express is designed to have both applications work together. The AA functionality in Cisco Unity Express is not licensed separately, so all Cisco Unity Express installations have this functionality by default.

Sections in this chapter address the following topics:

Routing PSTN Calls to the AA

The decision on call routing for PSTN calls is partially dependent on what PSTN service you get from your carrier, as well as what trunk types you use. Option include the following:

- Direct inward dial (DID) Service— Employees (some or all) have individual PSTN phone numbers, and typically these calls would be automatically switched to the person's extension. Non-DID calls would typically go to the AA or a receptionist.
- PSTN lines—You can have one or more PSTN numbers for your business (but these are not associated with particular employees; you just have three or four general lines from the PSTN). When the call comes in, you know which PSTN number was dialed, either because the dialed number from the PSTN was delivered with the call (and this depends on trunk type), or the number is not delivered, but you can derive that information from which port the call came in on, such as line 1 on port 1/0/0 is yyy-1212 and line 2 on port 1/0/1 is yyy-1212.

DID calls typically terminate directly on the employee's extension, although there is nothing that stops them from terminating into AA if you should want to do so.

General PSTN lines—where the dialed number is either not available (FXO trunks) or is meaningless—are typically terminated at the receptionist or AA. If the number is available and meaningful (for instance, yyy.1212 is the main business number and yyy.1213 is for employees to retrieve voice mail from home or while traveling), then calls can be automatically routed to the appropriate destination.

Topics addressed in this section include the following:

Trunk Types and DNIS

All PSTN trunk types provide dialed-number information (DNIS), except Foreign Exchange Office (FXO). On trunk types that provide DNIS, you can optionally have DID service. Therefore you can route calls based on the number that was delivered by the PSTN (DNIS)—except for FXO. With FXO, you must apply specific configuration changes to route calls because there is no dialed number delivered by the PSTN.

Call Agent Routing Decisions

Call routing decisions based on PSTN numbers are done by the call agent you deploy with Cisco Unity Express. This section summaries considerations for Cisco CME and Cisco CallManager.

Cisco CME

With Cisco CME, call routing is done on the router using the Cisco IOS dial-peer feature. With this implementation, you have the router can perform digit manipulation and use features like private line automatic ringdown (PLAR) to direct PSTN calls to destinations, such as the AA pilot number. If you have FXO trunks, use a PLAR configuration to autoterminate PSTN calls onto the AA (3100 is the AA pilot number). The following example illustrates the PLAR configuration:

```
voice-port 1/0/0
  connection plar-opx 3100
```

Cisco CallManager

The digits delivered by the PSTN are passed on to Cisco CallManager's dial plan, and routing decisions are implemented there. Under normal operation, PSTN calls are routed to Cisco CallManager, and Cisco CallManager redirects the call to the appropriate destination. You can route PSTN calls to Cisco CallManager by using H.323, SIP, or MGCP, and this configuration must be present on the router. For FXO ports, the same PLAR statement given in the preceding example can be used to direct the PSTN calls to the H.323 or the SIP dial-peer pointing to Cisco CallManager.

If Cisco SRST is configured for the site served by the Cisco Unity Express AA, additional configuration is necessary to route PSTN calls during SRST operation (when Cisco CallManager is out of contact). This configuration is similar to the Cisco CME configuration (a SIP dial-peer routes calls into Cisco Unity Express). If Cisco CallManager uses H.323 or SIP to control PSTN calls, ensure that the

SIP dial-peer to Cisco Unity Express is of a lower preference than the Cisco CallManager dial-peers, such that this fallback dial-peer is only selected when Cisco CallManager (the primary dial-peer) is unavailable.

Digit Manipulation of the Pilot Number

The PSTN number called to reach your business is most likely a longer number than the extension associated with the Cisco Unity Express pilot number. For example, your PSTN number might be xxx.yyy.3100 and the AA pilot number is defined as 3100. When the full number xxx.yyy.3100 is delivered to the Cisco Unity Express AA, the number is not recognized and the call is not accepted because the dialed number does not match the configured pilot number (the call hears overflow tone).

There are two ways to configure your system to route calls to two or more numbers to the Cisco Unity Express AA:

- The call agent can do the appropriate digit manipulation and deliver only a fixed number of digits to Cisco Unity Express.
- You can associate multiple pilot numbers with the Cisco Unity Express AA (this is further described in the "Single or Multiple AA Pilot Numbers" section on page 62.

The following example shows a Cisco CME configuration where the call agent (Cisco CME router) translates the PSTN number xxx.yyy.3100 to extension 3100 before delivering it to Cisco Unity Express. In this configuration, Cisco Unity Express has only a single pilot number (extension 3100) associated with the AA. A similar function can be done by translating numbers on Cisco CallManager before the number is delivered to Cisco Unity Express.

```
voice translation-rule 10
 rule 1 /xxxyyy3100/ /3100/
 rule 2 /xxxyyy3105/ /3105/
 rule 3 /xxxyyy3106/ /3106/
!
voice translation-profile to_cue
 translate called 10
!
dial-peer voice 3101 voip
 description VM-AA-PSTN
 translation-profile outgoing to_cue
 destination-pattern xxxyyy31..
 session protocol sipv2
 session target ipv4:a.3.229.128
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
```

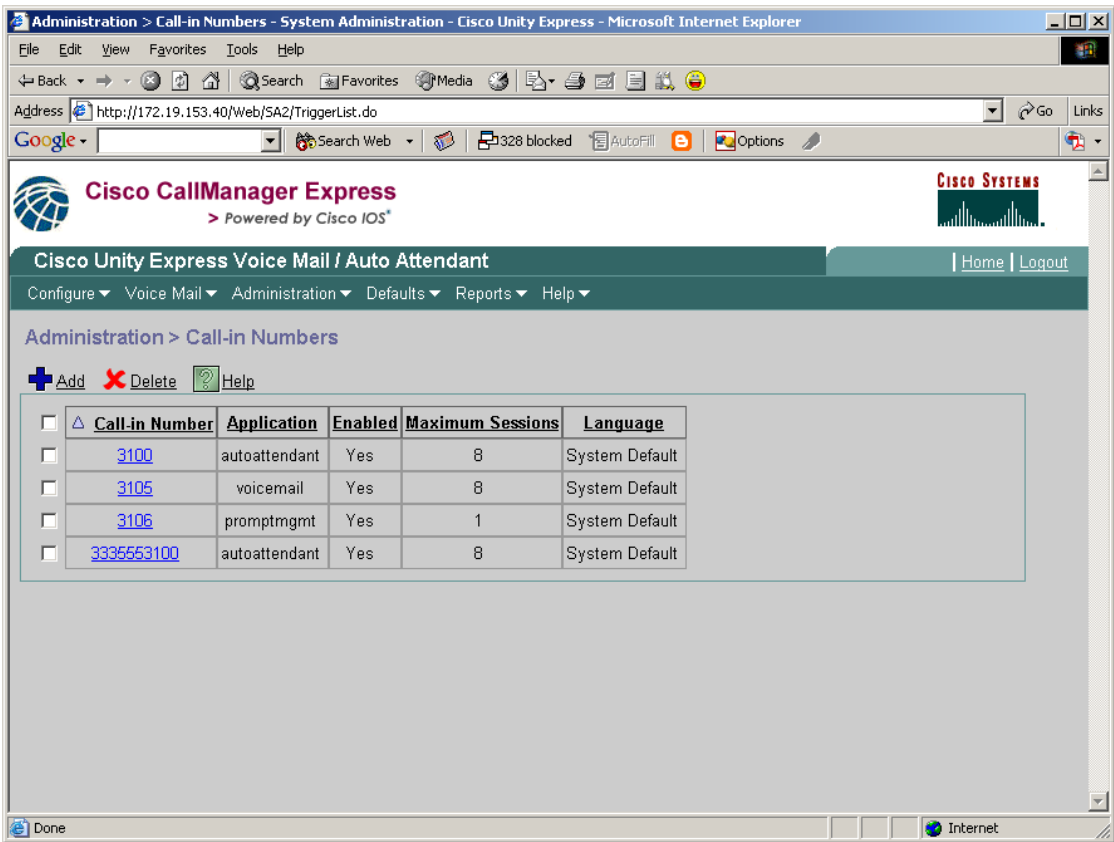
The following example depicts an alternative configuration where the call agent (Cisco CME) passes calls to both numbers that are unchanged for Cisco Unity Express. The Cisco Unity Express AA has multiple pilot numbers that are configured, so that both numbers match the AA entry point. Again, you can configure Cisco CallManager in a similar manner to route calls to both numbers.

```
dial-peer voice 3100 voip
 description VM-AA
 destination-pattern 31..
 session protocol sipv2
 session target ipv4:a.3.229.128
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
dial-peer voice 3101 voip
```

```
description VM-AA-PSTN
destination-pattern 333yyy31..
session protocol sipv2
session target ipv4:a.3.229.128
dtmf-relay sip-notify
codec g711ulaw
no vad
```

Figure 13 shows Cisco Unity Express 2.1 configured with 3100 and 333.yyy.3100 associated with the Cisco Unity Express system AA. Together with a routing configuration for Cisco CME (such as the preceding example) and equivalent configuration on a Cisco CallManager, calls to both numbers reach the Cisco Unity Express AA menu.

Figure 13 Cisco Unity Express AA Multiple Pilot Numbers



127742

AA or Receptionist

Many small businesses require that PSTN calls be answered by a receptionist—rather than an AA—during normal business hours because the human interface to customers is often very important to a small-medium business model, or to a branch office of an enterprise.

The first decision you have to make is how calls should be routed into your business. The choices include (but are not limited to) the following:

- All calls are always routed to the AA.

- All calls are always routed to a receptionist (in this case Cisco Unity Express is used only as a voice mail application).
- Calls during business hours are routed to the receptionist and after hours to the AA.
- Calls are routed first to the receptionist and if not answered within a few rings, then redirected to the AA.
- Different PSTN numbers are available to callers, one of which is your main business number and calls to this number are routed to the receptionist while the other PSTN number is for information only. Calls to this number are routed to the AA where location, address, fax numbers, hours of operation, and various other static pieces of information about your business are given to the caller.
- You have DID service for some employees, and those calls are routed directly to their extensions while all other PSTN calls are routed as per the previous bullets.

If you decide to use both a receptionist and the Cisco Unity Express AA to handle some portion of your calls, there are several considerations to take into account.

Topics addressed in this section include the following considerations:

Receptionist Configuration

There are several possible configurations to have the receptionist answer calls during business hours while the Cisco Unity Express AA takes calls when the receptionist is not available.

CFB and CFNA the Receptionist to the AA

Call forwarding can be accomplished in a number of ways. The easiest is to set up your system by using the Call Forward All (CFA) feature to route PSTN calls to a receptionist's extension (instead of to the AA as described in the "Routing PSTN Calls to the AA" section on page 47). Add this configuration by using the Call Forward Busy (CFB) and Call Forward No Answer (CFNA) features to reroute calls to the AA pilot number that are intended for the receptionist extension. In this configuration, calls route to the AA when the receptionist is busy, or is not able to answer.

The side effect of this configuration is that the receptionist cannot have voice mail. The receptionist's phone is set up for use the CFNA and CFB features (rerouting calls to AA) and cannot use CFNA and CFB to route calls to voice mail (which is a common alternative configuration).

CFA the Receptionist to the AA

Refining the configuration in the"CFB and CFNA the Receptionist to the AA" section on page 51 to allow voice mail for the receptionist, you can have the receptionist press the CFA button on the phone at the end of the day and call forward all calls to the AA pilot. The configuration of the phone can then be set to CFNA and CFB to voice mail. However, this configuration means that the receptionist has to remember to CFA calls manually at the end of each day, and undo it each morning, as well as call forwarding to voice mail for the receptionist is only available during business hours (CFA takes precedence over CFNA and CFB).

Separate Receptionist Extension

Another way to adjust the configuration to allow the receptionist to have voice mail is to use a generic extension for the receptionist that is separate from the employee's personal extension. For example, User1 has a personal extension 3001 and User2 has extension 3002. The "receptionist" extension is 3050. All non-DID PSTN calls are routed to 3050. The receptionist's extension 3050 appears as button 2 on both User1 and User2 phones, while both personal user extensions appear on button 1. The personal extensions (3001 and 3002) CFNA and CFB to voice mail (pilot number 3105), while the "receptionist" extension 3050 CFNA and CFB to the AA pilot 3100. This configuration (using Cisco CME as the call agent) is shown in the following example:

```
! SIP dial-peer to direct calls to AA (3100) and voice mail (3105)
!
dial-peer voice 3100 voip
 description VM-AA
 destination-pattern 31..
 session protocol sipv2
 session target ipv4:172.19.153.37
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
! Personal extensions for User1 and User2; CFNA and CFB to voice mail at 3105
ephone-dn  1
 number 3001
 description User1
 name User1
 call-forward busy 3105
 call-forward noan 3105 timeout 10
!
ephone-dn  2
 number 3002
 description User2
 name User2
 call-forward busy 3105
 call-forward noan 3105 timeout 10
!
! Receptionist extension, CFNA and CFB to the AA at 3100
ephone-dn  42
 number 3050 secondary 408yyy3050
 description Receptionist
 name Receptionist
 call-forward busy 3100
 call-forward noan 3100 timeout 20
 hold-alert 30 originator
!
! User1's phone with 3001 on button 1 and 3050 on button 2
ephone  1
 username "User1" password user1
 mac-address 0009.B7F7.5793
 button  1:1 2:42
!
! User2's phone with 3002 on button 1 and 3050 on button 2
ephone  2
 username "User2"
 mac-address 0002.FD06.D959
 button  1:2 2:42
```

Call-Agent Time-of-Day Routing

Time-of-Day (ToD) routing of calls to a receptionist (in contrast to the AA) requires a ToD routing feature on your call agent. With Cisco CME, this can be done by using a Tool Command Language (TCL) 2.0 script named “Time of Day Routing and Barring” that is available on Cisco.com Developer Support Central under TCL 2.0 technologies (this page requires a login). This feature is also available with Cisco CallManager Release 4.1.

Dial-by-Name to Groups

You can reach group and personal extensions via the AA dial-by-number feature or via a receptionist. You cannot reach groups, however, via the Cisco Unity Express AA dial-by-name feature—only personal names can be reached. Reaching a group by name therefore requires one of the following call routing alternatives:

- A receptionist.
- The caller to know the extension that is associated with the group.
- A custom AA menu that leads the caller through the available group choices (for example “Press 1 for Sales, 2 for Support”) and transfers the call appropriately using dial-by-number.

Receptionist Transfer to Voice Mail

A call that arrives at the AA and subsequently redirected to the chosen extension (by dial-by-number or by dial-by-name) can be forwarded to voice mail if the extension is not answered or is busy. The same The receptionist can do the same thing. If a PSTN caller calls for User1, the receptionist looks this up in a directory to determine that User1 is at extension 3001 and transfers the call to 3001. If User1 is not available, the call CFNA and CFBs to voice mail and enters User1’s voice mailbox. The mailbox greeting played by the Cisco Unity Express voice mail system is determined by the last redirected number field, in this case set to 3001, in the call information given by the call agent to Cisco Unity Express.

However, the receptionist may wish not to transfer the call to the User1 extension and have it ring there, but instead transfer it directly into voice mail. If a PSTN caller calls for User1 at 3001, and the receptionist transfers the call to the voice mail pilot at 3105, the caller hears the receptionist’s voice mail greeting as the last redirected number field in this call flow is set to the receptionist’s extension.

Note It is recommended that if a receptionist is used to front PSTN calls, that calls are transferred to the actual desired extension and not directly to the voice mail pilot number.

Cisco Unity Express (up to Cisco Unity Express 2.1) does not have a feature for direct transfer to voice mail. Workarounds depend on the call agent (Cisco CME or Cisco CallManager) that you are using with Cisco Unity Express.

Directory Information

The user or extension directory information that is available to the Cisco Unity Express AA versus the receptionist may be different. The Cisco Unity Express AA dial-by-number feature does not consult any directory information at all; instead, it processes the digits entered by the caller. The Cisco Unity Express dial-by-name feature uses the built-in Light Weight Directory Access Protocol (LDAP) directory within Cisco Unity Express, so only extensions associated with users (and not with groups) and their associated names are accessible via the AA dial-by-name feature.

These users do not need to have mailboxes assigned to show up in the Cisco Unity Express LDAP directory, the configuration requires only a user definition and valid First Name and Last Name fields as shown in the following example, illustrating a user profile and name configuration for AA Dial-by-Name.

```
cue# show user detail username User1
Full Name:           User
First Name:          User
Last Name:           One
Nickname:            User
Phone:               3001
Phone(E.164):        444yyy3001
Language:            en_US
cue-2691#
```

A receptionist is likely to use either a printed list of extensions (employees and groups), the directory Cisco CME provides on the display of the IP phone, or some other online directory application you may have in your office. The phone-based Cisco CME directory feature uses its own database, possibly from an XML server, and does not use Cisco Unity Express's LDAP information, so the entries can potentially be different (depending on how the configuration of the system was done, and which fields' values are manually coordinated).

Distributed and Centralized AA

If you have already decided that your business will be using an AA, and you have multiple sites in your network, one of the key network design decisions you must make is whether your AA will be centralized at one site or distributed.

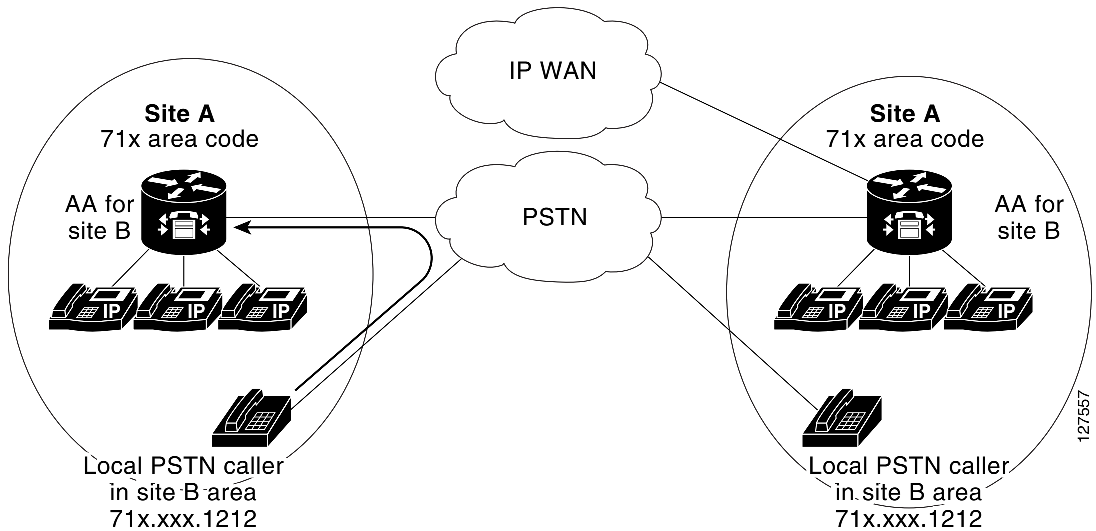
Topics addressed in this section include the following considerations:

- Distributed AA, page 54
- Centralized AA, page 55
- Hybrid Model, page 57

Distributed AA

Cisco Unity Express is designed as a per-site system and therefore provides the best fit for a distributed deployment model where each site has its own local AA and voice mail. Figure 14 depicts a distributed AA model in which local PSTN calls enter each site through trunks at that site. These calls are routed to the Cisco Unity Express AA at each individual site and are redirected to employees who typically also reside at that site.

Figure 14 Distributed Cisco Unity Express AA



This model works well if you have a local presence in each geographic area where you have an office and publish local PSTN numbers to your customers in that area. When customers call, they want to conduct business with an employee in the local site and to obtain the PSTN number from a local phone directory or a website posting specific to your branch's location. These are likely to be local PSTN numbers (either within the local area code, or toll-free type numbers of limited geographic coverage).

If you have a multi-site business and have a national (or large geographic area coverage) toll-free number for general customer service enquiries, these calls are typically delivered to one particular location by the PSTN, and the AA at that site can be set up to handle those calls or transfer them to other locations as required. If the Cisco Unity Express AA is set up to transfer calls out to another site, you can choose to route calls via VoIP between the sites or via the PSTN—depending on the configuration of the call agent. The Cisco Unity Express AA sees only the dial-string (such as the caller presses 1 and the call transfers to a configured number of yyy.1212) and does not know how the destination number translates to a call setup path (VoIP or PSTN).

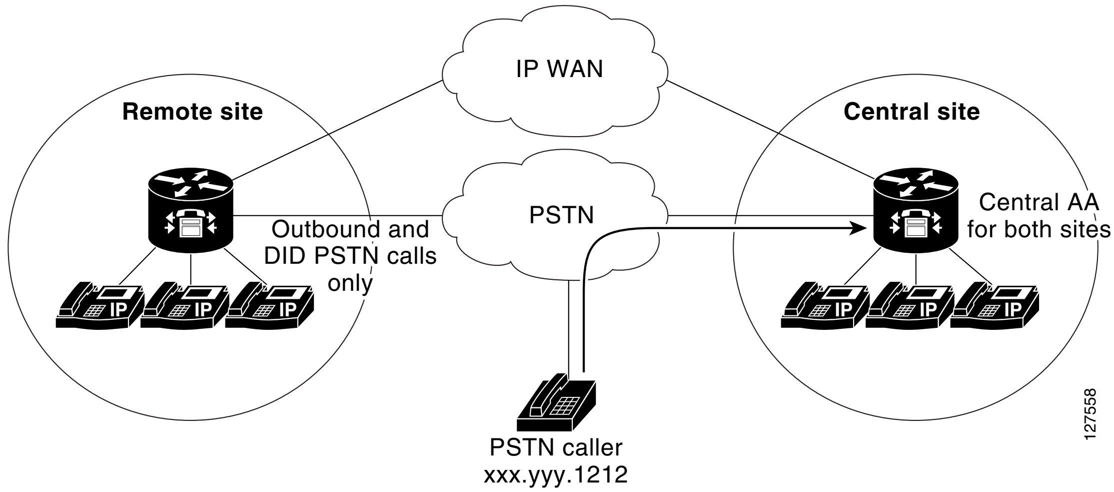
Centralized AA

With a centralized AA for all the sites, you might want to consider Cisco products other than Cisco Unity Express, which is not designed to serve as a "centralized" solution for multiple sites. Instead, it is designed to be a local AA for a standalone site, or a distributed AA (as per the "Distributed AA" section on page 54) where each site's Cisco Unity Express AA serves only users and calls at that site.

However, if you have already decided that Cisco Unity Express is the best product for your business (for other feature or product reasons) and you must have only a single AA across multiple sites, the design considerations for this are elaborated in this section.

A centralized AA model is shown in Figure 15. In this scenario, all non-DID PSTN calls to your business enter at one location, even if the call is ultimately destined to an employee at a different location (such as Site B in Figure 15).

Figure 15 Centralized Cisco Unity Express AA



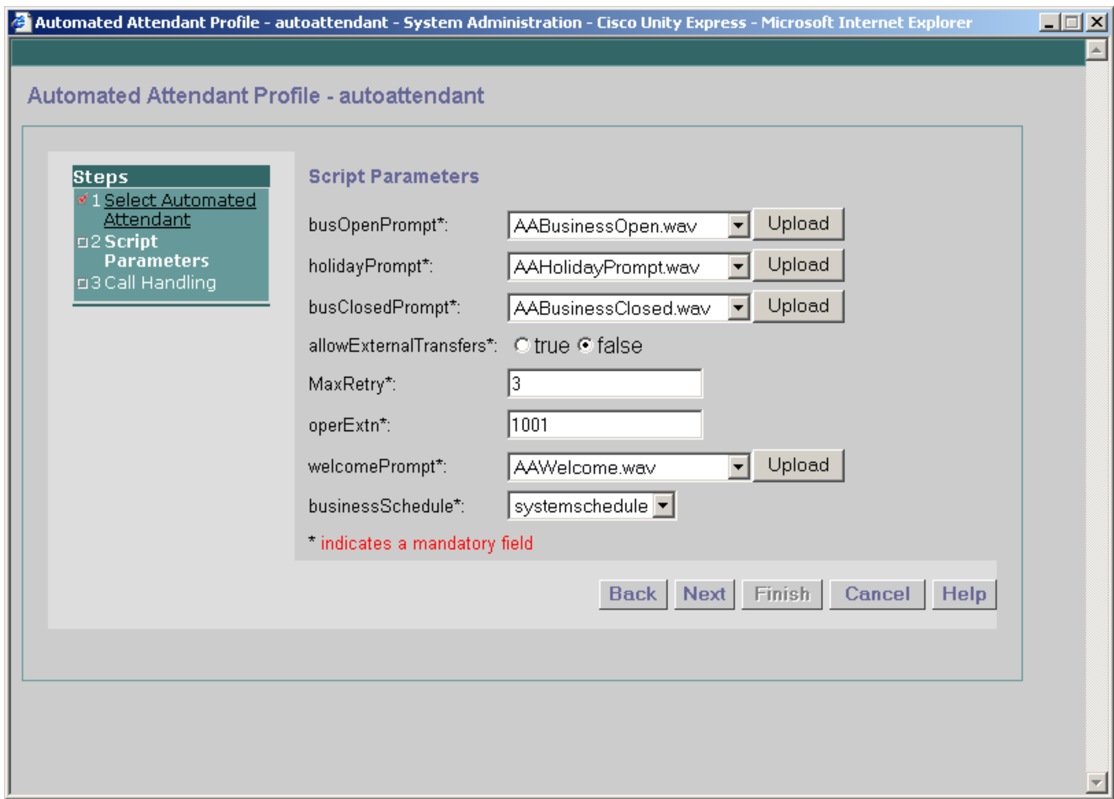
Considerations for this design include the following:

- Dial-by-extension can be configured to reach any VoIP extension or PSTN location in your network. By writing your own custom AA script, you can restrict or allow any numbers you choose. You can also block (or allow) certain destinations on your call agent (Cisco CME or Cisco CallManager).
- Dial-by-name in the AA contains only the names of the users entered locally on the Cisco Unity Express system hosting the AA. Dial-by-name is not available for users defined at remote locations, unless a separate user definition for them is inserted at the central site as well (in addition to the definition in the remote site) so that their names appear in the central AA's LDAP directory, and there are associated extensions that the AA can access to transfer the call. On the call agent, these extensions are then routed to the appropriate site where the IP phone is resident.
- If both the central and remote sites have Cisco Unity Express installed (in this scenario, Cisco Unity Express at a remote site is only used for voice mail), and you desire the central dial-by-name configuration, also consider that there is no automatic database synchronization between sites. If you make a user name change on a remote site or add a user, you must manually reflect that same change in the central site's configuration, or the AA dial-by-name capability will be unaware of this new information.
- If you desire the central dial-by-name configuration, also consider that the number of user definitions on Cisco Unity Express is limited. In current releases of software (up to Cisco Unity Express 2.1), this limit is twice the number of mailboxes in the license. For example, if you have a 100-mailbox Cisco Unity Express license installed on your central Cisco Unity Express system, you can enter a maximum of 200 user definitions (to support dial-by-name access).
- The AA functionality in Cisco Unity Express is not licensed separately from the voice mail capability, so you have to purchase a voice mailbox license, even if you intend to use only the AA capability. If you plan to use only the dial-by-extension AA capability, then the smallest mailbox license (12 mailboxes) will suffice for the application. If you intend to use the dial-by-name AA capability, then review the previous bullet on the maximum number of user definitions and determine the appropriate mailbox license to purchase from that information.
- If you use the Cisco Unity Express system AA (as of Cisco Unity Express 2.1) as your central AA, the default operation is to allow transfers only to local extensions (extensions associated with users defined on the system hosting the AA). To allow external transfers (including PSTN locations and extensions at other sites), configure the system AA to allow these transfers as shown in Figure 16 (set the value of the *allowExternalTransfers* parameter). If you plan to use the "centralized" AA

scenario described in this section, it is recommended that you write a custom AA script to control which destination numbers may be allowed as transfer destinations from the AA (this is to contain possibilities of misusing your AA for toll fraud purposes).

- Cisco Unity Express can process only a limited number of simultaneous calls into the AA. Port capacity for the various hardware form factors, releases and licenses of Cisco Unity Express was covered in the "Chapter 3: Cisco Unity Express System Design Considerations" chapter. The maximum Cisco Unity Express 2.1 port capacity is 16.
- Users configured into the Remote Users directory (the Configure > Remote Users GUI window) of Cisco Unity Express are not available for AA dial-by-name. The remote user configuration is used solely for voice mail VPIM networking between sites.

Figure 16 System AA Transfer to PSTN



127743

Hybrid Model

The "Distributed AA" section on page 54 and the "Centralized AA" section on page 55 described distributed AA (every site has its own AA) and centralized AA (only a single site in the network has an AA) deployment scenarios. A more likely situation is a combination of the two scenarios in which each site uses its AA capability for locally originated PSTN calls into that site. For example, a national 800 number for general customer service queries—with all 800-number calls terminating on a single site's AA.

As discussed in the"Centralized AA" section on page 55, Cisco Unity Express is not designed to be a central AA capability, but can be leveraged to do this to some extent. The same preceding considerations for Centralized AA apply to any Cisco Unity Express AA used in a "centralized" manner, regardless of whether all PSTN calls or only some of them enter that site. As long as you only use the dial-by-extension capability, there are few considerations (most of them apply to dial-by-name AA capability).

Cisco Unity Express Time-of-Day Routing

There is often a need to route calls based on time of day. This requirement might apply to routing calls to the AA only during certain times of day (such as after hours) or to routing calls from the AA. Different prompts or information might be given depending on whether the business is currently open or closed.

Call-agent based routing calls *to* the AA based on time of day was discussed in the "Call-Agent Time-of-Day Routing" section on page 53.

You can set up routing calls *from* the Cisco Unity Express AA based on TOD is a feature introduced in Cisco Unity Express 2.1. Business schedules (**Voice Mail** > **Business Hours Settings**) and Holiday lists (**Voice Mail** > **Holiday Settings**). These routing calls can guide your system or custom AA prompts and call treatment.

AA Customization

Cisco Unity Express ships with a system AA (which cannot be deleted) and has the ability to accommodate up to five total AAs. The AA prompt flow for Cisco Unity Express 2.1 is as follows:

1. If alternate greeting active
   a. Play alternate greeting
2. Play welcome greeting
3. If holiday
   a. Play holiday greeting
   b. Else If business open
      Play business open greeting (empty by default)
   c. Else
      Play business closed greeting
4. To enter the phone number of the person you are trying to reach, press 1
5. To enter the name of the person you are trying to reach, press 2
6. To transfer to the operator, press 0

In addition to the system AA, Cisco Unity Express offers a Script Editor that allows you to write your own AA scripts, install these into the system, and build your own customized AA applications. Cisco Unity Express does not offer full Interactive Voice Response (IVR) capability—only AA capability. The Cisco Unity Express Editor supports a subset of the steps available in the Cisco CRS Editor (and some additional steps).

Topics addressed in this section include the following considerations:

- Considerations for Customizing the System AA, page 59
- Customizing the System Prompts, page 59
- Create a Custom AA, page 60
- AA Script and Prompt System Limits, page 61

Considerations for Customizing the System AA

The highlighted greeting fields in the preceding AA operational system flow are greetings you can record to be used with the system AA. There are also several more script variables that you can set to the appropriate values for your office. These include the following:

- Whether or not transfers to local extensions, or to all destinations are allowed (parameter allowExternalTransfers).
- The number of times the main menu is repeated if no, or erroneous, input is received (parameter MaxRetry).
- The operator extension where calls should be transferred if you choose 0 from the menu (parameter operExtn).
- The schedule that specifies the business hours for your office (parameter businessSchedule).

The following aspects of the system AA cannot be customized:

- Flow of the system AA.
- Menu choices (press 1 for…, press 2 for…).
- The welcome greeting is non-interruptible and must finish before digit input from a caller is acted upon.
- You cannot enter extension numbers without choosing an action from the menu.

If you find the system AA generally satisfactory for your purposes but want to adjust a few of the items above that cannot be customized, get a copy the system AA script, edit it to add the feature or operation you require and install it on Cisco Unity Express as a custom AA script. The system AA cannot be uploaded or copied from the Cisco Unity Express system itself, so the easiest way to get a copy of it is to use the "aa_sample1.aef" available on the Cisco Unity Express software CD.

Customizing the System Prompts

The Cisco Unity Express system prompts, used in both the AA and voice mail, cannot be rerecorded, replaced, or customized. Custom AA prompts can be rerecorded and replaced as needed.

Create a Custom AA

The following steps are necessary to write and activate a custom AA on a Cisco Unity Express system:

Note It's almost always easier to adjust an existing script than to write a new one—several sample scripts are available on the Cisco.com software center and on the Cisco Unity Express software CD.

Step 1 Ensure the Cisco Unity Express Script Editor is installed on your PC (if not, download it from Cisco.com Software Center).

Step 2 Open an existing script file that you want to modify or an empty file.

Step 3 Edit the script to your needs. Ensure that you define all the variables, and enter the values that you want to assign. Ensure all variables whose values you want to control from the Cisco Unity Express GUI are defined as parameters and are defined in the top-level script (if you have multiple scripts).

Note Parameters in subflow scripts do not appear on the Cisco Unity Express GUI window.

Step 4 Validate the script and fix any errors or warnings.

Step 5 Upload the scripts or scripts to Cisco Unity Express.

Step 6 Log in to the Administration via Telephony (AVT) interface and record the prompts.

Step 7 Rename the files to have descriptive names rather than the system-assigned names). Or record the prompts offline (format: G.711 u-law, 8 kHz, 8 bit, mono) and upload them to Cisco Unity Express.

Step 8 Choose **Voice Mail** > **Auto Attendant**.

Step 9 Select **Add**. Click your script file name in the Select Automated Attendant Script field. If your AA contains multiple scripts, enter the name of the top-level script. Ensure a descriptive name for your AA in the Application Name field. Click **Next**.

Step 10 Provide values for all the parameters shown on this page. If some parameters are missing, go back and edit your script to export all the appropriate variables as parameters. Upload the changed script to Cisco Unity Express and repeat Steps 5, 8, 9 and 10. Click **Next**.

Step 11 Assign a pilot number in the Call-in Number field. Click **Finish**.

Step 12 Ensure that your call agent has the correct configuration to route calls to this pilot number to Cisco Unity Express (on Cisco CME this is a SIP dial-peer, on Cisco CallManager this is a CTI route point). Ensure that digit manipulation is done such that Cisco Unity Express sees a number that matches its pilot number (such as in a case in which the PSTN number is 4xx.yyy.1212 and the pilot number in Cisco Unity Express is defined only as 1212, the call agent must do digit manipulation before delivering this call to Cisco Unity Express).

Step 13 Make a test call to the new AA and ensure it operates the way you want. If you want to test the AA out before taking live calls, then first associate a pilot number with the new AA that is known only to you. Once satisfied with the AA's operation, change the pilot number to the number where PSTN calls arrive at your business.

AA Script and Prompt System Limits

The Cisco Unity Express system limits the following AA related attributes:

- Up to five total AAs with a maximum of four custom AAs and one system AA
- A maximum of eight (on an NM) or four (on an AIM) custom scripts
- No specific limit on the number of steps per AA
- No specific limit on the number of nesting levels within each AA script (although a script with too many levels becomes difficult to manage)
- A maximum of 50 (on an NM) and 25 (on an AIM) custom prompts
- A maximum of one MByte file size per prompt (two minutes)

System scripts and prompts do not count against the preceding limits.

Language Customization

Cisco Unity Express language settings affect the system prompts for the AA and voice mail. These language settings do not affect your custom prompts. You can write a custom AA that has multi-lingual prompts (menus) and queries the caller for preferred language. Based on the selection, the remaining prompts in that branch of the AA can be recorded in the applicable language. A multi-lingual AA flow might be as follows:

Play Welcome Greeting [bilingual]

1. For English press 1, for Spanish press 2 [same instruction repeated in Spanish]
2. If English
   a. To enter the phone number of the person you are trying to reach, press 1
   [rest of the of the menu]
3. If Spanish
   a. [Same prompt as above, but recorded in Spanish]
   [rest of the Spanish part of the menu]

To implement this AA you do not need language support or any special language settings on Cisco Unity Express. The system is unaware of the content of any custom prompts; they are .wav files. However, if a caller selects the Spanish branch of the menu structure and hits an error or a timeout (which results in a system prompt played to the caller), the system prompt is played in the default language installed on Cisco Unity Express.

System prompts can not be rerecorded or replaced. Up to Cisco Unity Express 2.1, only a single language selection per system is supported. While it is possible to craft multi-lingual custom AAs, the system prompts are unilingual until such time as Cisco Unity Express supports multiple concurrent languages.

Script Validation

The Cisco Unity Express Script Editor includes a validation step that checks for syntactical and grammatical correctness in the script. It also checks cross references within the script for variables and labels. A script must validate cleanly before you can upload the script to Cisco Unity Express. However, the validation step does not perform the following tasks:

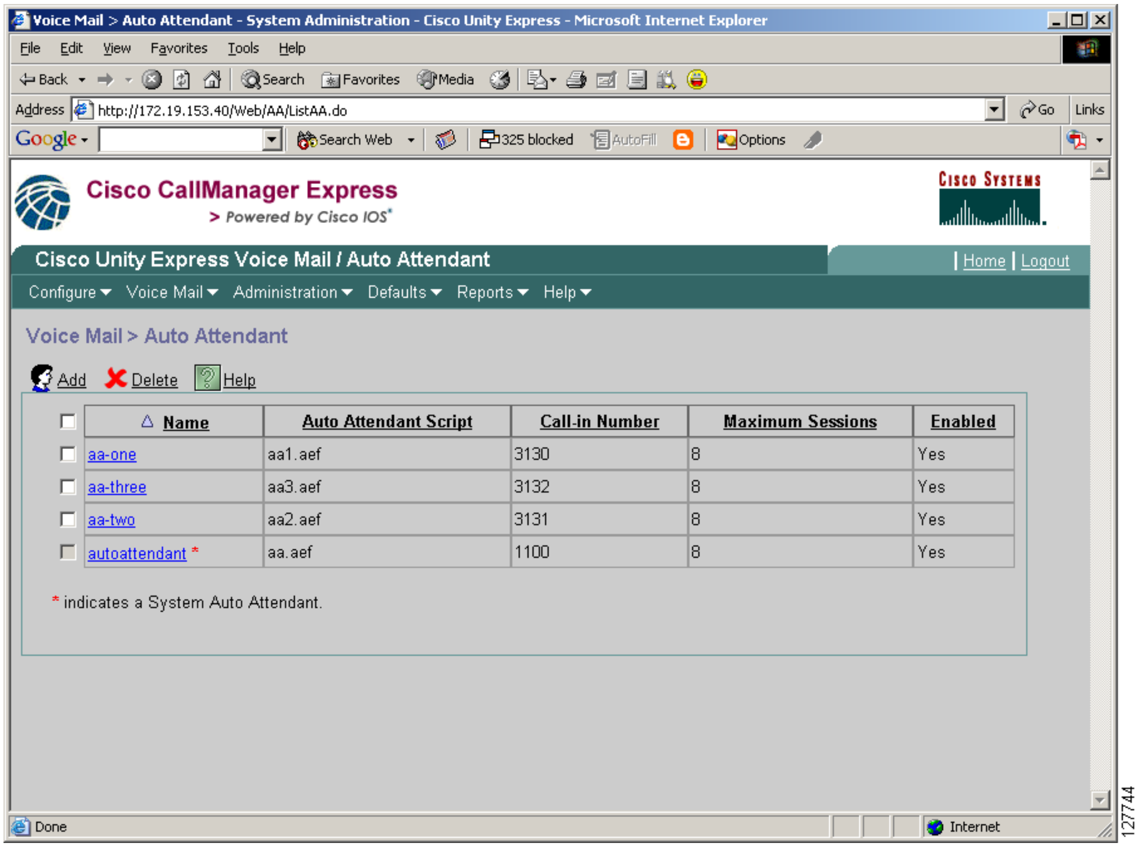
- Check the logic of the script
- Warn against run-time errors
- Check that subflows called by the script are present or defined

The run-time script flow can only be tested by uploading the script to Cisco Unity Express, associating a pilot number with the AA, and making calls through the system. Before you start doing this, ensure that all the subflows called by the script are also installed and present on Cisco Unity Express.

Single or Multiple AA Pilot Numbers

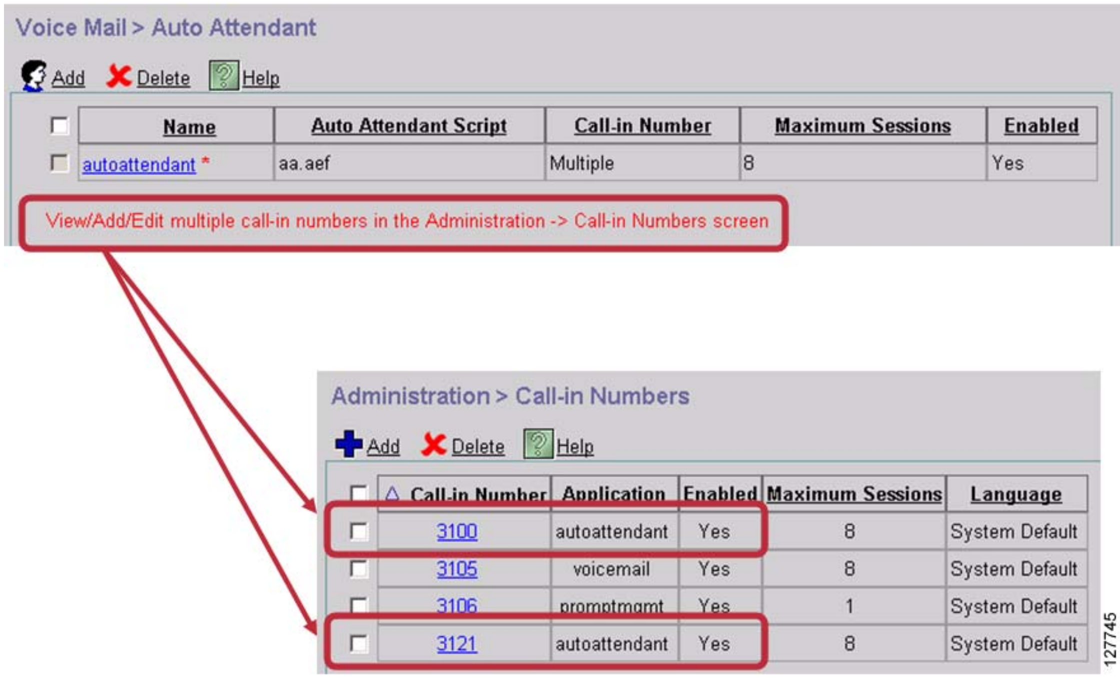
Typically a single pilot number is associated with the AA. If you define multiple AAs, then typically there is still a single (separate) pilot number associated with each of the individual AAs. See Figure 17. This scenario represents a situation in which there are multiple departments within a site. Each department has a specific PSTN number to which calls particular to the given department are sent and each department requires a distinct AA menu flow. For example, a stockbroker department may reside in a bank branch, but the normal bank business and the stockbroker business take place on different PSTN numbers. These departments just co-reside in the same building and share the same communications system. Two separate AAs, with separate pilot numbers would make sense for this situation.

Figure 17 Single Pilot Number for Each AA



While not a typical configuration, this type of configuration can have multiple pilot numbers associated with the same (or a single) AA. Within the AA script, a check for DNIS is made (to see which number was called) and call treatment or menu options are based on this information. Figure 18 illustrates a configuration where two separate pilot numbers (3100 and 3121) have been associated with the system AA. A situation where this makes sense is where the different pilot numbers may indicate different language preferences of callers. The AA flow is the same, so it is desirable to maintain a single script, but based on the DNIS (pilot number) called, the prompts may be given in language A or language B.

Figure 18 Multiple Pilot Numbers for the AA



This capability to associate multiple pilot numbers with a single AA script (system or custom) has always been available in the Cisco Unity Express CLI, but it has first become available in the GUI with Cisco Unity Express 2.1. The following example shows the CLI where multiple pilot numbers are associated with the same application. In this case, the system AA mirrors the configuration given in Figure 18.

```
ccn trigger sip phonenumber 3100
 application "autoattendant"
 enabled
 maxsessions 8
 end trigger

ccn trigger sip phonenumber 3105
 application "voicemail"
 enabled
 maxsessions 8
 end trigger

ccn trigger sip phonenumber 3106
 application "promptmgmt"
 enabled
 maxsessions 1
 end trigger

ccn trigger sip phonenumber 3121
 application "autoattendant"
 enabled
 maxsessions 8
 end trigger
```

Sample Scripts

It is easier to copy and adjust an existing script than to write one from scratch. Places from which you can download sample scripts include the following:

- The Cisco Unity Express software CD.
- The Cisco.com software center (from which you download Cisco Unity Express software).

In general, you should not use a script written by the CRS Editor, for example, the Cisco Unity Express script. The CRS Editor supports many more steps than the Cisco Unity Express Editor, and the Cisco Unity Express Editor might not be able to open a script written by the CRS Editor (depending on the content).

Recording Prompts

Recording AA prompts via the AVT Cisco Unity Express interface assigns an automatic system-chosen file name to the prompt, such as UserPrompt_01172005111156.wav that contains a timestamp. If you later log in to the AVT again, you cannot rerecord the contents of an existing file (the file name your script already refers to). You can record a new prompt to replace the existing prompt, and it will be assigned a new file name.

Rerecord Prompts via AVT with Cisco Unity Express GUI Access

Assume the prompt you want to rerecord is currently named greeting.wav. Use the following process to rerecord this prompt via the AVT if you have access to the Cisco Unity Express GUI from a computer:

Step 1 Log in to the AVT and record the changed prompt. The system assigns a new file name, such as UserPrompt_01312005121740.wav.

Step 2 Download file UserPrompt_01312005121740.wav to your computer and rename that file **greeting.wav**.

Step 3 Upload file greeting.wav from your computer to the Cisco Unity Express system (the upload operation automatically overwrites the existing file by the same name, so no changes to the script are required).

Step 4 Delete UserPrompt_01312005121740.wav from the **Voice Mail** > **Prompts** window (or via the CLI).

Rerecord Prompts via AVT without Cisco Unity Express GUI Access

Use the following process to rerecord this prompt via the AVT if you do not have access to the Cisco Unity Express GUI from a computer:

Step 1 Log into the AVT and record the changed prompt. The system assigns a new file name, such as UserPrompt_01312005121740.wav.

Step 2 To rename the file to **greeting-v2.wav**, use the **ccn rename prompt** CLI command on Cisco Unity Express 2.1.

Step 3 Navigate to the **Voice Mail** > **Auto Attendant** GUI window and click your AA application.

Step 4 Click **Next** to get to the Script Parameters window. Change the appropriate prompt variable to refer to greeting-v2.wav instead of greeting.wav.

Step 5 Delete greeting.wav from the **Voice Mail** > **Prompts** window.

Record Prompts Offline

Use the following steps for an offline recording method:

Step 1 Record the changed prompt and name the file greeting.wav.

Step 2 Upload file greeting.wav from your computer to the Cisco Unity Express system (the upload operation automatically overwrites the existing file by the same name, so no changes to the script are required).

Managing Custom Scripts and Prompts Across Sites

Even though a distributed AA (an AA in each site) might be the best fit for your organization, it might still be desirable to manage the scripts and prompts that comprise all the site AAs from a single central place. There is no facility in Cisco Unity Express itself to coordinate scripts and prompts between sites. There are no network management applications to do so, although this capability is likely to become available at some point from Cisco partner management solutions.

You can craft your own central management and storage application by using a Unix or Linux platform to issue CLI instructions against several individual Cisco Unity Express sites. Your application needs a scripting capability and the ability to open a Telnet session to each router that hosts a Cisco Unity Express. Issuing Cisco Unity Express CLI requires enable-mode login on the router, so the person who develops the application must be someone with access to these levels of security within your organization.

Identical AAs at all Sites

Consider a situation where your network has multiple Cisco Unity Express sites and the AA for each site is identical, including the business hours, the fax numbers, the prompts and the script flow. Assume that the AA application consists of the following two scripts and three prompts:

- main-aa.aef
- subflow-aa.aef

- welcome.wav
- bus-closed.wav
- fax-numbers.wav

Also assume that each Cisco Unity Express site already has a custom AA with a pilot number set up to point to script main-aa.aef (if this is not the case, then a one-time creation of a custom AA for each site is necessary, which you can do individually at each site, or via a CLI script of its own, issuing the AA creation commands to each site—this must only be completed once).

The above five files constituting your AA reside on the Unix/Linux application server in a directory on the disk. If you change anything to the script flow, or rerecord any of the prompts, you replace the files in this directory. You can run a script that does the following:

Step 1 Open a Telnet session to a Cisco Unity Express site.

Step 2 Log in to the Cisco Unity Express CLI interface.

Step 3 Upload the five AA files to Cisco Unity Express.

Step 4 Log out.

Step 5 Repeat Steps 1 through 4 for each Cisco Unity Express site in your network.

As long as the file names constituting the AA do not change, the above is all that is required. If the file names change (because you added more scripts or prompts, or because you desire to have version numbering included in the file name), updating each Cisco Unity Express system requires a few more steps:

Step 1 Open a telnet session to a Cisco Unity Express site.

Step 2 Log in to the Cisco Unity Express CLI interface.

Step 3 Upload the five AA files to Cisco Unity Express.

Step 4 If the subflow script file name has changed, ensure the main script file refers to this new subflow.

Step 5 If the prompt file names have changed, adjust the script parameters to point to the new prompts.

Step 6 If the main script file has changed, adjust the script file name associated with the AA pilot number to point to the new script name.

Step 7 Log out.

Step 8 Repeat the Steps 1 through 7 for each Cisco Unity Express site in your network.

Note There is no versioning of scripts and prompts on Cisco Unity Express itself. If a file with the same name is uploaded, the current file of that name is overwritten. You can only retrieve the old version of the file if you have done a backup while that was the active file in the system. If so, you can now do a restore. Performing a restore operation restores *all* the files on the system, not just the script and prompt files, and all changes to the system, including mailbox content, are lost and reset back to the state it was in at the last backup.

Cisco Unity Express maintains a time/date stamp on each script/prompt file that you could use as some indication of versioning (**Voice Mail** > **Scripts** and **Voice Mail** > **Prompts** GUI windows, or **show ccn scripts** and **show ccn** commands in the CLI).

Different Business Hours Across Sites

If the AAs for all your sites are identical, but the business hours for some (or all) sites differ from each other, Cisco Unity Express can accommodated these differences independent of the AA scripts and prompts. When your office is open or closed is specified by the Business Hours schedule (**Voice Mail > Business Hours Settings**) of each individual Cisco Unity Express and this schedule can have the same name (a variable referenced from the AA script, such as *systemschedule*) at all sites, but different contents for each site individually. The AA script may refer generically to the business hours schedule, but the Cisco Unity Express automatically picks up the time periods specified in the local system where the AA application runs.

Different Prompts Across Sites

If the AA is largely the same at all sites, but not identical, you can manage the files centrally. However, you must refine your management script. Assume the network has four sites, and the AAs across all the sites are identical, except for a prompt that contains the location (address and driving directions) of each site office. The files constituting the AA are the following:

- main-aa.aef
- subflow-aa.aef
- welcome.wav
- bus-closed.wav
- fax-numbers.wav
- location-site1.wav, location-site2.wav, location-site3.wav, location-site4.wav

The same scripting application that was described earlier in this section can be used, but include the following additional configuration accommodations:

- Be aware of which site a script is logged in to, and upload only the appropriate location-xx.wav file to each site.
- Set the script parameter (which is a generic variable value as this is a shared script across all sites) to point to this particular prompt (this setting is different for each site).

Coordinating AA Updates by Time

Another advantage of the centrally managed scripting application is that it is easier to coordinate AA changes across sites than leaving the changes up to an individual administrator at each site. For example, if a new welcome greeting must become active next Monday, then this prompt can be prerecorded, placed in the application server directory, and the scripting application can be scheduled to execute Sunday night at midnight to roll out the updated AA prompt to all your sites.

Dial-by-Extension

A key part of the system AA (and a subflow of several of the sample scripts on Cisco.com that you can use to customize AA operation) contains the dial-by-extension AA functionality. This subflow is usually executed after a prompt of the form "To enter the phone number of the person you are trying to reach, press 1…". The caller selects this from the menu and follows it by a varying number of digits terminated by a #, and the script acts on the digits entered by transferring the call.

Topics addressed in this section include the following:

Internal and External Destinations

Up to Cisco Unity Express 2.0, the system AA allowed for the transfer calls to any destination—it treated the destination merely as a string of digits, and any call dialable on the associated call agent would succeed. To limit the destinations to which the AA can transfer calls (such as no calls to the PSTN), the call agent's features—such as Class of Restriction (COR) on Cisco CME—were required.

As of Cisco Unity Express Release 2.1, the system AA has a parameter to control whether calls are allowed to transfer only to internal numbers (default operation), or to internal and external numbers. Your own custom AA scripts can employ similar mechanisms to limit the valid destinations of calls. The system AA script parameter was shown earlier in Figure 16 (the value of the *allowExternalTransfers* parameter).

An internal number is considered to be an extension that exists in Cisco Unity Express's LDAP directory. Information that appears in LDAP includes all extensions defined and associated with a user (**Configure** > **Users**) on Cisco Unity Express. This does not include remote user (**Configure** > **Remote Users**) definitions entered on Cisco Unity Express for networking spoken name confirmation (these are not stored in LDAP). The validity of a destination number is independent of extension length or dialing plans and is not coordinated with your call agent's dial plan on what might be local extensions versus remote extensions.

Cisco Unity Express considers an extension that appears in an LDAP entry an internal destination. External destinations include everything else, such as the following:

- All other extensions that exist at the local site, but do not appear in the Cisco Unity Express configuration, such as local phones/extensions that do not have mailboxes.
- All VoIP destinations, such as extensions present at other sites, but a PSTN call is not required to reach them.
- All PSTN destinations.

If you want to refine the destinations that the Cisco Unity Express AA can transfer calls to, you have to limit calls either on the call agent (with features such as COR), or write a custom Cisco Unity Express AA script that does the checking based on your requirements (such as perhaps extension length, or numbers starting with certain sequences such as 9).

Script Control on Transfer

The method Cisco Unity Express uses to transfer a call varies depending on the associated call agent, and this in turn means the AA script operation is different.

- Cisco CME—Cisco Unity Express (up to and including 2.1) uses a SIP Bye/Also sequence to transfer a call from the AA. This means Cisco Unity Express hands off control of the call to the call agent (blind transfer) before the success or failure of the transfer is known. There is no means to get control back into the script. Once the call is transferred, the call will get whatever treatment Cisco CME provides (busy tone, overflow tone, ringback, and the like). If your script tests on failure cases after a transfer (Call Redirect step), these code segments will never execute.
- Cisco CallManager—Cisco Unity Express uses a JTAPI sequence to transfer a call, and the actual call is transferred by Cisco CallManager. If failures occur (busy or non-existent destination), the call is still within control of the Cisco Unity Express AA script and failure code segments following the transfer (Call Redirect step) statement in the script will execute.

Dial An Extension at Any Time in the AA

You can write a custom AA script that does not enforce a menu choice before a caller is able to dial an extension. By default, Cisco Unity Express system AA requires that you select a menu item before the extension number of a destination employee is entered. As an alternative, you can write a custom AA script that offers the behavior where an extension number (if known by the caller) can be dialed at any time, and at the same time that the caller can select from menu items offering choices other than dialing an extension. such as an AA prompt.

Writing a script that dials an extension number without a menu prefix requires knowledge of your dial plan. For example, assume that your extensions area all in the 2xxx format. Menu items starting with digits other than 2 present no problem. A menu item starting with 2 can be handled as follows:

- When the caller presses 2, proceed to a collect digits state without presenting another prompt, in this case 3 more digits to complete the extension.
- If 3 more digits are received, prepend a 2 to the number, and transfer the call to the extension.
- If no more digits are received (and a timeout occurs), assume menu item 2 was selected, and proceed to the next menu level or prompt.

For more information, see the following URL:

- http://www.cisco.com/en/US/products/sw/voicesw/ps5520/products_tech_note09186a008041d950.shtml

Dial-by-Name

A second key part of the system AA and a subflow of several of the sample scripts on Cisco.com that you can use to customize an AA, contains the dial-by-name AA functionality. This subflow is usually run after a prompt. The caller spells the name, and the script provides matches based on information stored in LDAP for users defined on the Cisco Unity Express system.

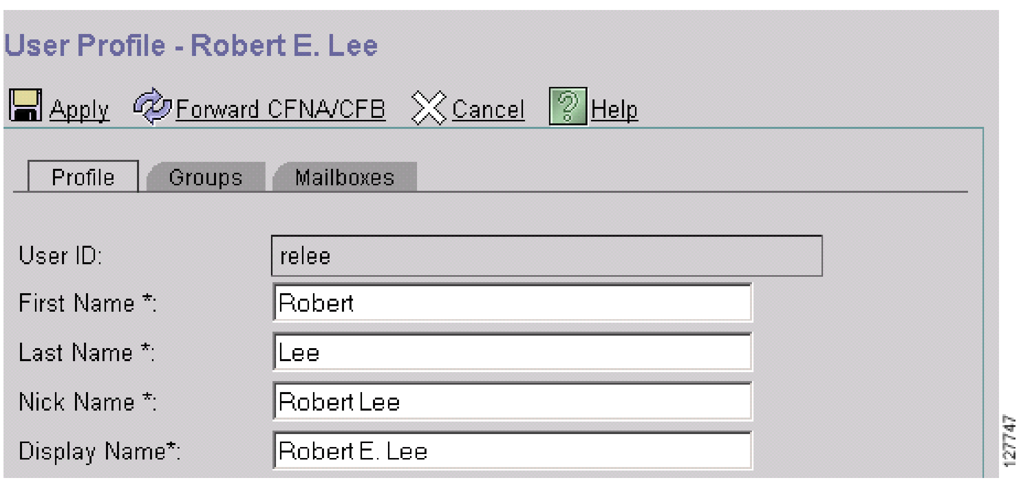
Topics addressed in this section include the following considerations:

- Name Fields Used in Dial-by-Name, page 71
- Customize Last and First Name Sequence, page 72
- Set Up AA for Dial-a-Group, page 72
- Dial-by-Name to Non-Users, page 73

Name Fields Used in Dial-by-Name

For users (not groups), the dial-by-name AA function uses a last name, first name approach. Use the similarly named fields in the **Configure** > **Users** configuration shown in Figure 19.

Figure 19 User Configuration for Dial-by-Name



If you are using Cisco CME as your call agent, the Cisco CME CLI username (see the following example configuration) is not used for dial-by-name, and the configuration of this field has no impact on the Cisco Unity Express LDAP directory used for Cisco Unity Express's dial-by-name function.

The following example depicts configuration of the Cisco CME username field:

```
ephone  13
 username "relee"
 mac-address 1111.2222.3366 button  1:3
```

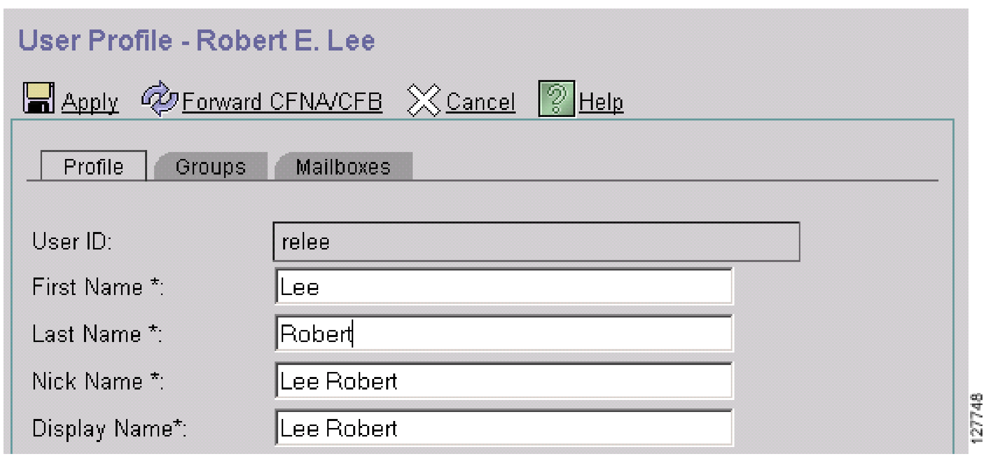
Customize Last and First Name Sequence

Cisco Unity Express's dial-by-name function matches the Last Name, and if not unique, the dial-by-name function proceeds to match the First Name field. This sequence cannot be changed or customized. If you want is to match the First Name, then the Last Name, the fields in the configuration must be reversed.

For example, Robert (first name) Lee (last name) works for the company. Figure 20 depicts that the dial-by-name matches Lee (the last name in the configuration), and then Robert (the first name in the configuration).

If you want to match "Robert" first, followed by "Lee" in the dial-by-name application, then configure "Robert" as the last name and "Lee" as the first name, as shown in Figure 20. This configuration has no side effects on the system as these fields are passive and are not used to control anything else (such as Caller ID, phone displays, or login names).

Figure 20 User Configuration for Dial-by-Name



Set Up AA for Dial-a-Group

The Cisco Unity Express AA searches LDAP only for user definitions, so group definitions (such the Customer Service or Sales departments) cannot be accessed via the dial-by-name function of the AA. To reach someone in a particular department of your organization, implement dial-a-group functionality into the AA menu itself. For example: "Welcome to XYZ company, for Customer Service press 1, for Sales press 2, if you know the extension of the person you wish to reach press 3, to dial by name press 4…"

Selecting 1 from this menu must (in the custom AA script you write) transfer the call to the extension associated with the Customer Service group. This extension in turn must CFNA and CFB to voice mail, so the caller can leave a message in the General Delivery Mailbox (GDM) if the call is not answered.

Note The Cisco Unity Express AA and the voice mail send function both access a dial-by-name directory based on the system's LDAP content. The AA function searches only users, while the voice mail send function searches both users and groups within LDAP.

Dial-by-Name to Non-Users

There might be employees in your office who do not need a voice mailbox, but require the ability to be reached using the dial-by-name feature via the Cisco Unity Express AA. If so, these employees can be entered in the Cisco Unity Express system (as users) without having mailboxes assigned to them. By virtue of the Cisco Unity Express user definition (and associated extension and phone), these employees appear in the Cisco Unity Express LDAP database and therefore are recognized by the Dial-by-Name AA function.

These users do not have a mailbox defined, and therefore do not count against the Cisco Unity Express license (the license counts mailboxes, not users).

Note The number of users allowed to be defined on the Cisco Unity Express system is derived from the number of licensed mailboxes, and is currently set to two times the number of mailboxes. If a 12-mailbox license is installed on the Cisco Unity Express system, a maximum of 24 users can be defined.

Additional AA Topics

This section addresses a number of additional AA-related topics. Topics addressed in this section include the following:

- Cisco Unity Express AA as a Contact Center Front-End, page 73
- Using Cisco Unity Express as a Standalone AA, page 74
- Reaching Voice Mail via the AA, page 75
- Cisco Unity Express AA and Cisco CME Basic Automatic Call Distribution AA, page 75
- AA Reports, page 75

Cisco Unity Express AA as a Contact Center Front-End

Cisco Unity Express does not offer a full-fledged IVR—it offers only AA functionality. For some contact center applications, this may be sufficient as there is a significant overlap between AA and IVR system features. The Cisco Unity Express AA can be used as the IVR front-ending a contact center application, as long as you do not require any of the following types of features:

- Database access for storing or retrieving customer information.
- Checking the existence or content of files.
- Reporting menu selections and call flows through Cisco Unity Express AA.
- Reporting abandoned calls.
- Returning control of a call to the IVR menus if agents log out or choose not to answer calls ringing on their phones.
- Initiating outgoing calls from the IVR (calls can be transferred by the Cisco Unity Express AA but not initiated).
- Authenticating a caller based on a PIN.
- Any email or HTTP interaction with other server, or applications.
- Connecting music on hold while the call is waiting in queue.

- Checking on agent status while the call is still in the IVR queue.
- Coordinating window information based on digits the caller keyed in via DTMF in response to a menu item.

Cisco Unity Express AA offers the following features and if these are sufficient for your needs, then you can leverage the AA to act as a front-end for your contact center application:

- Customizable (and rerecordable) greetings
- Any number of greetings or announcements with customizable timeouts between them
- Loops with repeated (interruptible and non-interruptible) announcements
- Transfer of a call to a queue or an extension number (the AA script gives up control of the call at this point)
- The option to leave a voice mail instead of speaking to an agent
- Passive information (information not dynamically updated based on a database query, but periodically updated by rerecording the voice prompt) such as address, business hours, driving directions and fax numbers

Using Cisco Unity Express as a Standalone AA

Cisco Unity Express is designed to offer a combined AA and voice mail application. However, if you only want to use the AA and not voice mail component, Cisco Unity Express can be installed for the sole purposes of leveraging its AA functionality. There are some considerations in such a design:

- As addressed in the "Centralized AA" section on page 55, the AA functionality in Cisco Unity Express is not licensed separately from the voice mail capability, so you must purchase a voice mailbox license, even if you intend to use only the AA capability. The size of the mailbox license depends on what you want to do with the AA. If you plan only dial-by-extension menu items, then the smallest (12-mailbox) license is sufficient. If you plan to use the dial-by-name functionality, then you have to configure user definitions with the names on Cisco Unity Express. The number of users is currently double the number of mailboxes in the license.
- You must configure a call agent. Cisco Unity Express cannot be used without either Cisco CME or Cisco CallManager as the call agent. It is not sufficient to install Cisco Unity Express on a router and enter a dial peer to get calls into Cisco Unity Express AA.
  - If you use Cisco Unity Express as a standalone AA with Cisco CallManager, the configuration is exactly the same as if you were using both the AA and voice mail, so follow exactly the same steps as you would for a normal system setup. You do not have to define the pilot number by Cisco CallManager because it will not be used.
  - If you use Cisco Unity Express as a standalone AA with Cisco CME, the telephony-services keyword must be enabled on the router, but no phones or extensions need to be defined. Additionally, the SIP dial-peer redirecting calls into the Cisco Unity Express AA must exist on the router. No other Cisco CME functionality is required.
  - If you use Cisco Unity Express entirely without a call agent, the Cisco Unity Express Initialization Wizard does not allow you to proceed to the point of getting the system online as it requires contact with a call agent (either Cisco CME or Cisco CallManager) to proceed. You could bypass the Initialization Wizard and configure Cisco Unity Express for the AA to work via the CLI. Because you cannot use a GUI on such a system, the GUI comes up with a blanket window showing "Lost Contact with the call agent" whenever you log in. Using Cisco Unity Express without a paired call agent is an experimental, untested, and not recommended configuration. However, this setup works—with configuration entirely via the

CLI—insofar as high-level, proof-of-concept testing for this guide was done. The recommended configuration is to purchase the smallest Cisco CME license and install Cisco Unity Express with Cisco CME on your router.

- Cisco Unity Express can process only a limited number of simultaneous calls. Port capacity for the various hardware form factors, releases, and licenses of Cisco Unity Express was described in the "Chapter 3: Cisco Unity Express System Design Considerations" chapter. Cisco Unity Express 2.1 port capacity varies between 4 and 16.

Reaching Voice Mail via the AA

A typical configuration contains separate PSTN phone numbers for different Cisco Unity Express pilot numbers, such as the AA, voice mail, and the AVT. Each service can be called independently by employees of your business. However, if you have a configuration in which you have a single PSTN number (such as yyy.1212) for your business, you can use the Cisco Unity Express AA to redirect calls to voice mail (for message retrieval) or the AVT (for system administration).

Calls to your main business number (yyy.1212) are terminated on the Cisco Unity Express AA (such as pilot number 3100). PSTN callers who wish to reach voice mail to check their messages (such as pilot number 3105) can dial 3105 from the dial-by-extension menu in the Cisco Unity Express system AA (or a similar menu item in a custom AA).

To enable this capability (if Cisco Unity Express is deployed with Cisco CME), ensure that the *allowExternalTransfers* script parameter in the system AA is set to allow external transfers. The voice mail and AVT pilot numbers are not considered internal numbers as they are not extensions associated with users. See the script parameter in Figure 16.

If Cisco Unity Express is deployed with Cisco CallManager, use the "xfermailbox.aef" system script to enable the ability to reach voice mail via the AA, as described in the Tech Tip at the following location:

- http://www.cisco.com/en/US/products/sw/voicesw/ps5520/products_tech_note09186a00802ab979.shtml

Cisco Unity Express AA and Cisco CME Basic Automatic Call Distribution AA

The basic automatic call distribution (ACD) functionality in Cisco CME 3.2.1 includes a small AA application. This is useful particularly for Cisco CME customers who do not also have Cisco Unity Express installed. However, if you do have Cisco Unity Express installed on your Cisco CME, and you use the basic ACD function of Cisco CME, you have to craft the two AAs carefully to enable the correct call flows for your business.

AA Reports

Cisco Unity Express does not provide any reports currently (up to Cisco Unity Express 2.1) on call traffic through the AA. By using CDRs, you can tell how many calls terminated on the AA, but there is no way to report peg counts on the menu items within your AA.

Best Practices

In summary, the following best practices apply to the Cisco Unity Express AA:

- Determine if the Cisco Unity Express system AA is sufficient for your business needs (a small amount of customization can be done on the system AA). If not, a custom AA script must be developed.
- If you plan to use a receptionist or attendant to answer most of your business calls and use the AA only as a backup mechanism, plan your call flows carefully (especially voice mail access for the receptionists).
- Use Cisco Unity Express 2.1 or later releases as that introduces two key AA features: setting up business hours schedules and a list of holidays to check against.
- If you develop a custom AA script, test the flow thoroughly with test calls to determine whether the script operates per your requirements before allowing live calls to terminate on the AA. The validation step in the Cisco Unity Express Editor does only syntactical checking, not logic flow checking.
- All parameters whose values you want to control through the Cisco Unity Express GUI must be specified in the top level AA script. Parameters in subflow scripts cannot be accessed via the GUI.
- If you rerecord a prompt, make sure that the script refers to the correct file name to pick up the new content of the prompt (the TUI does not replace prompts; it adds new ones).
- If you record AA prompts on an offline system, ensure that they are in the correct format. Cisco Unity Express does no error checking on the format of uploaded .wav files. Incorrectly formatted prompts will simply not play out, or not play correctly.

Chapter 5: Voice Mail Design Considerations

This chapter focuses on Cisco Unity Express voice mail design considerations, including space allocation to mailboxes, setting up (and using) different types of mailboxes, and setting up a message waiting indictor (MWI). Some AA features are also described that can help you design your voice mail system. For an in-depth discussion specific to the Cisco Unity Express AA features, see "Chapter 4: Auto-Attendant Design Considerations."

The Cisco Unity Express voice mail design considerations addressed in this chapter are presented in the following sections:

Voice Mail Pilot Number Operation

The Cisco Unity Express voice mail application has a single entry point number (pilot number) for all types of calls. A caller can presented with a mailbox login prompt or with a greeting to leave a message, depending on how the call is directed to the voice mail pilot number. Specifically, it depends on the content of the "redirected number" field in the call setup message that enters Cisco Unity Express.

If the "last redirected number" field *is* present (which means the call terminated to an extension first and was subsequently redirected to the voice mail pilot via a call forward feature), the following rules are applied:

- If the extension in the "last redirected number" field has a mailbox, Cisco Unity Express assumes that it is a call-forward from the subscriber's phone and the mailbox's greeting is played to the caller.
- If the extension in the "last redirected number" field has no mailbox, then the call is transferred to the "Voice Mail Operator" extension after an announcement. The default setting for the "Voice Mail Operator" is the AA pilot number, but you can change this to any extension (use the **Voice Mail** > **Call Handling** GUI window).

If the "last redirected number" field *is not* present (which means the caller dialed the voice mail pilot number directly), then Cisco Unity Express assumes that the subscriber is calling into voice mail to retrieve messages and the subscriber login prompt is played and the following rules are applied:

- If the caller (the "calling number" field) has a mailbox on the system, then the caller is prompted to enter a PIN.
- If the caller (the "calling number" field) does not have a mailbox on the system, then the caller is prompted for an ID (extension) and a PIN.

Cisco Unity Express cannot be configured to enter a mailbox based on the "first redirected number" because this is not currently (up to and including Cisco Unity Express 2.1) a field provided to Cisco Unity Express by the associated call agent (Cisco CME or Cisco CallManager). If a call is redirected to Cisco Unity Express, the mailbox associated with the "last redirected number" field is entered.

Calling into Voice Mail to Retrieve Messages

Subscribers can call the voice mail pilot number to check messages from their desks by pressing the Messages button on their IP phones. How this button is programmed (mapped) with the voice mail pilot number depends on which call agent you are using.

- Cisco CallManager—The number dialed by pressing the Messages button is controlled by a system administrator programming the phone so that a Voice Mail Profile is attached to the Directory Number (extension) configuration for the phone. The Voice Mail Profile contains the pilot number called when the Messages button is pressed on the IP phone. This pilot number must be associated with a route point registered with Cisco CallManager by Cisco Unity Express.
- Cisco CME—The following example shows the voice-mail CLI setting within the **telephony-services** command configuration that controls the number automatically dialed (3105 in this example) when a subscriber presses the Messages button on an IP phone controlled by Cisco CME.

  The following configuration example illustrates the voice mail pilot number setting for Cisco CME:

  ```
  telephony-service
   load 7960-7940 P00305000300
   max-ephones 100
   max-dn 300
  .
  .
  .
  voicemail 3105
   max-conferences 8
  ```

- Cisco SRST—Cisco SRST uses similar CLI commands as that shown for Cisco CME in the preceding example, except that the **voicemail** command is a setting within the call-manager-fallback configuration.

If a subscriber calls to the voice mail pilot number from an assigned IP phone, the calling number field in the call setup matches the subscriber's assigned mailbox and Cisco Unity Express prompts only for a PIN to log in. If a subscriber calls from someone else's IP phone, Cisco Unity Express assumes the subscriber wants to log in to the mailbox that matches that phone's extension (provided a mailbox exists for the extension) and also presents just the PIN prompt. The subscriber can now press # on the phone keypad to force Cisco Unity Express to present the User ID prompt to permit logging in to a specific mailbox from any phone.

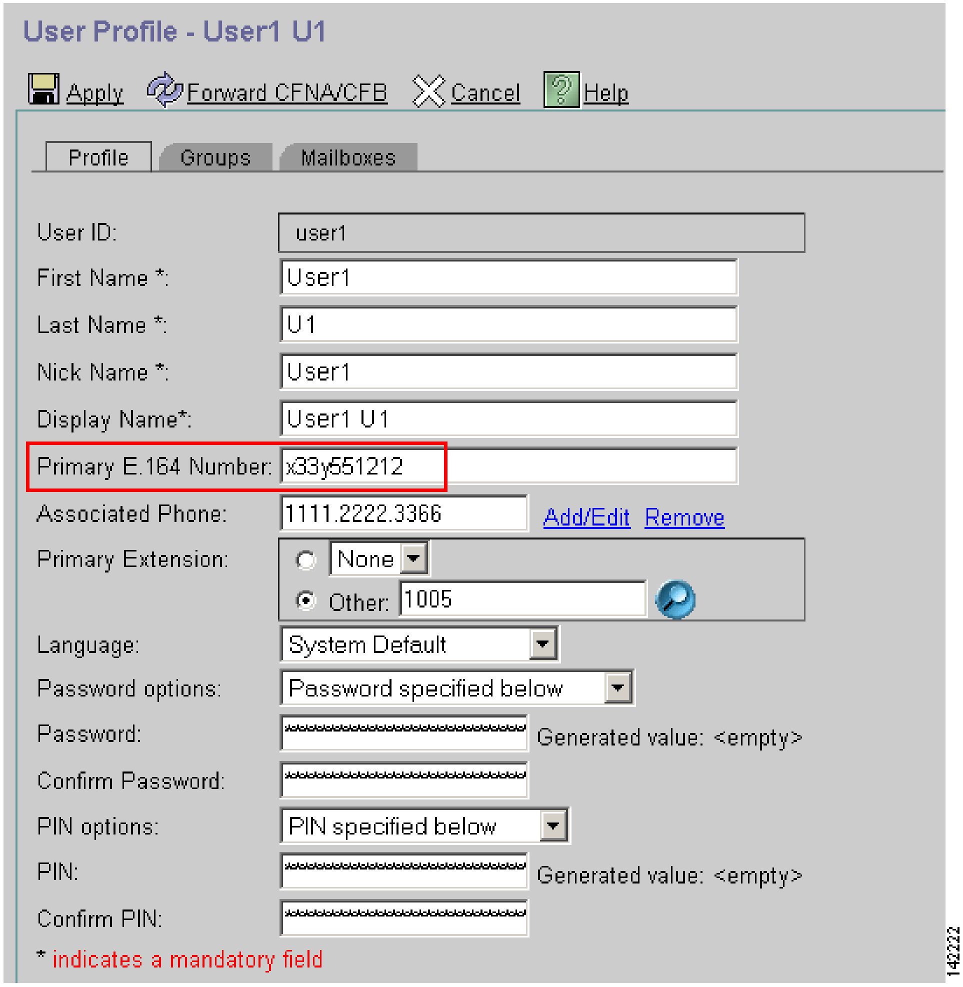
You should also consider how your employees call into voice mail from PSTN locations to retrieve messages. You can have either a separate (dedicated) PSTN number for this specific purpose (which is routed to the voice mail pilot number), or these calls can use your main business number (and therefore terminate on the AA). If you choose to terminate calls at the AA, you must redirect calls to voice mail via the AA menu by dialing the voice mail pilot number as an extension.

If a subscriber wants to call in to check voice mail from any off-net location (such as home or a cell phone) and to be presented only with the PIN login menu (and not the User ID followed by PIN login menu), then Cisco Unity Express must recognize the caller ID delivered with the PSTN call and be able to map that to a mailbox on the system. This call flow requires the following:

- The PSTN must deliver caller ID to your location.
- You must associate a secondary number (the PSTN phone number) with the mailbox in addition to the extension.

You can associate a secondary number with a Cisco Unity Express mailbox by setting the Primary E.164 Number field in the user's profile to this number as shown in Figure 21.

Figure 21 Associating a Secondary Number with a Mailbox



Note The arrangement illustrated in Figure 21 is not the typical use of the Primary E.164 Number field in the user profile. Typically this field is used to map the subscriber's DID number to a mailbox so that PSTN calls to the extension correctly forward to voice mail. In the example configuration in Figure 21, User1 U1's extension is 1005; User1's DID number is x44y551005; and User1 U1's cell phone number is x33y551212. You can use the Primary E.164 Number to either route DID calls (x44y551005) to User1 U1's mailbox, or to allow User1 U1 to call in to retrieve voice mail and bypass the mailbox User ID prompt by setting this field to his cell phone number (x33y551212). You cannot do both. If it is more important to have the DID number mapped, then calling in from User1 U1's cell phone will require stepping through both the User ID and the PIN prompts. If it is more important to bypass the User ID prompt, then the DID number must be changed to the extension (converting x44y551005 into 1005) by the PSTN voice gateway, Cisco CME, or Cisco CallManager digit manipulation features before the call enters Cisco Unity Express and is matched to a mailbox.

Mailbox Operation

This section addresses various aspects of voice mailbox operation and configuration that allow you to customize Cisco Unity Express's features to the best advantage for your business, and to integrate Cisco Unity Express mailboxes with the rest of your network. Cisco Unity Express offers all the basic expected features of a voice mail system, and these are not described individually. Please refer to Cisco Unity Express feature documentation for descriptions of supported features and their operation.

The following mailbox operational considerations are presented in this section:

Associating Multiple Extensions with a Mailbox

Up to two numbers can be associated with a mailbox:

- Primary extension—For a Cisco CME system, this is an extension configured on the system and exists as an **ephone-dn** command statement in the Cisco CME configuration. For a Cisco CallManager system, this is a free-form field and no cross-checking is done between Cisco Unity Express and Cisco CallManager to ensure that it matches a valid extension on Cisco CallManager (although this is the intended use of the field).

- Primary E.164 number—This is any secondary number that you intend to associate with the mailbox. Its primary use is to map the subscriber's DID number to the mailbox so that calls arriving from the PSTN can enter the mailbox unaltered. As described in the "Calling into Voice Mail to Retrieve Messages" section on page 78, it can also be used for voice mail retrieval functionality; DID numbers can go through digit manipulation to match the extension before entering the Cisco Unity Express mailbox.

When a call arrives at Cisco Unity Express, the "called" (for leaving a message) or "calling" (for retrieving voice mail) number is compared with these two fields. If either one of them matches, then the mailbox is recognized at the destination for this call.

If you intend to map more than two numbers to a mailbox, you must use the digit manipulation features on the router, Cisco CME, or Cisco CallManager to adjust the number to one of the Primary Extension and Primary E.164 Number fields before the call reaches Cisco Unity Express.

Phone Types Supporting Mailbox Implementation

Cisco Unity Express 2.1 provides mailboxes for SCCP-controlled IP phones managed by either Cisco CME or Cisco CallManager.

Voice mail for analog phones is not supported when the analog phone is connected behind H.323, Media Gateway Control Protocol (MGCP), or SIP-controlled voice-gateway foreign exchange station (FXS) ports. With these three gateway configurations, there is no direct way to complete the following tasks:

- Forward (busy or no-answer) a ringing call on an FXS port to voice mail without the help of a call agent or some other call routing intelligence—such as a Tool Command Language (TCL) script.
- Enable MWI for the analog phone.

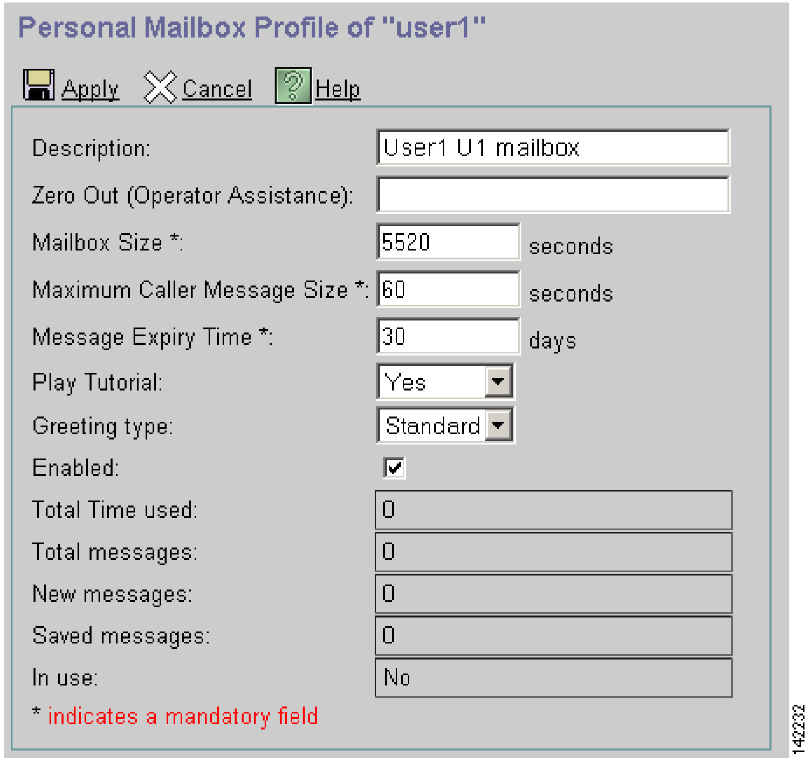
Voice mail for analog phones connected behind SCCP-controlled voice gateway FXS ports is supported in Cisco Unity Express 2.1, because these ports appear as IP phones to the system. Such ports use stutter dial tone for MWI (created by the FXS voice gateway, not directly by Cisco Unity Express).

Voice mail for general-purpose SIP phones is not supported in Cisco Unity Express 2.1, due to the lack of RFC 2833 DTMF relay support in Cisco Unity Express. Calls to SIP phones can be deflected to a Cisco Unity Express system, and direct SIP calls can be made to a Cisco Unity Express AA or voice mail pilot number. The caller cannot interact with Cisco Unity Express via DTMF, so there is no way for the subscriber to retrieve the message or a caller to interact with the AA menus.

Users and Subscribers

A mailbox belongs to a user (or subscriber). A mailbox cannot be defined without first defining a user profile. The user profile contains the extension number, the secondary phone number (Primary E.164 Number field), and the PIN used for mailbox login. A mailbox is associated with the user profile, which in turn is associated with an extension. There is no direct linkage between the mailbox and the extension. Therefore, the mailbox profile, shown in Figure 22, shows no extension number or PIN fields (these are contained in the associated user profile).

Figure 22 Personal Mailbox Profile



Note If a user profile is deleted from the system via the GUI, the associated mailbox is automatically also deleted. If the user profile is deleted from the CLI, the mailbox is not automatically deleted and must be deleted manually.

Although a mailbox cannot exist without a user profile, a user profile can exist without a mailbox. The Cisco Unity Express license installed on your system directly controls the number of mailboxes you can define. It indirectly also controls the number of users you can define. The number of users allowed is always larger than the number of mailboxes. In releases up to and including Cisco Unity Express 2.1 the number of users allowed is twice the number of mailboxes defined by the license installed on the system.

You might choose to define users that do not have mailboxes for the following reasons:

- To define system administrator accounts that do not need a mailbox or may not belong to the same organization. For example, the administrator might be an outsourced company that is not part of the end-user community served by the voice mail system.
- To define administrators (that do not require voice mail themselves) to manage group membership and distribution lists.
- To define usernames that show up in the AA dial-by-name feature but do not require voice mail.

Personal Mailboxes

A personal mailbox is typically used by one person and belongs to an individual subscriber. This person is typically the only one who knows the PIN of the mailbox and logs in to the mailbox to retrieve messages. As explained in the "Users and Subscribers" section on page 82, the user profile associated with the mailbox determines the extension, user ID, and PIN used for access to a personal mailbox. A personal mailbox can be associated only with a single User ID.

Multiple people can log in to a personal mailbox only if the same User ID and PIN combination is known to both of them, which is normally considered a security violation.

General Delivery Mailboxes

A general delivery mailbox (GDM) is typically used by multiple people (a shared mailbox) who work in the same functional group, such as the help desk or customer service. All members of the group can log in to the GDM (only one person can be logged in at any one time) and retrieve messages.

GDM Access and Login

A GDM is associated with a group profile in the Cisco Unity Express configuration and does not have a login user ID or a PIN associated. Members of the group gain access to the GDM by logging into their personal mailboxes first (where individual User ID and PIN authentication checks are done) and then following a voice menu choice that allows them to access specific group mailboxes—for groups to which they belong. Employees who are not members of the group cannot access the GDM.

An Example of GDM Use

An example of a typical use of a GDM is for a group of people who work in customer service. Callers do not generally know the individual's names, nor do they require this information. Although each member of the customer service group has a personal mailbox, the GDM is a collective mailbox for customer service queries where all staff members check for nonpersonal messages and any member can respond, depending on who is available or on shift.

Figure 23, Figure 24, and Figure 25 show such a configuration. The members and owners of the customer service group are defined in Figure 23. The GDM profile is shown in Figure 24. The group profile for the GDM is show in Figure 25.

Figure 23 Group Members and Owners

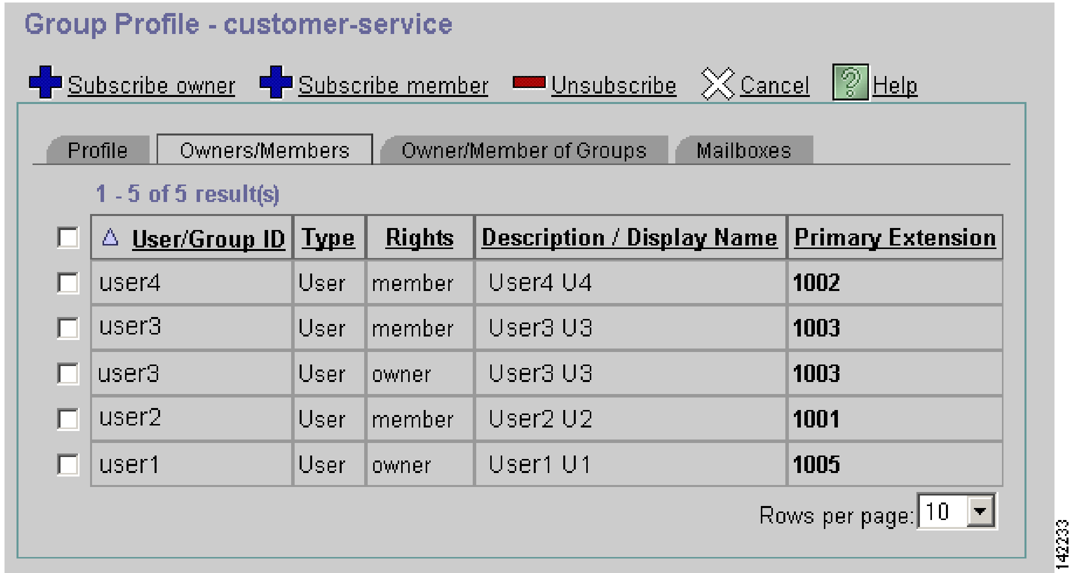
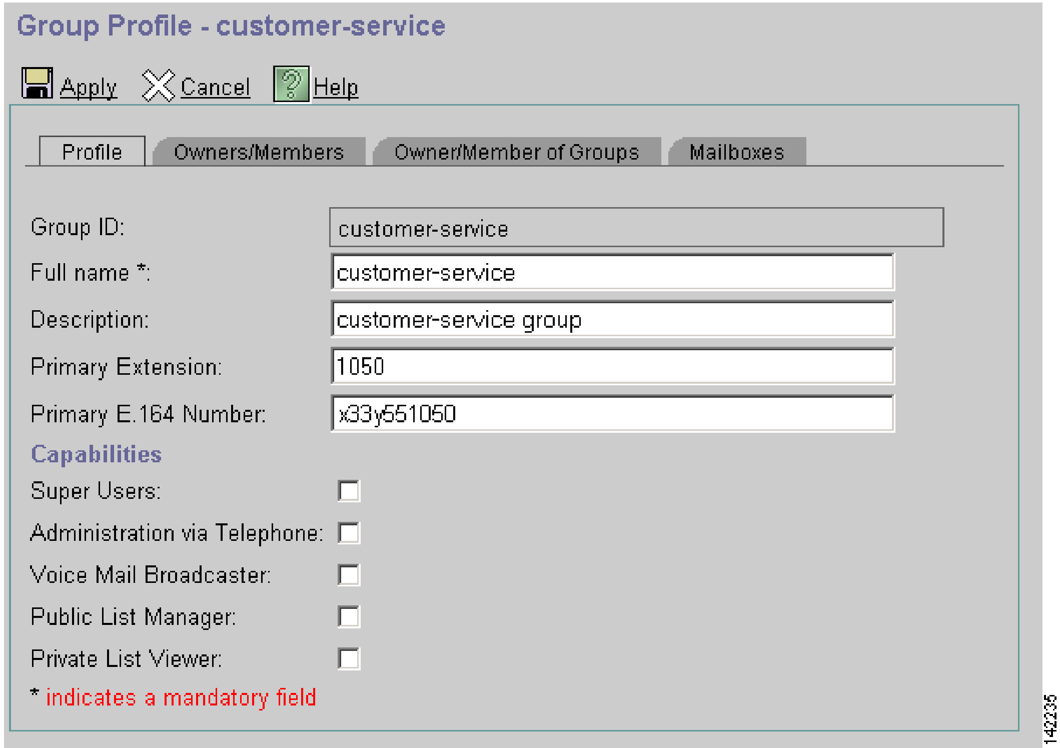


Figure 24 GDM Profile

Figure 25 Group Profile

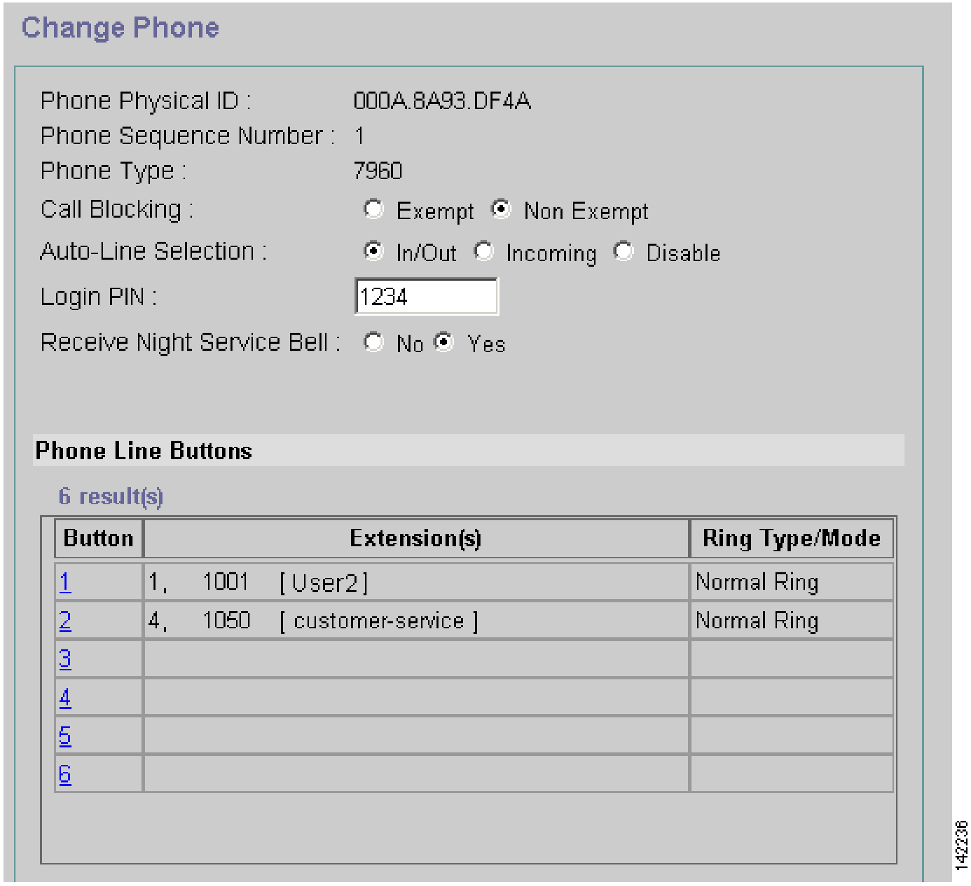


The extension (1050) associated with customer service—and with the group definition (customer-service)—is shown in the Group Profile in Figure 25. This is an extension different from the individual extensions of the members of the group and would normally appear as a secondary button appearance on their phones.

MWI for GDMs

Any phone with a button appearance of the extension associated with the group receives MWI for message content in the GDM. This configuration is shown in Figure 26. The customer-service GDM extension (1050) appears on button 2 of group member User2 U2's phone (extension 1001).

Figure 26 GDM Extension Appearance for MWI



Further information on MWI for GDMs is given in the "MWI Operation" section on page 104.

Number of GDMs and Personal Mailboxes

GDMs have no direct login, therefore a GDM can not generally be leveraged to increase the number of personal mailboxes on the system. All GDM members also require a personal mailbox definition because the login authentication happens via the personal mailbox (User ID and PIN). However, with Cisco Unity Express 2.1—where the number of personal mailboxes and GDMs becomes flexible (as long as the total number of mailboxes for the license is not exceeded)—different types of applications become possible.

One example illustrating the tradeoffs between GDMs and personal mailboxes is to define all mailboxes as personal mailboxes and define no GDMs. In this configuration, you have effectively leveraged your GDM allocation as personal mailboxes instead. If you have no need for GDMs, then you can define a number of mailboxes higher than the number allowed by the license (see Table 10) on your system.

Table 10 Cisco Unity Express Mailbox Licensing

License	Personal Mailboxes	GDMs	Total Mailboxes
12-Mailbox	12	5	17
25-Mailbox	25	10	35
50-Mailbox	50	15	65
100-Mailbox	100	20	120

In contrast to defining zero GDMS, you might define all (or almost all) mailboxes as GDMs. If you have a need only for GDMs (perhaps you are designing a temporary system to support a conference facility and various groups of staff members need to communicate via shared mailboxes, but no one requires any personally targeted voice mail), you could define all but one of the mailboxes on Cisco Unity Express as GDMs and a single personal mailbox. Provide the User ID and PIN of the single personal mailbox to all users for login access to the GDMs. Although it is possible to do this in the configuration, the side effect is that only a single person can be logged in to a mailbox at any one time, and because users all enter the system through a single personal mailbox, this configuration effectively reduces Cisco Unity Express to a single session access (no simultaneous access). If this is problematic for your application, you can define a few more personal mailboxes to allow some simultaneous access. The point remains that you can have far more GDMs than you require personal mailboxes (although the personal mailbox count can never be zero) if your situation is such that users can share knowledge of the PIN of a personal mailbox without creating security or privacy issues. If the number of personal mailboxes defined is less than the number of ports available on the system, then the lesser of the two numbers is the limit on the number of simultaneous voice mail logins you can achieve on the system. A personal mailbox must be defined with at least 10 seconds of storage space; it cannot be empty.

Note A GDM cannot be changed to a personal mailbox or vice versa. In other words, mailbox cannot be changed from being associated with a group profile to being associated with an individual user profile (or vice versa). To achieve this configuration change, the GDM must be a deleted and a new mailbox must be defined for the individual user (or vice versa). The contents of the deleted mailbox cannot be preserved, or transferred.

GDMs Only, but No Need for a Personal Mailbox

A user cannot have access to a GDM without also having a personal mailbox on the system. A user cannot have a personal mailbox without having a personal extension assigned. If the business environment is such that the user should have access only to a shared extension and its associated GDM, and is not to receive personal calls or personal voice mails, then the dial plan must be constructed to limit this access.

For example, the person works in the bakery of a small grocery chain and answers only calls to the bakery department, all outgoing calls are made from a payphone in the employee breakroom or a personal mobile phone. The bakery department’s extension 2005 appears on the phone in the bakery department and the bakery GDM is associated with extension 2005. The three employees who work shifts in the bakery have personal extensions 3001, 3002, and 3003, and each has a personal mailbox set to the minimum size of 10 seconds (this effectively prohibits anyone from leaving voice mail in this mailbox). Further, extensions 300x are not forwarded on busy or no-answer, and they do not appear as button appearances on any phones, thereby effectively prohibiting users from receiving and making calls from these extensions.

Members and Owners

A group profile contains both owners and members, as shown earlier in Figure 23. Members of the group have access to log into the GDM and retrieve messages. Owners have administrative access to change the membership of the group they own. Group owners cannot log into a GDM unless they are also defined as a member of the group, as is User U3 in the example shown in Figure 23.

Mailbox License Control

The license purchased with the Cisco Unity Express system generally indicates the number of personal mailboxes allowed on the system, as shown in the "Personal Mailboxes" column in Table 10. A number of GDMs are allowed by the license in addition to the number of personal mailboxes that appears in the license.

Until Cisco Unity Express 2.0, the number of personal mailboxes or GDMs allowed by the license was strictly controlled as given in the "Personal Mailboxes" and "GDMs" columns in Table 10. In Cisco Unity Express 2.1, only the "Total mailboxes" column is strictly controlled by the license and the system allows you to define any combination of personal mailboxes and GDMs as long as the aggregate number does not exceed the "Total mailboxes" column.

The number of mailboxes allowed by the license can be displayed in the Cisco Unity Express GUI and CLI, but cannot be changed through these interfaces. Changing a license requires the purchase of a new license and an installation of a new license package file onto the Cisco Unity Express system.

Voice Mail Customization

The items that a voice mail subscriber can customize on a Cisco Unity Express mailbox are as follows:

- Spoken name—This is blank on a newly installed system and can be recorded or rerecorded by the subscriber. Once recorded, it can never be deleted; it only can be changed. To delete the spoken name, delete the entire mailbox from the system.
- Greetings—Cisco Unity Express allows two greetings to be recorded per mailbox, a standard greeting and an alternate greeting. The subscriber chooses—via the telephone user interface (TUI) or the GUI—which of the two greetings is the current greeting for the mailbox. The current greeting is played to all callers regardless of whether they are internal or external callers, or whether the call arrived at voice mail by virtue of CFNA or CFB. Cisco Unity Express ships with a basic system greeting that is played to callers if the subscriber has not recorded any customized greetings. Once recorded, the customized greetings cannot be deleted, or reset to the system greeting. To achieve this result, the mailbox must be deleted and reinserted into the system. Greetings can be rerecorded at any time.

When an external caller accesses a mailbox to leave a message, the caller can bypass the outgoing greeting by pressing # on the phone keypad.

The elements or order of the header playout (when a subscriber retrieves a message) is fixed and cannot be changed or customized in Cisco Unity Express.

The Cisco Unity Express voice mail TUI conversation (the menus, options, and directions presented to the user when logged in to a mailbox) cannot be changed, resequenced, translated, suppressed, or customized.

Cisco Unity Express does not support a feature comparable to the "call handler" approach offered by Cisco Unity.

Cisco Unity Express offers a tutorial mode for newly defined mailboxes (see the “Play Tutorial” field in the mailbox profile shown in Figure 22). This tutorial walks the subscriber through setting up the mailbox (spoken name, greetings, and change PIN) with the first login. After the subscriber has worked through the tutorial, it is automatically deactivated. As the administrator of the system, you can suppress the tutorial for newly defined mailboxes if you do not want this functionality, or you can turn the tutorial back on for a mailbox that has already been set up.

Voice Mail Language Customization

The voice mail system prompts can use a custom language if the desired language package is installed on Cisco Unity Express. Only a single language at a time is supported; activation of multiple simultaneous languages is not available.

Fax Calls

Cisco Unity Express cannot terminate fax calls into a voice mailbox. Cisco Unity Express 2.1 provides a voice mail functionality only—not unified messaging.

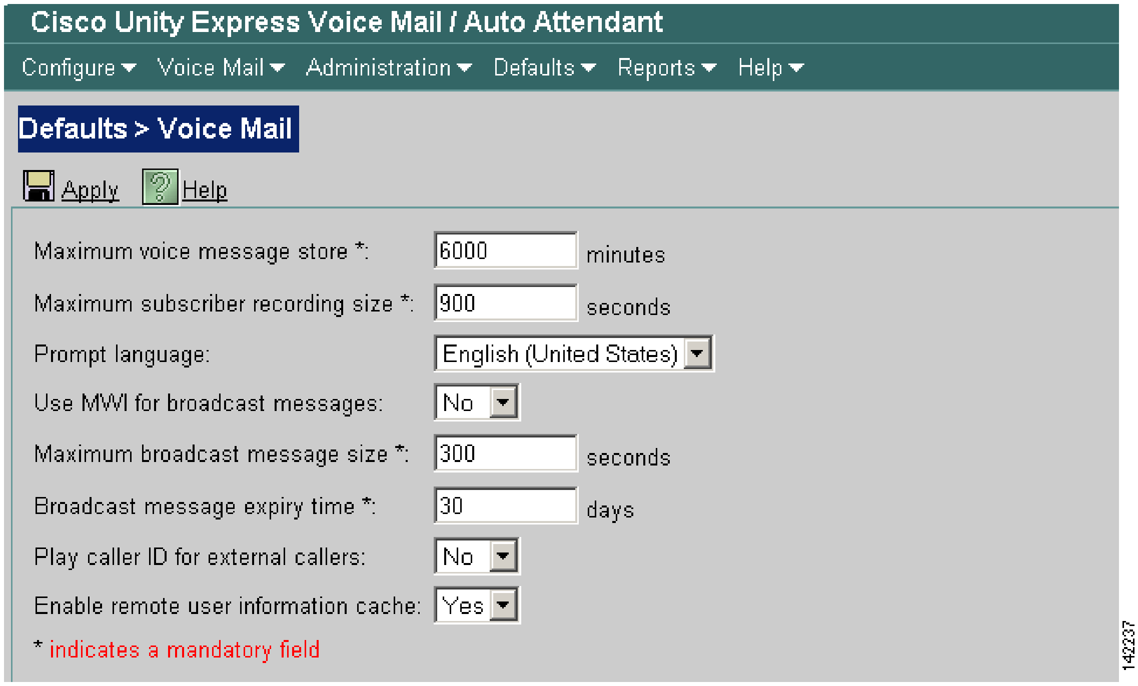
Caller ID in Message Header

Until Cisco Unity Express 2.0, only internal extensions were played out during the message header when a user retrieved a voice message. Messages from all other call origins played out as being from an “unknown caller,” even if the digits were known at the time the call arrived.

As of Cisco Unit Express 2.1, the Caller ID for “unknown” calls (calls from anywhere else except another recognized subscriber defined in a user profile on the Cisco Unity Express system) can be played out reading the digits received with the call. This applies to VoIP calls or PSTN calls arriving at the mailbox.

Reading out Caller ID is not the default operation of the system; it requires an administrator to set the “Play caller ID for external callers” field on the Defaults > Voice Mail window shown in Figure 27.

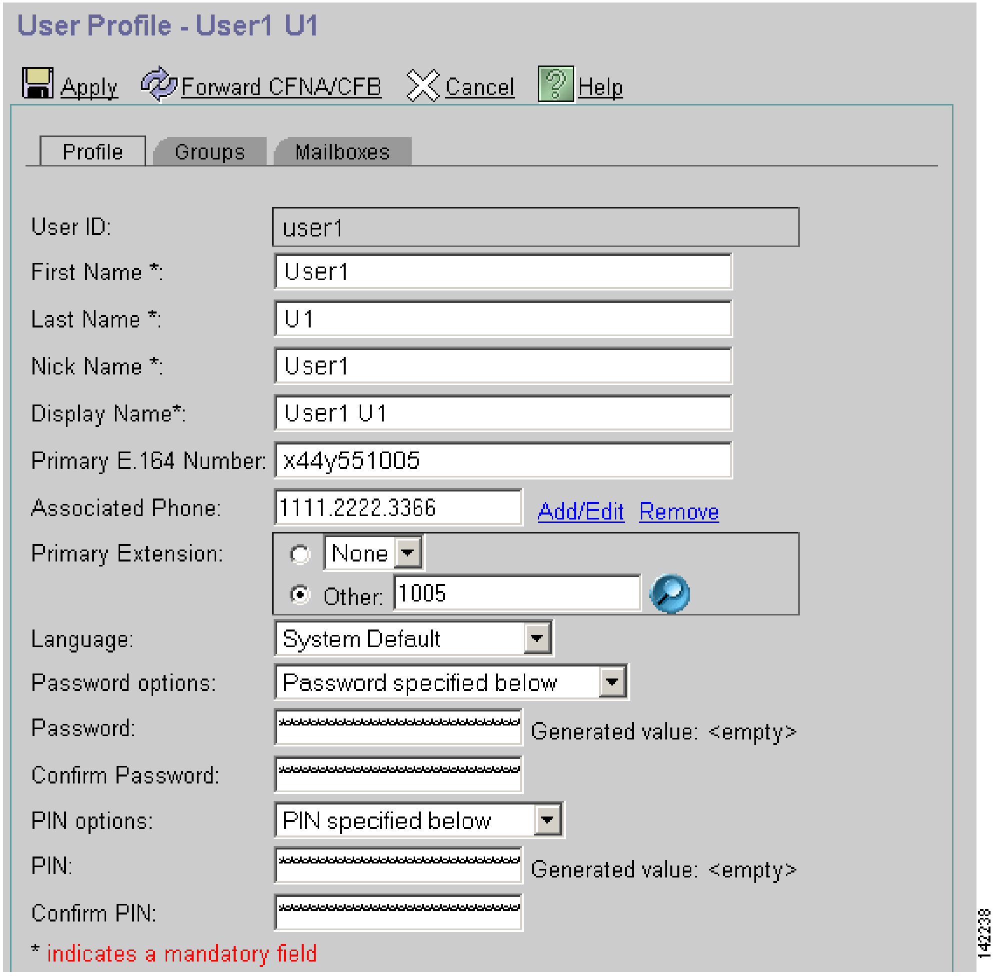
Figure 27 Caller ID in Message Playout



Dial-by-Name in Message Send

The names accessible via the Cisco Unity Express AA dial-by-name and voice mail send dial-by-name functions are based on the user profile configuration. The First Name and Last Name fields, as shown in Figure 28, are used to populate the names database used by the dial-by-name feature.

Figure 28 Name Fields in Local User Profile



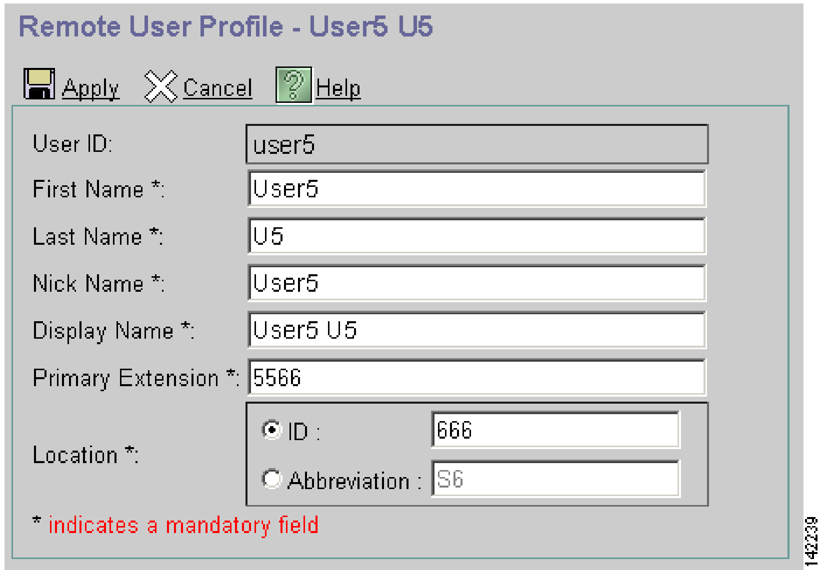
The Cisco Unity Express AA dial-by-name feature has the following characteristics:

- Names of users are defined on the local Cisco Unity Express system.
- Groups cannot be accessed via the AA dial-by-name feature.

The voice mail send dial-by-name function has the following characteristics:

- Names of users are defined on the local Cisco Unity Express system.
- Names of users are defined in remote user profiles on the local system. An example of a remote user profile is shown in Figure 29.
- Names of groups are associated with GDMs.
- Names of distribution lists.

Figure 29 Name Fields in Remote User Profile



Cisco Unity Express has no centralized or external directory access and cannot access name or user definitions defined anywhere else in the network.

Digit Manipulation

The use of Cisco CallManager or the routers (or any other piece of equipment in the call path) to perform digit translation on phone numbers could affect your call flows into Cisco Unity Express voice mail. When calls are not working correctly, you will experience overflow tone or dropped calls when attempting to enter voice mail. There are two aspects to consider regarding digit manipulation, including changes to:

- The voice mail pilot number
- The extension of the mailbox that must be entered

Voice Mail Pilot Number

The Cisco Unity Express voice mail pilot number is typically defined as an extension on the system, such as 3105. Very often there is also a PSTN number associated with the voice mail pilot to allow easy access for your employees to call in to retrieve their voice mail. This could be a number completely unrelated to the voice mail pilot number (such as x33.y55.1266) that is changed (via digit manipulation) to extension 3105 to route the calls. This could also be a DID number, for example, x33.y55.3105, that directly terminates without digit manipulation into voice mail.

You can configure the routing of calls to multiple variations of the voice mail pilot number (in this case 3105 from internal IP phones, and x33.y55.3105 from the PSTN) to Cisco Unity Express in one of two ways:

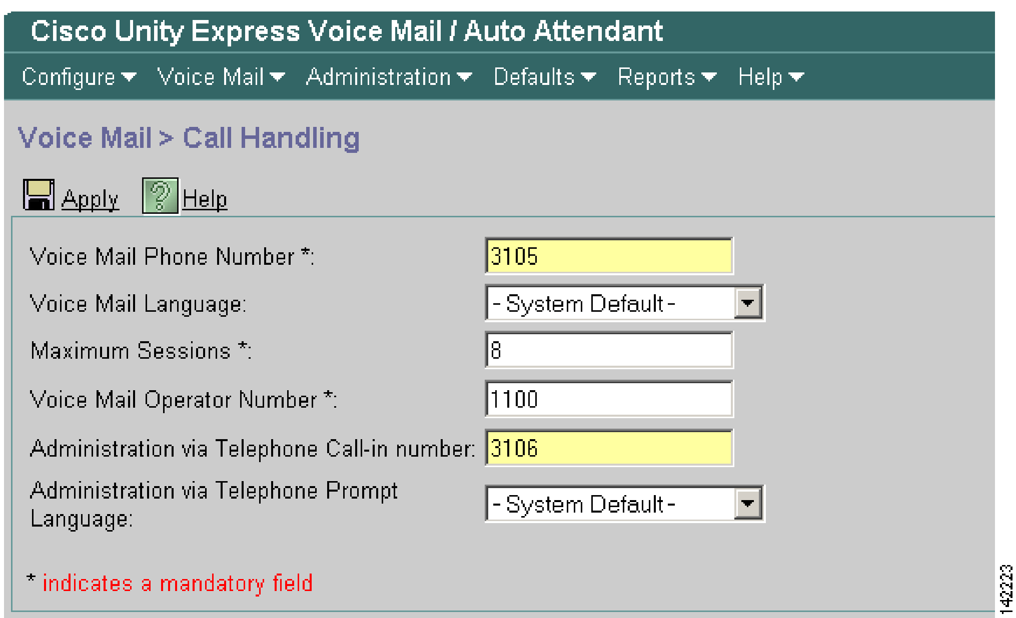
- Perform digit manipulation on the DID number (x33.y55.3105) and reduce it to the extension (3105) before delivering the call to Cisco Unity Express. In a Cisco CME environment, you can use translation rules on the router to accomplish this manipulation. In a Cisco CallManager environment, you can use route pattern tools to accomplish this manipulation.

- Define two voice mail pilot numbers in Cisco Unity Express to recognize both variations of the number as a valid pilot number. You can do this via the CLI in any release of Cisco Unity Express, but via the GUI only as of Cisco Unity Express 2.1.

The following configuration example shows a Cisco CME router configuration using translation rules to change the DID number (x33.y55.3105) to extension 3105 before the call enters Cisco Unity Express. For this scenario, Cisco Unity Express has a single voice mail pilot number (3105) defined, as shown in Figure 30.

```
voice translation-rule 10
 rule 1 /x33y553100/ /3100/
 rule 2 /x33y553105/ /3105/
 rule 3 /x33y553106/ /3106/
!
voice translation-profile to_cue
!
 translate called 10 dial-peer voice 3100 voip
 description VM-AA
 destination-pattern 31..
 session protocol sipv2
 session target ipv4:a.3.229.128
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
dial-peer voice 3101 voip
 description VM-AA-PSTN
 translation-profile outgoing to_cue
 destination-pattern x33y5531..
 session protocol sipv2
 session target ipv4:a.3.229.128
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
```

Figure 30 Cisco Unity Express Single Voice Mail Pilot Number Configuration



As an alternative to digit manipulation, you can define two pilot numbers on Cisco Unity Express to accept incoming calls to the two numbers. For this configuration you should ensure that your call agent can route calls intended for both pilot numbers to Cisco Unity Express. The following configuration example shows SIP dial peers for Cisco CME or Cisco SRST deployments:

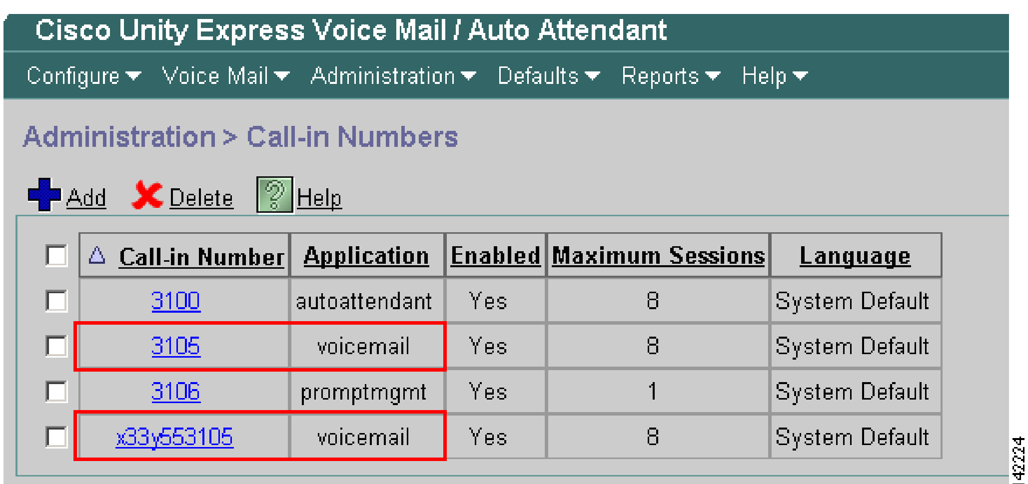
```
dial-peer voice 3100 voip
 description VM-AA
 destination-pattern 31..
 session protocol sipv2
 session target ipv4:a.3.229.128
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
dial-peer voice 3101 voip
 description VM-AA
 destination-pattern x33y5531..
 session protocol sipv2
 session target ipv4:a.3.229.128
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
```

On Cisco CallManager, you can define multiple route points to be associated with the Cisco Unity Express JTAPI user. The following configuration example shows the Cisco Unity Express CLI for the definition of both pilot numbers, and Figure 31 shows the Cisco Unity Express 2.1 GUI window for the same configuration:

```
ccn trigger sip phonenumber 3105
 application "voicemail"
 enabled
 maxsessions 8
 end trigger

ccn trigger sip phonenumber x33y553105
 application "voicemail"
 enabled
 maxsessions 8
 end trigger
```

Figure 31 Cisco Unity Express Multiple Voice Mail Pilot Number Configuration



Extension of the Mailbox

As described in the "Voice Mail Pilot Number Operation" section on page 77, Cisco Unity Express uses the "last redirected number" field delivered by the call agent to decide which mailbox to enter. The digits in this field must map to an extension assigned to a mailbox, or the call will fail with a Cisco Unity Express system message announcing "Sorry, there is no mailbox associated with this extension…".

To ensure that calls enter the desired mailbox in Cisco Unity Express, remember the following digit manipulation considerations:

- Cisco Unity Express can associate up to two numbers with a mailbox (the Primary Extension and the Primary E.164 Number fields in the Cisco Unity Express user profile). A call containing either of these two numbers will correctly enter the mailbox for this subscriber. If you have more than two numbers that must be mapped to a single mailbox, those numbers must be translated on the call agent to match the Primary Extension or the Primary E.164 Number fields before the call reaches Cisco Unity Express.
- If you are leveraging the Primary E.164 Number field for a purpose other than the DID number for the subscriber (as described in the "Calling into Voice Mail to Retrieve Messages" section on page 78), then the DID number must be translated to the extension by the call agent before the call enters Cisco Unity Express.
- If you are using Cisco CME as the call agent, and implement **dialplan-pattern** commands to "normalize" numbers, be aware that these commands translate (or expand) the dialed number of internal calls to the digit string specified in the **dialplan-pattern** command statement. This might be a number that Cisco Unity Express does not recognize because it no longer equals the extension associated with the mailbox. Set the Primary E.164 Number field to the expanded number created by the **dialplan-pattern** command.

If Cisco CME has primary and secondary numbers defined on an ephone, the number that was dialed by the originator is the number delivered to Cisco Unity Express. For an ephone-dn configuration of "number 3001 secondary x33y553001," either of the two numbers associated with that phone may be delivered to Cisco Unity Express, depending on which number the caller dialed. Unless the Primary E.164 Number is configured to match the secondary number, calls to both numbers cannot get forwarded to voice mail.

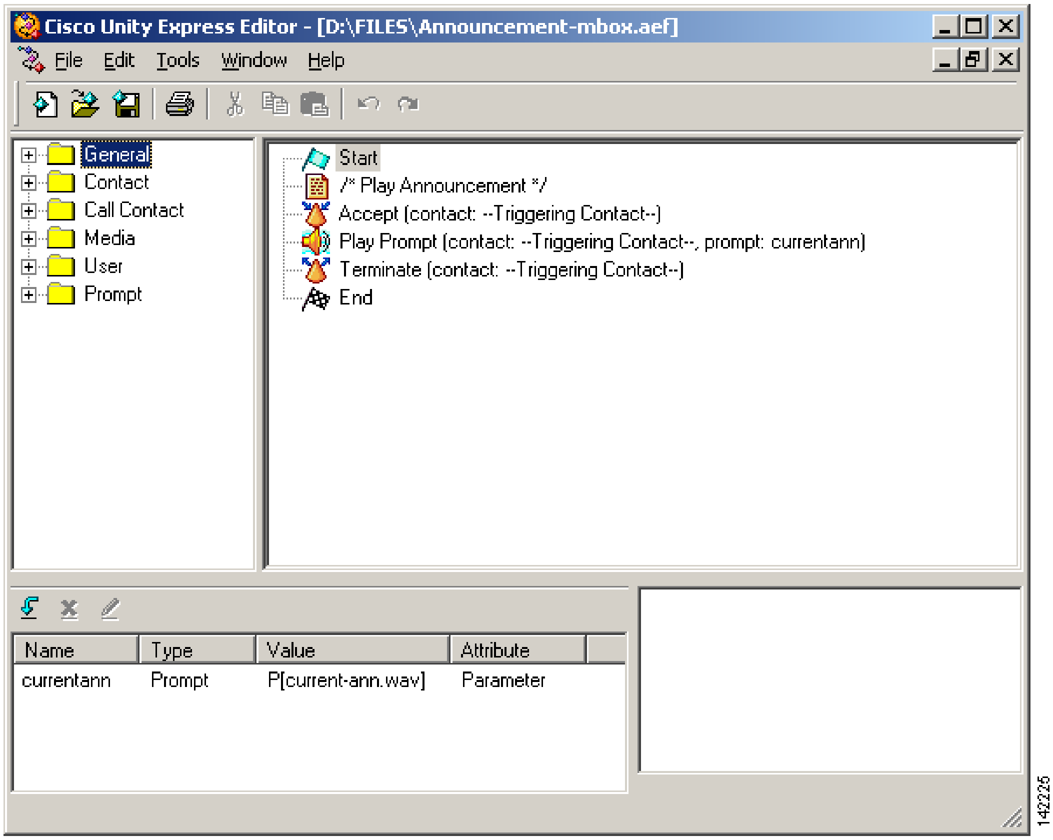
"Announcement Only" Mailbox

You can use either the Cisco Unity Express AA or a voice mailbox in order to play an announcement to callers that changes frequently (perhaps daily or hourly). Cisco Unity Express does not have a direct feature or mailbox type called an "announcement-only" mailbox, but you can use various other Cisco Unity Express features in combination to achieve this operation.

AA Application

The Cisco Unity Express AA is the most flexible way of implementing an "announcement-only" mailbox implementation. Write an AA script that plays an announcement (prompt) to callers. The simple example file (Announcement-mbox.aef) is shown in Figure 32. Associate this script with a pilot number (in the same way you would build a Cisco Unity Express AA application). Callers to the pilot number will hear the announcement and the call will be automatically disconnected by the Terminate step.

Figure 32 Announcement Script Example



To change the announcement played by the script, follow these steps:

Step 1 Log in to the Administration via Telephony (AVT) interface of Cisco Unity Express.

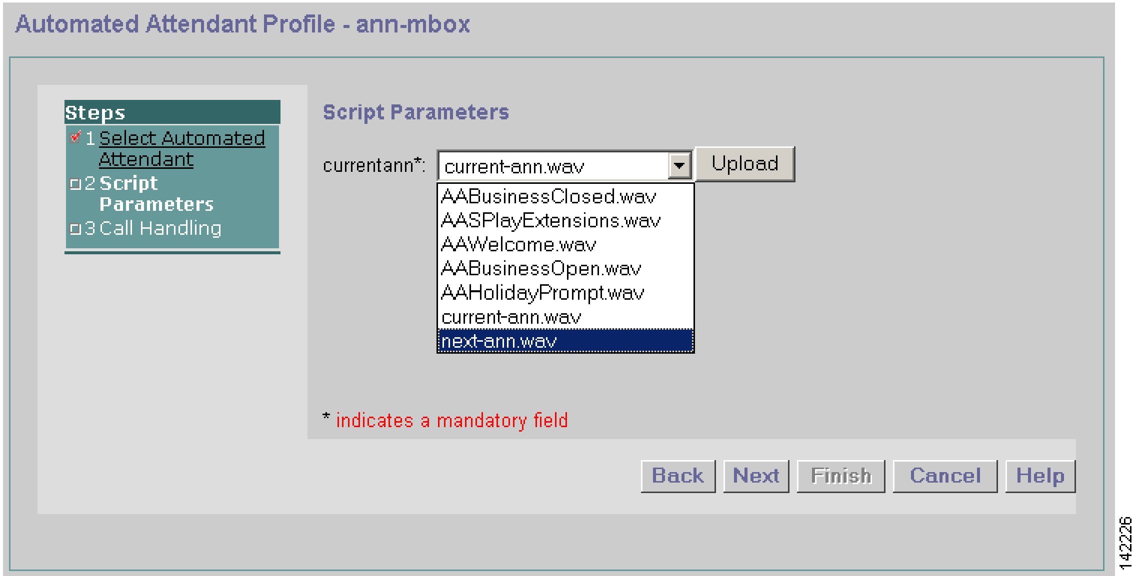
Step 2 Record the new prompt.

Step 3 Change the system-assigned filename via the GUI to the filename you want (**Voice Mail** > **Prompts** window).

Step 4 Associate the new prompt file with the script via the **Script Parameters** GUI window as shown in Figure 33 (**Voice Mail** > **Auto Attendant**, click on the application name, and click **Next**).

The new prompt will take effect with the next new incoming call. Existing calls already active in the application are not affected by this change.

Figure 33 Updating the Announcement

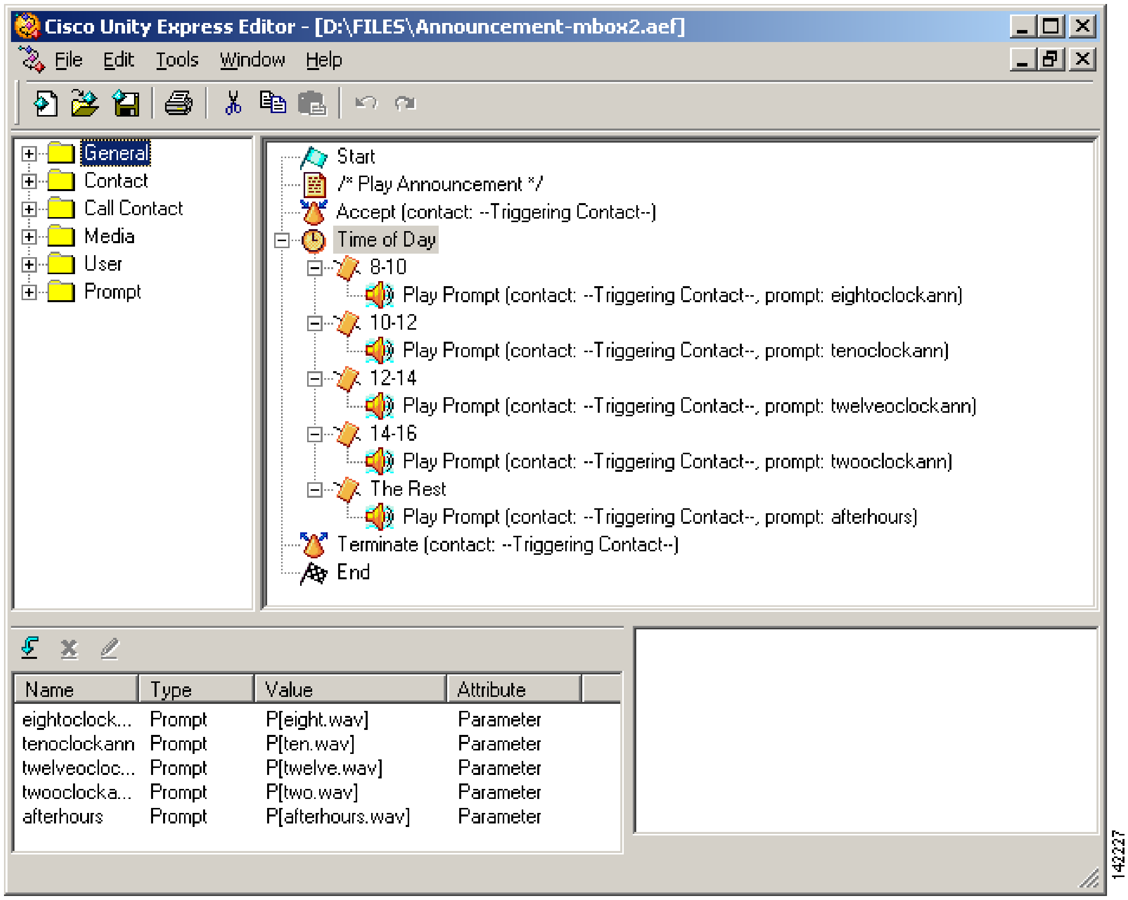


Building the "announcement mailbox" application using the Cisco Unity Express AA features has the following characteristics and tradeoffs:

- The person making changes to the prompt recordings and assignments requires AVT access (to gain this access, define a group with the privilege to access the AVT and then add the users that must have this access as members of the group). This provides automatic PIN authentication so that only designated administrators can make changes to the announcements.
- The person making changes to the prompt recordings and assignments requires browser access to the Cisco Unity Express GUI to change the prompt filenames and assignments to the script. Although these changes can also be made via the CLI, this interface is likely not well suited to the person who would be maintaining these prompts.
- The simple script example shown in Figure 32 disconnects the call immediately after the announcement, but you have full flexibility in the script instead to request and process input (DTMF) from the caller, or provide other information or choices (such as being transferred to an operator) subsequent to the announcement.
- You have full control over the exact content of the phrases spoken to the caller and you can disconnect the call at a time of your choice. You need not rely on the caller to hang up or take any action.
- You can have the same announcement available in multiple different languages. You can either direct the caller to a language of choice by presenting a menu step before the announcement is played, or you can derive the language preference from the called number (provided you have different PSTN numbers for the different language preferences, and therefore also multiple pilot numbers associated with the application script).
- You can easily prerecord announcements, and have them automatically activated at a later time by using the time-of-day, day-of-week, or business-hours steps in the script. The example script in Figure 34 shows four different announcements given during the day in two-hour blocks, and a fifth announcement is given after hours. These announcements can all be recorded at the start of the day

(or the end of the previous day) and each will take effect based on the actual time of day as specified in the script. By designing your own custom script, you have full control over the schedule and timing of the announcements that the application plays.

Figure 34 Time-of-Day Announcement Script Example



Voice Mailbox Application

A Cisco Unity Express GDM can also be used to implement an "announcement mailbox" application. Define a GDM, associate it with an extension (which becomes the equivalent of your pilot number for this application), and log in to the GDM and record the announcement you want played as the outgoing greeting of the mailbox. You can record an alternate greeting as well and therefore, by changing the greeting of the mailbox between standard and alternate, you could alternate between two different prerecorded announcements.

Building the "announcement mailbox" application by using the Cisco Unity Express GDM voice mail features has the following characteristics and tradeoffs:

- The person making changes to the GDM greetings (rerecording the announcement) requires access to the GDM. This person must therefore have a personal mailbox defined, and be a member of the group associated with the GDM. The person's personal mailbox provides PIN authentication so that only designated administrators can make changes to the announcement.

- The person making changes to the GDM greetings requires only telephone (TUI) access to the Cisco Unity Express system; no browser or IP access is necessary.
- You do not have full control over the exact content of the phrases spoken to the caller. The recorded greeting for the GDM is played out to the caller (which you can fully control), but that is followed by the system prompt "You may record your message at the tone. When you are finished you can hang up, or press pound for more options," which cannot be bypassed, suppressed, or provided in a language other than the system language installed on Cisco Unity Express.
- You cannot disconnect the call from the Cisco Unity Express system—the caller must disconnect.
- If the active greeting of the GDM is rerecorded, it becomes live immediately. If the alternate greeting is rerecorded it can be made live by manually changing the active greeting of the mailbox—this action cannot be scheduled to happen automatically at a future time.
- To provide an announcement in different languages you can define multiple different GDMs, each containing the announcement in an individual language. This call flow requires separate PSTN call-in numbers to differentiate which language the caller wants. The caller cannot be prompted for a language choice.
- The smallest size mailbox that can be defined on Cisco Unity Express is 10 seconds. It cannot be zero. If the caller does not hang up after the announcement is completed, the caller is presented the normal mailbox dialog and is offered an opportunity to leave a very short message.

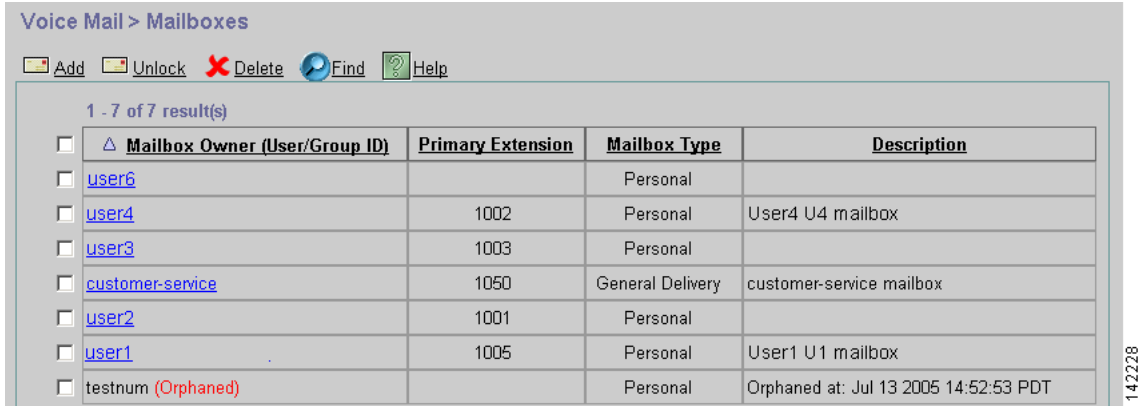
Disabled Mailboxes

A mailbox can be disabled by the Cisco Unity Express system administrator. The administrator does this by unchecking the Enabled field in the mailbox profile (see Figure 22). A subscriber cannot log in to a disabled mailbox, and callers cannot leave messages in a disabled mailbox. Disabling a mailbox is equivalent to deleting it, from a functional point of view; however, this preserves the content of the mailbox if that should be of value to your organization. If a mailbox is deleted, the messages are deleted too. A disabled mailbox can be reenabled by the administrator at a later date to restore full operation of the mailbox.

Orphaned Mailboxes

If a user or group profile is deleted using the Cisco Unity Express GUI, the associated mailbox is also deleted. However, if a user or group profile is deleted using the CLI, the mailbox is left intact, causing it to become orphaned (disassociated from a specific active subscriber profile). See Figure 35.

Figure 35 Orphaned Mailbox



The Cisco Unity Express maintains an orphaned mailbox for seven days; during this time, the user or group profile can be rebuilt and the mailbox reassociated with its owner. After seven days, orphaned mailboxes are automatically deleted by the system. Orphaned mailboxes cannot be associated with a different User ID; an orphaned mailbox must be reassociated with same User ID for which it was defined originally.

Mailbox Space Allocation

Messages are stored in G.711 u-law format—An encoding scheme designed to be transmitted at a data rate of 64 Kbps. Each minute of audio uses bandwidth according to the following calculation:

60 seconds * 64 Kbps = 3840 Kb/minute = 480 KB/minute

The audio of a voice message is physically stored only once regardless of how many mailboxes in which the message may appear—either by being sent by the originator to multiple subscribers, or being forwarded to other subscribers by recipients of the message. However, the time for the message is counted against each individual mailbox where the message appears.

Space used by an individual mailbox includes:

- Standard greeting size
- Alternate greeting size
- Size of all voice messages in the mailbox

Spoken name recordings are not counted as part of the space allocation of a mailbox.

When a new mailbox is created, it is set to the default system mailbox size, unless it is explicitly set to a particular size by the administrator. Changing the system default mailbox size does not affect existing mailboxes; it governs only the size allocated to mailboxes created after the default is changed.

Note Upgrading the license on Cisco Unity Express to a higher number of mailboxes does not affect the storage allocation on the system. For example, if a 12-mailbox license is installed on a Cisco Unity Express AIM module with 16 hours of storage, and an hour is allocated to each of the mailboxes, then 12 of the 16 hours total storage is allocated on this system. When this system is upgraded to a 25-mailbox license, there is only 4 hours left to be allocated to the 13 new mailboxes. If this is insufficient, each of the original 12 mailboxes must be resized to make more space available to the new subscribers. A mailbox's size can be lowered by the administrator, but requires a value at least big enough to contain the current message content in the mailbox.

Spoken Names

The limit on spoken names recorded by using the TUI for local subscribers, network locations, and remote subscribers is 10 seconds.

Spoken Name Confirmation

When a subscriber addresses a message to another subscriber, spoken name confirmation is given to the sender of the message whenever possible. If spoken name confirmation is not available, the destination extension is read out. The spoken name of the recipient might not be available due to one of the following issues:

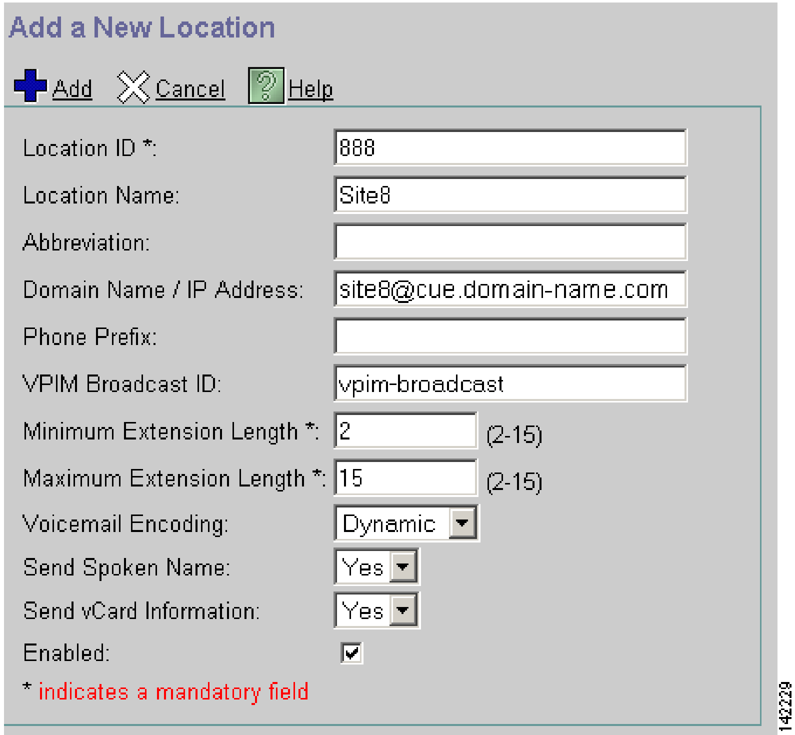
- Local recipient—The recipient subscriber has not recorded a spoken name for the assigned mailbox.
- Remote recipient—The spoken name for the subscriber does not exist in either the static directory (remote user configuration) or the dynamic cache of entries accumulated via receiving networked messages from other sites.

Spoken Name Delivery

When a subscriber receives a message, a spoken name is delivered as part of the message header readout whenever possible. If spoke name delivery is not available, the originating (sending) extension is read out. The spoken name of the sender might not be available due to:

- Local or remote sender—The sending subscriber has not recorded a spoken name for their mailbox.
- Remote sender—The sending system's intersite networking is set up not to include the spoken name with the message when transmitting it to the recipient. Cisco Unity Express sends the spoken name by default with networked locations. Figure 36 shows the Send Spoken Name field for a networked location that can be used to control this operation (use the **Administration > Networking Locations** window, then click on the desired location, or **Add** for a new location, to bring up this window). Cisco Unity does not send this field by default, but it can be enable by toggling the Sender's recorded name field on the Delivery Locations window for the particular location in question.

Figure 36 Send Spoken Name for Networked Locations



Outcall Notification

Cisco Unity Express 2.1 does not support any means of outcall notification.

Directories

Cisco Unity Express uses an internal directory to store user and PIN information, and to do user mailbox, AVT, or browser administration login authentication. This directory information cannot be accessed externally from another system, nor can Cisco Unity Express access an external directory for its authentication purposes.

Cisco Unity Express keeps and uses several types of directory information:

- Local user and PIN information—This information is derived from the user profiles (Configure > Users) entered into the Cisco Unity Express configuration.
- Remote user information—This information is derived from the remote user profiles (Configure > Remote Users) entered into the Cisco Unity Express configuration.
- Dynamic Cache—This information is derived from Voice Profile for Internet Mail (VPIM) messages received by Cisco Unity Express. The sender user information, and the spoken name (if present), are kept in a short least recent user (LRU) cache for use (for example, to provide Spoken Name Confirmation) if messages are sent back (reply or a new message) to this same user. This cache is automatically enabled, but can be disabled by the Enable remote user information cache field on the Defaults > Voice Mail window if needed.

MWI Operation

Cisco Unity Express enables an MWI when a new voice message is left and disables MWI when the last new voice message is saved or deleted. Cisco Unity Express has no direct visibility into enabling or disabling MWI on a phone. Cisco Unity Express knows the extension associated with the change in MWI, and notifies the call agent of the extension and the desired MWI state. Upon receiving this message, the call agent is responsible for determining on which phones the extension appears, and to send an appropriate message to each affected phone to change its MWI state.

The following MWI considerations are presented in this section:

- Methods of Invoking MWI, page 104
- MWI Lamps and Icons, page 104
- Refresh, page 105
- Broadcast, page 105
- GDMs, page 106

Methods of Invoking MWI

The method of MWI notification used by Cisco Unity Express depends on the associated call agent:

- Cisco CME—Outdial directory numbers (DNs) are used between Cisco Unity Express and Cisco CME. Cisco Unity Express initiates an outbound SIP call to a predefined Cisco CME MWI extension and when Cisco CME receives this call attempt, it collects the extension for which MWI must be changed from the call setup attempt, and in turn lets the phone know to change its indicator to the requested state. Two separate MWI extensions are defined on Cisco CME, one for "MWI on" and one for "MWI off". Only one set of these MWI on/off extensions can be defined, which in turn implies that all Cisco CME extensions associated with mailboxes must be of a fixed length or MWI will not operate correctly.
- Cisco CallManager—JTAPI is used as the signaling protocol between Cisco Unity Express and Cisco CallManager. To notify Cisco CallManager of an MWI change, Cisco Unity Express sends a JTAPI message containing the extension and the requested MWI state. Cisco CallManager sends a message to the affected phones.
- Cisco SRST—There are no MWI changes for phones during SRST failover mode, regardless of message activity in the mailbox. If MWI state is on before SRST failover, it remains on until Cisco CallManager comes back into contact. Similarly, if the MWI state is off before failover, it remains off until contact is reestablished. MWI state on all phones is refreshed automatically when Cisco CallManager comes back into contact; no manual intervention is required.

MWI Lamps and Icons

The nature of the MWI indication depends on the capabilities of the phone, the configuration of the system, and the call agent used. Characteristics are as follows:

- Lamp—Cisco IP phones have a red lamp in the handset that can be lit for MWI. When you implement Cisco Unity Express with Cisco CME, this type of MWI is provided only for messages associated with the extension on button 1 of the phone. When a lamp is used as a MWI with Cisco CallManager, the configuration determines which buttons on the phone will trigger MWI via the red lamp of the phone set.

- Flashing Icon—Cisco IP phones with displays can provide a flashing envelope icon next to a button appearance. When Cisco Unity Express is implemented with Cisco CME, this type of MWI is provided for messages associated with the extensions on button 2 or higher of the phone. When a flashing icon is used with Cisco CallManager, the configuration determines which buttons on the phone will trigger MWI via a flashing icon.
- Stutter Dial Tone—Analog phones connected to an SCCP-controlled FXS port (for example, on a VG224 gateway) are provided with stutter dial tone MWI.

Note Cisco CME can activate MWI for the primary or secondary extension associated with an ephone-dn. MWI can be activated only for the first DN on an overlay. The subsequent DNs associated with an overlay do not trigger MWI on the phone.

Refresh

MWI state on all phones is refreshed when the Cisco Unity Express system reboots or starts up. It is not done as a periodic scheduled activity while the system is running. If MWI state should become unsynchronized with mailbox state, MWI must either be reset manually or Cisco Unity Express must be rebooted.

The administrator can reset MWI state manually, either for a particular phone, or for the entire system. If the entire system is selected, MWI state changes will be staggered over a short period of time; not all phones will be done at once.

Broadcast

Cisco Unity Express provides MWI for individual message activity in personal mailboxes and GDMs by default. This feature cannot be turned off.

MWI can optionally be provided for broadcast messages (the default is disabled). To disable MWI for broadcast messaging, set the "Use MWI for broadcast messages" field to Yes (on the Defaults > Voice Mail window).

The configuration of MWI for broadcast messaging is of local significance to the Cisco Unity Express system. Therefore, if you send a broadcast message to five different sites, MWI might be activated for that message on some of the recipient sites and not on others, depending on how each individual recipient system is configured for this parameter.

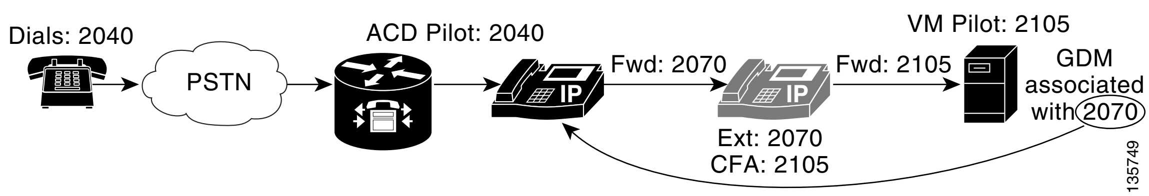
The configuration of MWI for broadcast messaging is a Cisco Unity Express system-wide setting. MWI operation for broadcast messaging cannot be controlled per individual mailbox, or individually per message. MWI state (on or off) is not an attribute of the broadcast message itself; it is an attribute of the system on which the message is delivered. If MWI for broadcast messaging is configured to be on, the MWI light is lit for all mailboxes on the system when a broadcast message becomes active. MWI is refreshed when a broadcast message expires so that any mailboxes that have not listened to the message will never receive it and the MWI state is turned off (unless there are other new messages in the mailbox).

GDMs

MWI for GDMs is done in the same manner as MWI for personal mailboxes. If the extension associated with a GDM appears on a phone, then that phone receives MWI for message activity in the GDM. MWI for GDMs is not done to the phones associated with the extensions of the group's members; it is done only to the extension directly associated with the group mailbox. For example, MWI is done to phones with an appearance of extension 1050 in the configuration shown in Figure 25.

GDMs can be associated with extension types that cannot be placed as button appearances on a phone, such as Cisco CME automatic call distributor (ACD) or hunt-group pilot numbers. If the GDM is associated with such a type of extension, there is no MWI for messages in that GDM on any of the phones that belong to the ACD or hunt group. You can work around this by configuring the ACD or hunt group to forward calls to an intermediate extension (which is set permanently to CFA calls to the voice mail pilot number), rather than forwarding directly to voice mail. The intermediate extension can now be placed on a phone as a button appearance and MWI for GDMs can be implemented even for GDMs functionally assigned to ACD or hunt groups. Figure 37 shows such a configuration.

Figure 37 MWI for GDMs Associated with ACD and Hunt Groups



In the example shown in Figure 37, the ACD pilot number is 2040. If you associate the GDM with extension 2040, then there is no MWI for any messages in the GDM. Instead, associate the GDM with intermediate extension 2070, which is permanently forwarded (via CFA) to the voice mail pilot number 2105. The ACD voice-mail number is now set to 2070 instead of directly to 2105. Extension 2070 may now appear on a button on the ACD agent phones and gets MWI for message activity in the GDM. The following configuration example illustrates the Cisco CME and Cisco Unity Express configurations for this setup.

The following Cisco CME configuration example illustrates configuring GDM MWI for an ACD group:

```
!
! Cisco CME ACD AA Configuration for pilot number 2040.
!
call application voice cme-aa flash:app-b-acd-aa-2.1.0.0.tcl
call application voice cme-aa second-greeting-time 30
call application voice cme-aa max-time-call-retry 60
call application voice cme-aa max-time-vm-retry 1
call application voice cme-aa call-retry-timer 20
call application voice cme-aa aa-pilot 2040
call application voice cme-aa number-of-hunt-grps 3
call application voice cme-aa service-name acd
call application voice cme-aa voice-mail 2070
call application voice cme-aa language 0 en
call application voice cme-aa set-location en 0 flash:
!
! Extension 2070 associated with the GDM. It is CFA to 2105,
! the Cisco Unit Express pilot number.
!
ephone-dn  11
 number 2070
 description GDM
 name Cust Svc GDM
```

```
 call-forward all 2105
!
! Ephone-dn 11 (2070) is defined as button 2 on the ACD Agent phone
! so that the agent can get MWI for the GDM.
!
ephone  1
 username "Agent1"
 mac-address 1111.2222.3333
 type 7960
 button  1:1 2:11
```

The following Cisco Unity Express configuration example illustrates configuring GDM MWI for an ACD group:

```
!
! The custservice ACD group (and GDM) is associated with extension 2070.
!
groupname custservice phonenumber "2070"
!
! Voice mail pilot number is 2105.
!
ccn trigger sip phonenumber 2105
 application "voicemail"
!
! Define the GDM associated with 2070, associated with the custservice group.
!
voicemail mailbox owner "custservice" size 5520
 description "custservice mailbox"
```

Leaving a Message After Business Hours Only

If calls must ring on phones indefinitely during business hours, and only forward to voice mail after hours, a time-of-day routing feature is required on the call agent—or the employees must manually call forward their phones to the voice mail pilot number when they leave the office at the end of the day. Cisco Unity Express itself does not provide this feature; the call agent makes a decision to forward the call (or not) to the voice mail system before it reaches the voice mail system.

Distribution Lists

Cisco Unity Express 2.1 introduces support for distribution lists. A distribution list allows a subscriber to send a message to a list of predefined recipients. Distribution lists can be addressed either by number or tag (the descriptive name associated with the distribution list). A spoken name can be recorded via the TUI (it cannot be uploaded as a .wav file) for a distribution list to assist in confirmation that the message is being sent to the correct recipient list (during addressing of a message).

The following distribution list considerations are presented in this section:

- List Types, page 108
- Membership and Ownership, page 108
- Privileges to Access and View Distribution Lists, page 109
- Remote Users and Remote Distribution Lists, page 110
- Everyone List, page 110

List Types

Cisco Unity Express supports public and private distribution lists as follows:

- Public—These are defined by an administrator (or suitably privileged system user), and are visible to all subscribers on the system and can have messages addressed to them by all subscribers.
- Private—These are defined by an individual subscriber and are visible (in general) only to the subscriber that defines the list.

If a subscriber is deleted from the system, all the private distributions lists belonging to that subscriber are also deleted from the system. Public lists, however, are deleted only when the administrator explicitly deletes them.

The following characteristics apply to the support of public distribution lists:

- A maximum of 15 public lists per system
- A total of 1000 members in all public lists collectively on a Network Module (NM) and a total of 500 members on an Advanced Integration Module (AIM)
- A maximum of 50 owners collectively across all public lists

Note The "everyone" list (described in the "Everyone List" section on page 110) and its members do not count toward these numbers.

The following characteristics apply to the support of private distribution lists:

- A subscriber can define up to five private lists.
- A total of 50 private list members are supported per subscriber (collectively over all lists belonging to this subscriber).

Membership and Ownership

Distribution lists have members and owners. Members are the recipients who receive a voice message when a sender sends a message to the distribution list. Owners are the subscriber User IDs who have the privileges to change the membership and other parameters of the distribution lists.

The members of a distribution list can be any combination of the following entities:

- Local
  - Subscribers
  - Groups
  - GDMs
  - Other (nested) public distribution lists
- Remote
  - Blind addresses (a numeric string representing a location code that is configured on the local system and the extension of a subscriber at another network location)
  - Remote subscribers (user IDs defined in the Configure > Remote Users GUI window)

The owners of a public distribution list can be one of the following entities:

- Local subscribers

- Groups

Public lists can be nested and can include other public lists as members, but public lists cannot include private lists. Private lists can include public lists as members.

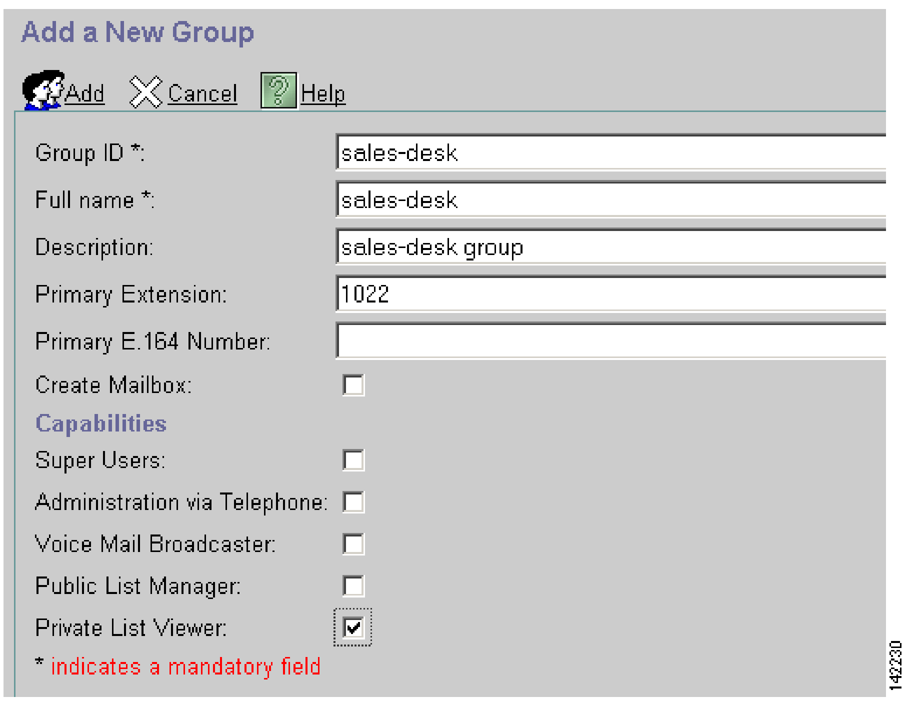
Both a group and a GDM can be members of a distribution list. If a group is a member, any message sent to the distribution list is placed in the personal mailbox of each member of the group (but not the group mailbox or GDM). If a GDM is a member, any message sent to the distribution list is placed in the GDM (but not any personal mailboxes of group members). Both the group and the GDM can be explicit members of a distribution list if you want the message to be delivered to both destinations.

Privileges to Access and View Distribution Lists

Private distribution lists are administered and owned by the subscriber who defined them. They are, in general, not visible to anyone other than that subscriber. The exception to this rule is if another user (likely an administrator) is given the explicit "Private List Viewer" privilege. In this case, the subscriber with this privilege can view (although not change) the members of the private lists held by other subscribers on the system (through the GUI).

"Private List viewer" is one of the system access privileges that can be awarded to a group. All members of that group inherit that privilege. Assigning this privilege for a new group is shown in Figure 38.

Figure 38 Assigning the Privilege to View Private Distribution Lists



Note Public lists are printed in the text configuration output of the Cisco Unity Express system (with the **show running-config** command), but private lists are not. If you make a "backup" of a system configuration by copying and pasting the output of the **show running-config** command, you cannot preserve the definition of private lists to the new system. Private lists can be explicitly listed in the CLI by using the **show lists owner** *user-id* command, where *user-id* is the User ID of the owner of the list.

Defining public distribution lists is controlled by the "Public List Manager" privilege (see Figure 38). All members of a group that has this privilege can define and manage public list membership on the system. To modify a public distribution list, the user must be a member of a group that has the "Public List Manager" privilege, or be an owner of the public list. By default, only users that belong to the Administrators system group have these privileges.

Table 11 summarizes the distribution list parameters that can be administered via the TUI, GUI, and CLI.

Table 11 Summary of Administration of Distribution Lists

Configuration Item	TUI	GUI	CLI
Public distribution list management	Yes	Yes	Yes
Private distribution list management	Yes	Yes	—
Create a list with name and number[1]	Yes	Yes	Yes[2]
Add/remove members of a list	Yes	Yes	Yes[2]
Record spoken name of a list	Yes	—	—
Add/edit description of a list	—	Yes	Yes[2]
Edit the name or number of a list	—	Yes	Yes[2]
Add/remove owners of a public list	—	Yes	Yes
Display public list membership	—	Yes	Yes
Display private list membership	—	Yes	Yes

1. If created through TUI, the list name is system autogenerated.
2. Public lists only.

Remote Users and Remote Distribution Lists

Distribution lists are local to the system on which they are defined and can be addressed only by local subscribers when they send messages. A distribution list that was defined at a remote site cannot be used as the destination address of a message sent on your local system. You can send a message to a local distribution list that includes remote users (as members) and blind addresses (location code and extension) that result in remote recipients receiving the message.

Everyone List

Cisco Unity Express defines a system public list named the "everyone" list. This list cannot be deleted and the membership cannot be changed. It is automatically maintained by the system and always contains a definitive list of every subscriber defined on the system. Groups and GDMs are not members of the "everyone" list—only local subscribers (user profile definitions).

The default list number for the "everyone" list is 9999. This number can be changed if it conflicts with your dial plan or you desire a different numbering scheme. The "everyone" list comes with a default spoken name that can be rerecorded by an administrator.

The “everyone” list and its members do not count against the list and member number limits for the system.

Broadcast Messaging

Broadcast messaging is the ability for an authorized subscriber to send a prioritized voice mail message that everyone receives and to which everyone must listen. A broadcast message is sent to all local subscribers and all subscribers at all (or specified subset of) remote systems in the network deployment. Broadcast messages can be sent from, or to, Cisco Unity Express and Cisco Unity sites.

On Cisco Unity Express a broadcast message is sent from the administrator’s AVT interface. GDMs cannot receive broadcast message; only the personal mailboxes of individual subscribers can receive broadcast messages. A broadcast message is treated like any other normal voice message, except for:

- Broadcast messages are played immediately after the subscriber logs in as the highest priority in the message playout list.
- Subscribers must listen to the entire broadcast message—a broadcast message cannot be skipped or fast forwarded.
- Broadcast messages cannot be forwarded or replied to (they can be saved).
- The recipient does not know who sent the broadcast message.
- A new (unread) broadcast message does not count against the recipient mailbox’s storage capacity, but once it is saved it does.
- You cannot send a broadcast message to a distribution list.

The following broadcast messaging considerations are presented in this section:

MWI for Broadcast Messaging

MWI for broadcast messaging is described in the “MWI Operation” section on page 104.

Sending and Addressing a Broadcast Message

Broadcast messages are sent from the administrative AVT interface by users with the appropriate privileges. The “Voice Mail Broadcaster” privilege, shown in Figure 38, is an attribute of a group profile. This privilege is required for an AVT user to log in and hear the menu selections pertaining to broadcast messaging. Members of the system-defined “Broadcasters” group have this privilege enabled by default, but you can also add it to any other group definition of your choice.

The following broadcast message creation and addressing options are available in the AVT:

- Local Broadcast message:
  - Option 3-1-1 from the AVT main menu.
  - The message is sent to all personal mailboxes on the local system.
- Global Broadcast message:
  - Option 3-1-2-1 from the AVT main menu.
  - The message is sent to the local system and all systems defined as remote networking locations on the local system.
- Broadcast message to a specific remote systems:
  - Option 3-1-2-2 from the AVT main menu.
  - The location codes of the individual systems (local or remote) where the message must be sent are entered—a distribution list cannot be used to contain this list of location codes.

Lifetime of a Broadcast Message

A broadcast message can be prerecorded and scheduled to be delivered, or become active, at a future date and time. Similarly, a broadcast message can be set to expire at a certain date and time such that if the relevance of a message is only for a few days or a week, then the message can be removed upon expiring from any mailboxes that have not yet listened to the message.

The time between when a broadcast message becomes active and when it expires is called the lifetime of the message. The lifetime is specified by the start and end time associated with the message:

- Start time—By default, this is immediately when the message is recorded. The start time could be set to be in the future so that a message becomes active on a specified date and time.
- End time—This is calculated as the start time plus the broadcast message lifetime, which is a configurable system parameter with a default of 30 days and a limit of not being more than a year into the future. When the end time occurs, the broadcast message expires and messages that have not yet been listened to by subscribers are removed from the subscribers' mailboxes and MWI (if configured) is turned off.

Start and end times can be changed only via the CLI, once a broadcast message has been recorded, and start and end times have been assigned. For a message that is already active, only the end time can be changed. For a broadcast message sent to multiple networked locations, the parameters must be changed on each individual location, the source system no longer has any control over the destination system's handling of the message.

A broadcast message is sent to recipient network locations with Coordinated Universal Time (UTC) time parameters such that it will be delivered simultaneously on all receiving systems in their respective time zones. It is the responsibility of the recipient system to convert the UTC time stamp to the local time zone and activate the message at the appropriate given time. This means that if a broadcast message is composed with a start time of 08:00 Pacific Daylight Time, and sent to recipient systems in New York and London, then that message will activate and be delivered at 11:00 Eastern Daylight Time for mailboxes on the system in New York and 16:00 British Summer Time for mailboxes on the system in London.

Broadcast Message Properties

The following behavior differences exist between normal voice messages and broadcast messages. In all other respects, broadcast messages behave just like other voice messages.

- Mailbox full condition—This condition cannot occur for a broadcast message. A new (not yet listened to) broadcast message is not counted against the recipient mailbox's storage allocation, so even if the destination mailbox is full, a new broadcast message can still be received and listened to. A broadcast message cannot be saved by the subscriber if the mailbox is full, but it can be listened to. Once a broadcast message is saved by a subscriber, the message is counted toward the storage allocation of the mailbox.
- Active time—Broadcast messages are active only between the start time and the end time specified for the message. Mailboxes will not receive a broadcast message until the start time passes. A broadcast message will be deleted from all mailboxes from which it has not yet been retrieved when the end time passes. MWI is updated according to when a broadcast message is active in the system.
- Message envelope—No sender envelope information (for example, sender name or number, or the date and time the message arrived) is played for a broadcast message. A recipient does not know who sent a broadcast message, only that it is a broadcast message.
- Message controls—Subscribers cannot ignore, fast-forward, reply to, or forward a broadcast message. The message can be repeated, deleted, or saved after the subscriber has listened to it.
- Message Send—A subscriber cannot send a broadcast message from a mailbox. To send a broadcast message, you must log in to the AVT interface. Only users with access privileges to the AVT, and the "Voicemail Broadcaster" privilege in their profiles, can access the broadcast message menu items in the AVT.

Broadcast Messaging and VPIM

A broadcast message can be addressed to all sites in a network, or a subset of locations in the network. A single broadcast message is sent across the network from the local system to each remote system to which it was addressed—the remote recipient system replicates the message to all personal mailboxes on that system.

The VPIMv2 voice mail networking standard does not support a method for broadcast messaging between sites, so Cisco Unity Express and Cisco Unity have implemented this functionality via extensions to VPIMv2. These extensions require the following minimum releases:

- Cisco Unity Express 2.1 or a later release
- Cisco Unity Release 4.0(5) or a later release

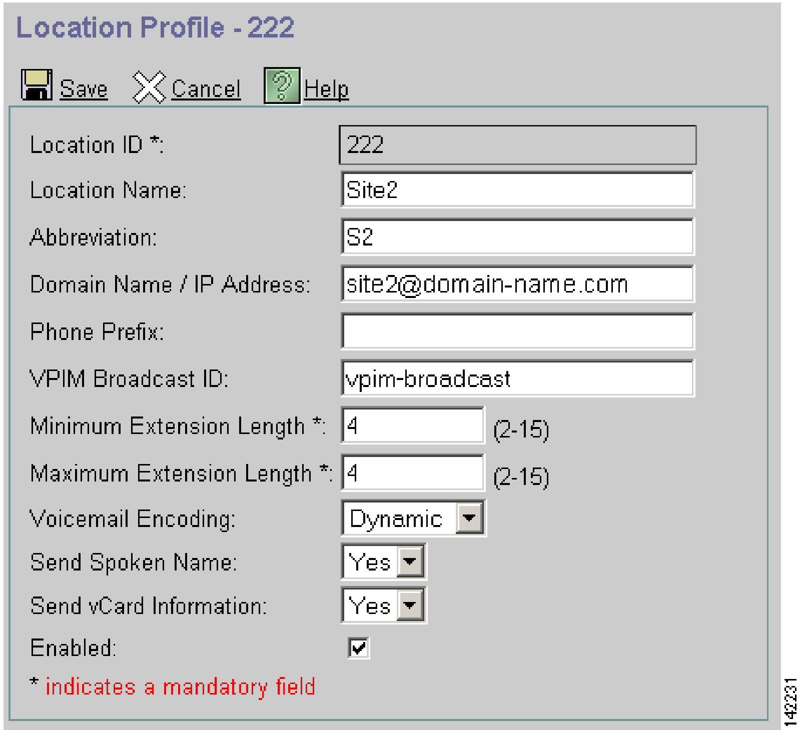
Previous releases of both Cisco Unity Express and Cisco Unity support standard VPIM networking, but not the broadcast extensions.

Broadcast Message Delivery to a Network Location

For a normal voice message, the recipient mailbox address is used by the destination voice mail system to decide whether an incoming VPIM message from a remote source system is a valid message, and thus whether to accept it. Cisco Unity Express rejects incoming VPIM messages addressed to invalid mailboxes.

Unlike a normal voice message, a broadcast message is not addressed to an individual extension (mailbox) on the destination system. To address a broadcast message, a "virtual broadcast message mailbox" tag must be used to allow the destination system to recognize the message as valid, to accept it, and subsequently to replicate it to individual mailboxes on the system. The "VPIM Broadcast ID" field in the configuration of a networking location is used for this purpose. See Figure 39.

Figure 39 VPIM Broadcast ID



The default value for the "VPIM Broadcast ID" field is "vpim-broadcast" for all Cisco Unity Express networking locations. Considerations about the use of this field are as follows:

- Broadcast networking on Cisco Unity Express is enabled by default. You can disable the ability for Cisco Unity Express to send and receive broadcast messages to or from other locations by entering an empty string (removing the current field value) in the "VPIM Broadcast ID" field of the destination location's configuration.
- The "VPIM Broadcast ID" field value is configured per networking location, including the local location. The value can be the same for each location provided the locations are all in different domains (that is, the domain name makes the full *xxx*@domain.name address unique).
- To enable network broadcast messaging between Cisco Unity Express and Cisco Unity sites in a network, the broadcast "VPIM Broadcast ID" field must be set to a numeric-only value (this is a Windows Exchange requirement that underlies the Cisco Unity messaging infrastructure), and must match Cisco Unity's broadcast mailbox ID. The general guideline is that you can use the Cisco Unity Express default "VPIM Broadcast ID" field value (alphanumeric) if your network contains only Cisco Unity Express sites. However, if you have a network of Cisco Unity Expresss and one or more Cisco Unity sites, then set all site values to a numeric value to ensure full intersite interoperability.

Nondelivery Receipt

Broadcast messages are sent to a large number of subscribers. No nondelivery receipt (NDR) is generated for a broadcast message that cannot be delivered to an individual subscriber at any of the destination locations (an NDR is generated for nonbroadcast voice mail messages to individual subscribers). If the destination location is the local Cisco Unity Express site, then an NDR will never be generated for a broadcast message. If the destination site is a remote location, an NDR for a broadcast message is provided for situations affecting the entire site, such as the following:

- Connectivity problems to the remote location
- Remote location not responding
- Mismatch in the "VPIM Broadcast ID" field
- Message content errors reported by the destination location

A separate NDR is generated for each location that cannot accept the broadcast message. Broadcast messages are sent from the AVT interface, but NDRs are placed into the sender's mailbox.

Comparison of "Everyone" Distribution List and Broadcast Message

There are two general methods to distribute a voice message to every subscriber on your system:

- The "everyone" system-provided public distribution list
- A broadcast message to the local system

There are various differences in how these two methods operate that may cause you to choose one method over the other for the distribution of a particular message. The following operational characteristics apply:

- Playout priority—A broadcast message is played out as the top priority in a recipient's mailbox. A message received via a distribution list is played out amid the normal list of new messages (based on its arrival time) and is not given any special priority.
- MWI control—A message received via a distribution list always gets MWI. A broadcast may or may not trigger MWI depending on the system's configuration (default is no MWI).
- Message options—A message received via a distribution list can be saved, deleted, ignored, and forwarded just like any other voice message; no special considerations apply. A broadcast message cannot be ignored, forwarded, fast-forwarded, or replied to, and must be listened to in its entirety by the recipient before other new messages can be reviewed. A broadcast message can only be saved or deleted.
- Future delivery—A message sent via a distribution list is delivered immediately to recipient mailboxes. A broadcast message can be recorded, but scheduled for a future delivery date and time.
- Identity of the sender—The sender's name and number are delivered to the recipient via the message header playout for a message received via a distribution list. The identity of the sender of a broadcast message is not known to the recipients, and the message cannot be replied to.
- Message expiry—A message received via a distribution list remains in a recipient mailbox as a new message until the recieving subscriber logs in and reviews the message, or the mailbox is deleted. A broadcast message can be set to expire on a certain future date and time so that recipients, who have not yet retrieved the message, will not hear the broadcast at all if they only log in to their mailboxes after the message has already expired. Broadcast messaging can therefore control the period of time for which a message's content is valid, but this cannot be done when a message is sent via a distribution list.
- Sender privileges—Any subscriber on the system can send a message to a public distribution list. Only users with administrative access to the AVT can send broadcast messages.

Voice Mail Number Handling

Various features within Cisco Unity Express are identified with numbers, as follows:

- Extension numbers associated with mailboxes
- Location codes identifying remote locations for voice mail networking
- Distribution lists

These numbers do not have to be mutually exclusive; for example you can define an extension 101, location code 101, and distribution list 101 on the same system. This is not a recommended configuration because it is confusing to the subscribers, but it is possible to do if needed by dial-plan considerations. When a voice message is addressed and the subscriber dials a number, Cisco Unity Express matches the number against all features identified by numbers. If there are multiple matches, the TUI prompts the subscriber to choose one of the elements to be entered into the message address.

Voice Mail Operator

Cisco Unity Express defines a system voice mail operator where calls are redirected if a caller does not respond to voice mail menus, or does not hang up after leaving a voice mail for a subscriber. The voice mail "operator" is triggered when the following voice mail prompt is reached: "If you have a mailbox on the system please press # or you will be transferred to the operator."

By default the voice mail operator is set to the AA pilot number. Alternately, you can set this to the extension of any employee in your office. To change this attribute, use the Voice Mail > Call Handling GUI window and change the "Voice Mail Operator Number" field.

AVT Operation for Voice Mail

The AVT interface offers administrative features for both the Cisco Unity Express AA and voice mail. Employees in your organization who are responsible for the following activities must have user profiles with access to the AVT defined on Cisco Unity Express (see Figure 25), regardless of whether they are also voice mail users:

- Send broadcast messages
- Manage (create or maintain membership) public distribution lists
- View private distribution lists of other subscribers
- Record spoken names on behalf of remote users entered into the local system

Voice Mail Deployment Models

Voice mail in your network can be designed as either a centralized, distributed, or hybrid deployment model. Which model is chosen depends in part on the voice mail availability you require during network outages.

The following sections summarize considerations to assess when selecting a voice-mail deployment model for your environment:

- Centralized, page 117

- Distributed, page 117
- Hybrid, page 118
- Voice Mail Failover, page 118
- Call Agent Failover, page 118

Centralized

A centralized deployment model provides for a the voice mail server that is located in a single site (central) and that is local to the employees located in that office, but remote for all employees at smaller outlying offices. Deploy Cisco Unity in a centralized model.

Cisco Unity Express 2.1 is not supported in a centralized deployment model and cannot to provide voice mail to employees that are not collocated with it in the same office. Cisco Unity Express can be used as the voice mail solution for a single site deployment (a standalone office), or in a distributed model (described in the "Distributed" section on page 117).

When Cisco Unity Express implemented with Cisco CME as the call agent, there is a 1:1 relationship between the Cisco Unity Express system and the Cisco CME system it serves (these two systems do not need to be collocated on the same router, but the relationship must be maintained and they should be collocated at the same site). You cannot configure a single Cisco Unity Express to provide voice mail to multiple Cisco CME sites, nor is it possible to configure two Cisco Unity Express servers to provide voice mail to the same Cisco CME system.

When Cisco Unity Express is implemented with Cisco CallManager as the call agent, there is a looser coupling between the physical location of the phone and the site where Cisco Unity Express is present as Cisco CallManager manages this relationship. It is technically possible therefore to have a single Cisco Unity Express provide voice mail to phones at multiple locations when under control of Cisco CallManager. However, this is not an officially supported or tested configuration and might have residual implications for the Cisco CallManager configuration components including the following:

- Codec choice used between sites
- Locations and regions configurations
- Route points
- Transcoder choices for calls

Note A network deployment featuring a single Cisco Unity Express to provide voice mail to phones at multiple locations under the control of Cisco CallManager is discouraged and is not supported by Cisco TAC.

Distributed

Although a centralized voice mail network design is often attractive from an administrative perspective, it is sometimes required to have local voice mail access, typically to increase availability during network failures. In a distributed design, the voice mail server is collocated at the same site as the employee for whom voice mail is provided. Either Cisco Unity (for large sites) or Cisco Unity Express (for small sites) can be deployed in a distributed design.

Hybrid

Many networks follow a hybrid deployment model with centralized Cisco Unity for the larger sites, and perhaps some Cisco Unity Express systems distributed at a selection of the smaller sites.

Voice Mail Failover

If Cisco Unity Express is deployed as the voice mailbox for an employee, then it is the permanent voice mailbox for that subscriber. Cisco Unity Express configuration does not allow for a deployment model in which Cisco Unity Express acts as a temporary "backup" for a permanent mailbox resident on a Cisco Unity (or other Cisco Unity Express) system elsewhere in the network. If voice mail must remain accessible during network outages, then a distributed voice mail network design should be deployed.

Call Agent Failover

When used with Cisco CallManager as the call agent, Cisco Unity Express works automatically with Cisco SRST to provide continuous access to voice mail regardless of the connectivity status between Cisco Unity Express or the IP phones and Cisco CallManager. Like the phones, Cisco SRST acts as the call agent of last resort when connectivity with Cisco CallManager is lost (primary, secondary, and tertiary Cisco CallManagers can be configured for Cisco Unity Express, just as they can for the phones). Call control automatically switches back from Cisco SRST to Cisco CallManager when contact is restored.

Note During Cisco SRST mode there are no changes in MWI state. All other Cisco Unity Express AA and voice mail functions continue to operate unchanged.

Cisco Unity Express is not consciously aware of "CallManager" versus "Cisco SRST" mode, and no configuration is required on Cisco Unity Express to enable this feature; however, the Cisco SRST router requires some configuration to determine voice mail call forward destinations for the phones and a SIP dial peer to route calls to Cisco Unity Express. Cisco Unity Express supports two means in which calls may arrive at the system—calls arriving via both mechanisms are handled at all times:

- SIP—Used for both Cisco SRST and Cisco CME as the call agent
- JTAPI—Used for Cisco CallManager as the call agent

When used with Cisco CME, Cisco Unity Express is collocated with the call agent and no failover scenarios apply.

Best Practices

The following summarizes the best practices in Cisco Unity Express voice mail design and configuration:

- On a new system, plan the license level to purchase carefully.

Cisco Unity Express licenses are not cumulative, so it is best to purchase the correct license for the number of mailboxes you expect to deploy in the office in the foreseeable future. If you purchase a 12-mailbox license to start with and then expand beyond that, you have to buy and install the 25 (or 50 or 100)-mailbox license. You cannot buy another 12-mailbox license and end up with a cumulative total of 24 mailboxes.

- On a new system, plan the appropriate default mailbox size carefully before you start entering the mailboxes into the configuration.

  The total system storage depends only on the hardware platform used (AIM-CUE or NM-CUE); it does not depend on the mailbox license installed. For example, if you start with the 25-mailbox license on an NM-CUE system, the default space allotted per mailbox is about 100 hours/25 = 240 minutes. If you enter 25 mailboxes, all the storage is allocated. If you subsequently upgrade to a 50-mailbox license, there is no space left to allocate to mailboxes 26 to 50. You must change the mailbox size of each of the existing mailboxes first, then add the new mailboxes. If you plan to grow or upgrade to more mailboxes, set the mailbox default parameters (default mailbox size) appropriately to allocate the actual time you require per mailbox, as opposed to using the system default calculation, which is total storage/mailbox license number.

- There are aspects of Cisco Unity Express operation that vary depending on which call agent is deployed with Cisco Unity Express.

  Most Cisco Unity Express AA and voice mail features are generic and operate the same way regardless of the deployment model used. There are some minor differences,though, between Cisco CME and Cisco CallManager operation, including the following:

  - AA control of calls after a transfer—With Cisco CME, a SIP blind transfer is done and once the call is transferred, the AA script has no further control of the call. So any error branches in the AA script to handle busy, not available, or nonexistent extension conditions will never execute. Instead, Cisco CME treatments (busy tone, overflow tone, or announcements) are heard by the caller. With Cisco CallManager, a consultative transfer is done via JTAPI and the AA script retains control of the call for error condition execution.

  - Rendering MWI on a phone—On Cisco CME, red light MWI can only be done for extension appearances on button 1, and a flashing icon is shown for other button appearances. This is not configurable. On Cisco CallManager, red light or flashing icon MWI can be configured for any button on the phone.

  - Direct transfer to voice mail—Although Cisco Unity Express 2.1 does not explicitly support this feature, there are Cisco Unity Express 2.1 configurations that can result in direct transfer to voice mail. These methods differ for Cisco CME and Cisco CallManager. More information on this is available in the Tech Tip entitled “Transfer a Caller Directly into a Unity Express Mailbox” at the following URL:
    http://www.cisco.com/en/US/products/sw/voicesw/ps5520/products_tech_note09186a00802ab979.shtml

  - Collocation of phones and Cisco Unity Express mailboxes—For Cisco CME there is a 1:1 relationship between the phones under control of Cisco CME router and the Cisco Unity Express system providing voice mail services to these phones. Multiple Cisco CME systems cannot be served by a single Cisco Unity Express, nor can multiple Cisco Unity Express systems serve a single Cisco CME. With Cisco CallManager, this relationship is looser. Although Cisco recommends that the phones for which the Cisco Unity Express system provides voice mail be collocated at the same Cisco Unity Express site, there is nothing in the configuration that enforces this relationship.

    - Extension length—For Cisco CME, all the phone extensions associated with mailboxes must be of a fixed length. The absolute length does not matter, but they cannot vary in extension length. If they do, MWI does not operate correctly. For Cisco CallManager, this restriction does not apply and extensions can be of any length.

- Cisco Unity Express is an integrated AA and voice mail system. Although the license level explicitly references only the number of mailboxes, the AA is always available as well. However, it is your choice of which features to use. You can deploy Cisco Unity Express as an AA system only or as a voice mail system only.
- For broadcast messaging, the Cisco Unity Express default value for the "VPIM Broadcast ID" field is" vpim-broadcast." If voice mail networking with Cisco Unity systems is required, this field must be set to a numeric-only value.
- MWI for GDMs require the extension associated with the GDM to be a button appearance on the phone where MWI is needed.
- Set location IDs for voice mail networking locations to be at least three digits if you require Cisco Unity Express to interwork with a Cisco Unity system now or in the future.
- Encourage new subscribers to work through the new mailbox enrollment tutorial. This ensures that each subscriber records a greeting, records a spoken name, and changes the default PIN. The spoken name is used in many other Cisco Unity Express features (such as address confirmation and sending the spoken name with the message for header playout to the recipient at a remote system). It enhances the overall user experience of the voice mail system.
- If a subscriber must administer (and log in to) a GDM, ensure that the subscriber is assigned to be both an owner and a member of the group with which the GDM is associated.
- All subscribers who must be able to send broadcast messages must be granted access privileges to the AVT.
- Various features within Cisco Unity Express are identified with numbers, such as extension numbers, network location codes, and distribution lists. To optimize the end user experience of addressing messages, it is best to configure numbers for these items that do not overlap.
- For user IDs to appear in the dial-by-name feature, a user profile definition must exist on Cisco Unity Express. A mailbox need not necessarily be assigned to a user with a profile defined for the purposes of dial-by-name functionality; however, if spoken name confirmation is required for such a user, a mailbox is requried.
- They do not need to have a mailbox assigned, although if spoken name confirmation for these users is required, that can only be done via a mailbox.
- Configure the Cisco Unity Express system to do regular backups so that you can recover voice mail configuration and message content after upgrades or destruction media failures.
- Cisco Unity Express subscriber PINs do not expire by default. For added security, it is recommended that you configure a suitable expiration time frame in the Cisco Unity Express system policy (use the Defaults > User GUI window).
- When making configuration changes to the system, be sure to make the configuration permanent by doing either a "write" statement from the Cisco Unity Express CLI, or choosing the Save Unity Express Configuration button on the Administration > Control Panel GUI window. If Cisco Unity Express reboots or loses power with unsaved changes, the last saved configuration will be loaded. Cisco Unity Express follows the Cisco IOS router model of a startup configuration and a running configuration.

- Although the Cisco Unity Express GUI allows you to look at the status of an individual mailbox, it does not have a single window overview with a consolidated listing of all the mailboxes on the system. If this view is necessary for tracking or monitoring purposes the **show voicemail mailboxes** command can be used to obtain needed information:

```
cue# show voicemail mailboxes

OWNER          MSGS NEW SAVE DEL BCST MSGTIME  MBXSIZE   USED
"User1"         3    2    1    0   1    77       5520      1 %
"User2"         0    0    0    0   0    5        5520      1 %
"User3"         1    0    1    0   1    21       5520      1 %
"User4"         2    1    1    0   0    47       5520      1 %
"User5"         0    0    0    0   1    0        5520      0 %
"User6"         1    1    0    0   1    21       5520      1 %
```

A

B

C

D

O

P