Cisco Unified Messaging Gateway 1.0 Design Guide

First released: March 10, 2008
Last updated: April 13, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number: OL-16087-01

Cisco Unified Messaging Gateway 1.0 Design Guide

CONTENTS

Overview

First Published: February 28, 2008

This chapter addresses the challenges in current VPIM messaging networks, why Cisco Unified Messaging Gateway (Cisco UMG) can resolve the issues, what extra features Cisco UMG can provide to the network, and basic information about Cisco UMG access and scalability.

This chapter contains the following sections:

Challenges of Today's Fully-Meshed VPIM Messaging Network

Cisco Unity Express provides networking functionality for message exchange between users of different Cisco Unity Express nodes. A networked Cisco Unity Express setup requires all Cisco Unity Express nodes to form a fully meshed network, within which each Cisco Unity Express must be able to reach all other Cisco Unity Express nodes directly, and current Cisco Unity and Cisco Unity Express networks can only scale up to 500 nodes. This approach carries the obvious limitations on features, scalability, and manageability.

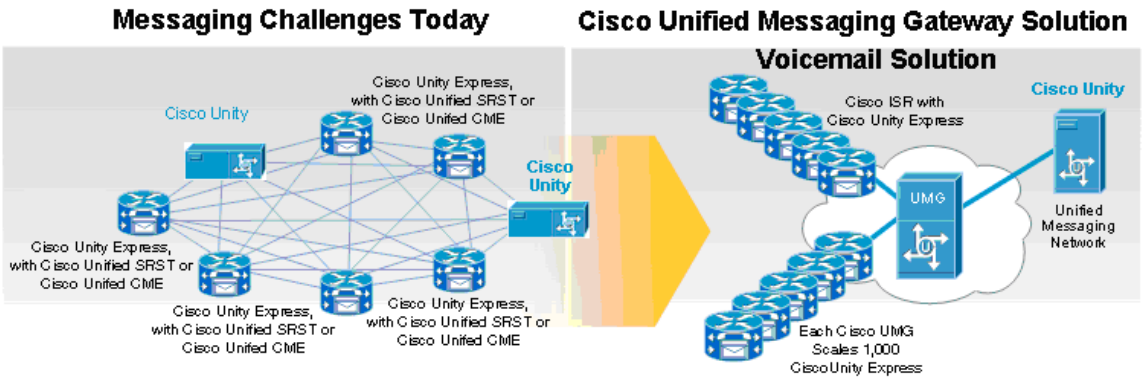
Benefits of Using Cisco UMG in Today's VPIM Messaging Network

Cisco UMG is software, based on Linux, that runs on a Network Module on Cisco Integrated Services Routers. Cisco UMG acts as the central hub for Cisco Unity, Cisco Unity Connection, and Cisco Unity Express to provide intelligent routing for voice mail messages, exchanging subscriber and directory information among the voice mail systems, and interoperability with third party voice mail systems (such as Avaya Interchange) over VPIM networks. This end-to-end message networking functionality is required by medium to larger distributed enterprises in order to seamlessly migrate to the Cisco Unified Communications solution.

From a management perspective, Cisco UMG allows Cisco Unity Express and Cisco Unity to be networked in a hub-and-spoke topology instead of today's fully meshed VPIM topology. This approach dramatically reduces the VPIM connections between mail systems, and simplifies the configuration

effort on each system. Each mail system (Cisco Unity Express, Cisco Unity, Avaya Interchange) only needs to configure the connection between itself and Cisco UMG. Cisco UMG then handles message routing and delivery using the directory information of all mail systems that register with it.

Figure 1 Comparison of a Current VPIM Network with a Cisco UMG Controlled Messaging Network



Cisco UMG also brings some new features into the VPIM network. The use of network wide spoken-name confirmation and a system distribution list enables the scaling of the single mail system feature to multiple nodes.

Note In this document, mail systems (Cisco Unity Express, Cisco Unity, or Avaya Interchange) in a Cisco UMG network are referred to as endpoints or nodes.

The following features are esupported by Cisco UMG 1.0.

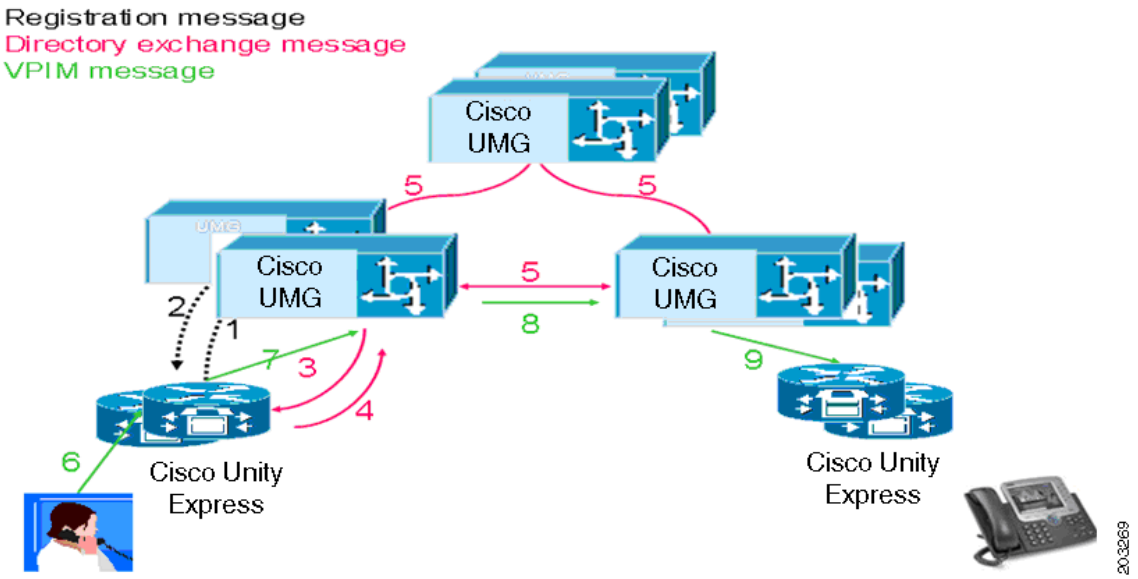
- Autoregistration with Cisco Unity Express (3.1 and later versions)
- Manual registration and provisioning of Cisco Unity, Cisco Unity Connection, and Avaya Interchange. You can manually provision versions of Cisco Unity Express earlier than 3.1.
- Centralized user directory depository
- Intelligent Message Routing and Delivery
- Spoken-name confirmation across the messaging network
- System Distribution List (SDL) and System Broadcast Messages (SBM)
- NAT support
- Simple Management and configuration using Cisco IOS software like CLI interface
- Seamless integration with Cisco Unity and Avaya Interchange systems
- Redundant and self-recoverable network
- Software Backup and Restore

As shown in Figure 2, the general procedures in a Cisco UMG controlled messaging network include:

- Cisco UMG registers voice mail systems as nodes into its database (see Steps 1 and 2 in Figure 2).
  - Manual registration for Cisco Unity, Avaya Interchange, and Cisco Unity Express 3.0 and earlier versions
  - Auto registration for Cisco Unity Express 3.1 and later versions

- Directory Information Exchanges between Cisco UMG and auto-registered endpoints (Cisco Unity Express 3.1 and later). For all manually registered voice mail systems, manual provisioning is required for directory information (see steps 3 and 4 in Figure 2).
- Directory Exchange Information is pushed out from the primary Cisco UMG (to which endpoints registered) to all peer Cisco UMGs in the network in a unicast, fully meshed way (see Step 5 in Figure 2).
- Originating Cisco UMGs perform message routing based on the directory table saved in their databases to find terminating Cisco UMGs (see steps 6 and 7 in Figure 2).
- Messages are delivered from a subscriber to remote SDL/SBM/subscriber(s) using VPIM across the Cisco UMG network (see steps 8 and 9 in Figure 2).

Figure 2 General Procedures in the Cisco UMG Network



Cisco UMG Access information

Cisco UMG is offered in two forms:

- Network Module (NME-UMG)
- Enhanced Network Module (NME-UMG-EC) that supports different number of nodes

Cisco UMG hardware includes a CPU to offload processing from the router CPU such that Cisco UMG has minimal impact on the router CPU, and also storage (hard disk on the NM) for directory exchange information.

Similar to Cisco Unity Express, the Cisco UMG network module connects to its host router using a back-to-back Ethernet configuration that physically travels across the backplane of the router. The most common way to configure the Cisco UMG module is to use the unnumbered IP address method. By entering the **ip unnumbered** command, as shown in the following configuration example, you enable the Cisco UMG module to consume an IP address in the subnet of the network associated with a particular router egress port, such as GigabitEthernet 0/0. The router interface with which the Cisco UMG interface is associated must be in an "up" state at all times for Cisco UMG to communicate.

Note This method requires the configuration of a static route to the Integrated-Service-Engine interface.

IP Unnumbered Configuration: Example

The following configuration example shows how to use the **ip unnumbered** command to enable the Cisco UMG module to consume an IP address in the subnet of the network associated with a particular router egress port (GigabitEthernet 0/0).

```
interface GigabitEthernet0/0
  ip address 10.68.10.1 255.255.255.0
!
interface Integrated-Service-Engine1/0
  ip unnumbered GigabitEthernet0/0
  service-module ip address 10.68.10.10 255.255.255.0
  service-module ip default-gateway 10.68.10.1
!
ip route 10.68.10.10 255.255.255.255 Integrated-Service-Engine1/0
```

The IP address of the Cisco UMG module in the example is 10.68.10.10. The default-gateway on the Integrated Service Engine must be set to the IP address of the Ethernet interface on the router that the unnumbered statement refers to (10.68.10.1 in the example). It is also possible to use a subinterface or a loopback interface as the parameter for the **ip unnumbered** command (for example, **ip unnumbered GigabitEthernet0/0.1**).

To access the Cisco UMG, initiate the session from enable mode on the hosting router using the following command:

```
service-module integrated-Service-Engine 1/0 session
```

Note Because Cisco UMG is an embedded Linux application, you cannot access the Linux operating system using CLI commands, Telnet, or any other interface.

For Cisco UMG 1.0, no GUI access is implemented.

Study and Analyze Your Cisco UMG Controlled Messaging Network

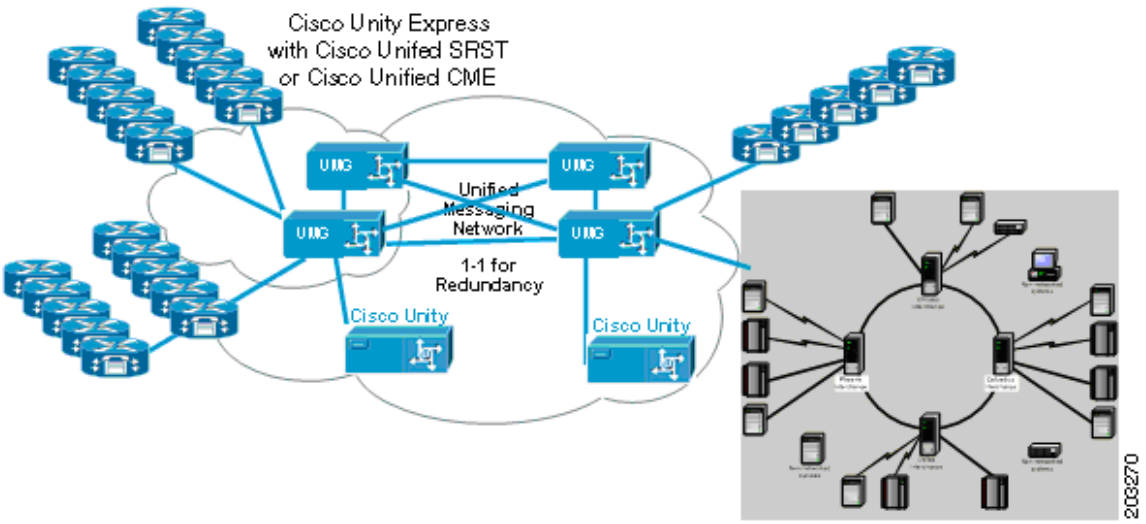
First Published: February 28, 2008

A complete Cisco UMG messaging network consists of one or more Cisco UMGs and the endpoints which can be Cisco Unity Express, Cisco Unity, or Avaya Interchange.

A Cisco UMG controlled messaging network is a mix of fully-meshed connections (between Cisco UMGs) and hub-and-spoke connections (between the Cisco UMG and its registered endpoints).

Note In this document, mail systems (Cisco Unity Express, Cisco Unity, or Avaya Interchange) in a Cisco UMG network are described as endpoints or nodes.

Figure 1 A UMG controlled Messaging Network Topology



Before designing a Cisco UMG network, you must have a complete knowledge of:

- How much new network traffic will be introduced by Cisco UMG. (The detailed bandwidth considerations are discussed in Cisco UMG deployment section.)
- How to setup network security and what agreement has been reached with the IT department regarding UMG requirements
- How to setup the network QoS parameter
- What is the distribution of system traffic, along with a geographic map and traffic patterns
- How does the Cisco Unity Bridge and compare with Cisco UMG based on system migration and call control configuration

Network Traffic Introduced by the Cisco UMG

Cisco UMG controlled messaging network introduces the extra network traffic into today's VPIM network during endpoint registration, directory exchange, and Cisco Unity Express remote lookup. (The detailed bandwidth consideration will be discussed in UMG deployment section below)

During Cisco Unity Express registration or de-registration process, the XML messages between Cisco Unity Express and Cisco UMG use HTTP request and response format. The registration implementation, which has no keep alive mechanism between endpoints and the Cisco UMG, allows endpoints to re-register with Cisco UMG with an expiration timer that is configurable on Cisco UMG.

The directory exchange messages are STMP based, and can be sent between Cisco Unity Express and Cisco UMG or between different Cisco UMGs. Directory exchange between Cisco Unity Express and Cisco UMG is invoked when the Cisco Unity Express first registers with its primary Cisco UMG, and when any subscriber information is modified on the Cisco Unity Express. When there is a change in the subscriber's information, the Cisco Unity Express accumulates the update on its own database until the configurable accumulation timer is reached and then sends the directory update to its primary Cisco UMG. A directory exchange between Cisco UMGs can be triggered by inserting a new Cisco UMG into the network or by modifying any directory information on the Cisco UMGs. Note that the directory exchange between the Cisco UMGs happens as soon as any information is updated on any of Cisco UMG in the network.

Cisco Unity Express remote lookup provides a real time method for a Cisco Unity Express to learn about the remote user's spoken name and location information. The remote lookup process utilizes the HTTP request and response mechanism in the Telephony User Interface (TUI) session.

You must carefully calculate the network bandwidth used by both the initial and ongoing extra traffic caused by bulk registration, directory exchanges, and remote lookups. If there is a large number of Cisco Unity Express subscribers on a Cisco UMG network, they might experience a delay if the network bandwidth is limited.

Note The Auto-Registration, directory exchange, and remote lookup are supported on Cisco Unity Express 3.1 and later with Cisco UMG 1.0

UMG Network Security

Cisco UMG release 1.0 does not support inherent security protocols. The message exchange between nodes is not encrypted by Cisco UMG. If encryption is needed, it should be done using VPN or IPSEC tunnels on your Cisco routers. Cisco UMG supports the configuration of a NAT table to map internal and external IP addresses, if needed. Cisco UMG also supports application level security with a shared secret (user name and password) between the UMG and the Cisco Unity Express version 3.1 nodes to prevent any unauthorized node from accessing the Cisco UMG network. Cisco UMG, when used in conjunction with its host router, supports the concept of white and black lists, which are lists of devices that are either allowed or blocked from accessing, registering, or transferring messages through the Cisco UMG.

Be aware that the following TCP ports are required by Cisco UMG to perform endpoint registration, directory exchange, Cisco Unity Express remote lookup, and the message delivery.

- Registration — default HTTP port 80
- Directory Request/Response/Update — SMTP/VPIM default port 25
- Directory remote lookup — default HTTP port 80
- Message Delivery — SMTP/VPIM default port 25

Cisco UMG Network QoS Overview

Unlike the voice network, the Cisco UMG network, a SMTP based VPIM messaging network, does not carry the delay sensitive real-time traffic. Therefore, there is no requirement on the Cisco UMG itself to provide any call admission control or QoS mechanism. The QoS of the Cisco UMG network relies on QoS control through the Cisco routers or other devices in the network.

Some extra resources are required with certain Cisco UMG features:

- Remote Lookup consumes extra CPU cycles on Cisco UMG blades. It may cause delays when a large amount endpoints or nodes are registered in a Cisco UMG controlled system.
- Spoken-Name which is attached to the message will increase the bandwidth usage. By default, Cisco UMG disables spoken-name.

Comparison of Cisco UMG and Unity Bridge in a VPIM Network

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

The Cisco Unity Bridge server is connected to a phone system and communicates with Avaya Octel servers by using the Octel analog networking protocol. The Cisco Unity Bridge server sends messages to Cisco Unity by using a digital protocol that is based on the Voice Profile for Internet Mail (VPIM) protocol, with proprietary extensions.

Cisco UMG acts as network gateway between Cisco Unity, Cisco Unity Express, and Avaya Interchange using the Voice Profile for Internet Mail (VPIM) protocol. With Cisco UMG, the subscribers on Cisco Unity, Cisco Unity Express, or Avaya Interchange can send and receive message across three different mail systems.

Because Cisco Unity Bridge and Cisco UMG provide similar functionality, consider the following points when deciding which product to use to fit a customer's network deployment. Cisco Unity Bridge provides a simple messaging network solution between Cisco Unity and Avaya Interchange. If this is all the functionality the customer needs, Cisco Unity Bridge can be used. If the customer's network has multiple Cisco Unity Express nodes and the customer has considered migrating subscribers from an Avaya phone system to a Cisco Unified Communication System (such as Cisco Unified Communications Manager or Cisco Unified Communication Manager Express), using Cisco UMG is a good way to satisfy the customers requirements.

Network Infrastructure Considerations for a Messaging Network Controlled by Cisco UMG

First Published: February 28, 2008

This chapter discusses how to prepare to deploy Cisco UMG in your messaging network. Topics addressed in this chapter include:

- Choose TFTP and FTP servers for Cisco UMG installation, backup, and restore
- Choose endpoint software versions (Cisco Unity Express, Cisco Unity, and Avaya InterChange)
- Choose Cisco UMG hardware based on message network scalability and sizing
- Choose the locations that Cisco UMGs will be installed
- Choose NTP servers for date and time synchronization between Cisco UMG and its endpoints

TFTP and FTP Servers

Similar to Cisco Unity Express, Cisco UMG boot loader uses TFTP to load the RAM-based Linux kernel from a network location as the first step of software installation or upgrade. FTP is used for the remainder of the software installation, upgrade, and for backup and restore communication.

Setup the FTP server so that all Cisco UMGs using it have reliable, high-speed, and secure access to the FTP server. Consider the following:

- Backup and restore bandwidth required— The size of the backup depends on the number of nodes registered with the Cisco UMG, the storage capacity of each site, and backup/restore options (configuration only or configuration + data with much higher bandwidth requirement)
- Security of the FTP connection — A Cisco UMG backup or restore operation transmits directory information of subscribers over the FTP connection. If ensuring the privacy of this information is important, use IPsec technology between the Cisco UMG site and the FTP server.
- Security of information on the FTP server — A Cisco UMG 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 UMG access to the FTP server — Ensure that Cisco UMG can access the FTP server by either name or IP address. If the FTP server is accessed by name, then ensure that Cisco UMG is DNS enabled. Any firewall between the FTP server and Cisco UMG must allow FTP traffic to go through.

FTP Server Configuration Guidelines

Each type of FTP server is configured differently. This section provides only general guidelines for the types of features and characteristics your FTP server needs to work with Cisco UMGs:

- 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).
- Do not use anonymous FTP for Cisco UMG 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 specific directory is configured as the backup directory for Cisco UMG, do not manually delete any files or directories from the directory configured on Cisco UMG.
- If a single FTP server is used to store backups from multiple Cisco UMGs or is shared with Cisco Unity Express, ensure that the directory for each Cisco UMG and for Cisco Unity Express is different.

Endpoint Software Versions Supported

The Cisco UMG supports the following endpoints with versions of:

- Cisco Unity Express 2.0 and higher versions
- Cisco Unity 4.05 and higher versions with Exchange only
- Avaya Interchange version 5.4 only

Cisco UMG 1.0 supports endpoint autoregistration with Cisco Unity Express 3.1 and higher versions only. Customers can stay with the older version of the Cisco Unity Express with manual provision all Cisco Unit Express information on the Cisco UMG. The benefit of this approach is that any existing Cisco Unity Express features will not be broken by an upgrade to a newer version. The trade off will be the flexibility and easy management introduced by auto registration with Cisco Unity Express 3.1 and higher versions. Because the automatic directory exchange is not supported between older versions of Cisco Unity Express and Cisco UMGs, all subscriber information on the Cisco Unity Express must be manually configured on the Cisco UMGs. When you make modifications on Cisco Unity Express, you must also manually update Cisco UMG. Certain features like spoken-name confirmation across multi-mail systems are be supported.

We recommend that you use Cisco Unity Express 3.1 and higher versions. This requires a full regression test of the existing Cisco Unity Express features on Cisco Unity Express 3.1 before deploying the Cisco UMG into the network.

When integrating Cisco Unity with Cisco UMG, Cisco Unity needs to work with Microsoft Exchange only (MX records are required for Cisco UMG). Avaya Interchange versions other than 5.4 are not supported by the Cisco UMG 1.0.

Note Cisco Unity with Domino is not supported with Cisco UMG 1.0

Cisco UMG Sizing and Network Capacity

Cisco UMG hardware has two forms, NME-UMG with a maximum of 250 nodes support, and NME-UMG-EC with up to 1000 nodes support. The number of total subscribers who can be supported are 12,500 on NME-UMG and 50,000 on NME-UMG-EC. The number of subscribers is calculated based on 50 subscribers on any single Cisco Unity Express node which is registered with Cisco UMG. The Cisco UMG capacity is tied to both the maximum number of nodes support and the maximum number of subscriber support that comes first. For example, if the Cisco UMG network has Cisco Unity and/or Avaya Interchange endpoints with a large number of subscribers, the number of nodes which can register on the UMG will be significantly less than 250 or 1000.

Note We recommend NOT mixing the NME-UMG-EC and NME-UMG hardware on the Cisco UMG primary and secondary pair setup.

The topology between the Cisco UMG and its nodes (Cisco Unity Express, Cisco Unity, or Avaya Interchange) is a hub-n-spoke. However Cisco UMG connects other Cisco UMGs in the same network with fully meshed topology. A complete Cisco UMG controlled messaging network can connect up to 20 Cisco UMGs (10 primary Cisco UMGs and 10 secondary Cisco UMGs as a fully redundant deployment) with total of up to 500,000 subscribers.

Below is the licensing information about Cisco UMG:

- Basic license levels thatyou can order with product
  - UMG-LIC-25
  - UMG-LIC-100
  - UMG-LIC-500
  - UMG-LIC-1000
- Additional license levels that you can added when ordering Cisco UMG
  - UMG-LIC-25-UPG
  - UMG-LIC-100-UPG
- Additional spare licenses you can add later
  - UMG-LIC-25-UPG=
  - UMG-LIC-100-UPG=

Note Aditional licenses can be ordered as spare licenses; however, upgrading a license from 250 nodes to a higher number may require purchasing the higher capacity hardware (NME-UMG-EC) if the original module is NME-UMG.

When purchasing Cisco UMG, preorder a Cisco Integrated Services Router (Cisco ISR) with a network module slot.

Locations to Install Cisco UMGs

As an application running on the Cisco ISR network module, the Cisco UMG can be installed on any Cisco ISR with a network module (NM) slot. Although the Cisco UMG software cannot be coresident with the Cisco Unity Express on the same NM, the Cisco UMG software can be installed on a separate NM slot but co-resident with Cisco Unity Express NM on the same Cisco ISR. The Cisco ISR can run Cisco Unified Communication Manager Express, Cisco Unity Express, Cisco UMG, gatekeeper, or any other IOS features from Release 12.4(15)T or higher.

When considering the location to install the Cisco UMG, the following factors should be taken into account:

- Is a spare Cisco ISR NM slot available in the current network? For example, if there is gatekeeper Cisco ISR with an extra NM slot open, installing Cisco UMG on the same router will consolidate both Voice and messaging network endpoint management, and eliminate a request for an extra Cisco ISR.
- Traffic pattern and characteristics on the current network. Besides the extra network traffic during endpoint registration, directory exchange, and Cisco Unity Express remote lookup, the Cisco UMG acts as proxy for message delivery between two registered endpoints. It is recommended to install the Cisco UMGs at the edge of each region, such that no extra WAN traffic will be introduced back and forward across regions during the message delivery.
- When deploying Cisco UMGs with redundancy, the primary Cisco UMG does not need to be the same location as the secondary Cisco UMG; however we recommend you install the secondary Cisco UMG in the same graphic region or area as the primary Cisco UMG. A reliable IP connectivity between primary and secondary Cisco UMGs is also required to reduce the directory information out-of-sync possibility. Comparing to a communication system with redundant call control agents, the Cisco UMG redundancy does not have strict delay restriction because of the nature of VPIM traffic, although less network delay is preferred.

Date and Time Management in UMG-Controller Messaging Network

Similar to Cisco Unity Express, Cisco UMG configures date and time via two system configurations:

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

With a NTP server which is Coordinated Universal Time (UTC) and the time zone setting (the offset from UTC to local time) in the network, the clock is synchronized with the NTP source during Cisco UMG software startup.

We recommend the following practices for optimal date and time control:

- Use a robust NTP server in the network for maximum clock stability.
- Synchronize all the mail systems with the NTP source in a Cisco UMG controlled messaging network. An NDR may be returned to the messaging sender if time out-of-sync exists between endpoints and Cisco UMGs.
- Use the Cisco UMG hosting router (or any other low-end router) as the NTP server only as a last effort. 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.

Domain Name Server in a Cisco UMG-Controlled Messaging Network

Cisco UMG and the Cisco Unity Express endpoints can choose to use IP address to address each other, instead of DNS hostname. The benefit of this approach is to improve the message exchange performance without involving the DNS lookup.

When DNS is enabled in the network, Cisco UMG performs a reverse DNS lookup to resolve the inbound IP addresses to the hostname. If one or more Cisco Unity nodes exist in the network, Cisco UMG must be assigned with a MX-record and hostname in the Cisco Unity DNS domain. When you configure the Cisco Unity node on the Cisco UMG, the hostname field can be a Cisco Unity IP address, Cisco Unity A record, or Cisco Unity MX record depending on how Cisco Unity DNS resolves the addresses.

When deploying the Cisco UMG redundancy with a Cisco Unity system, two MX rewords must be assigned to the Cisco UMG with the same Cisco UMG hostname but different IP addresses and different priorities. From the perspective of Cisco Unity, the primary and secondary Cisco UMGs are transparent because this information is configured only on the DNS server. The primary and secondary Cisco UMGs share the same hostname but with different IP addressed and different priorities on MX records. The Cisco Unity node sends an outgoing message to a Cisco UMG with higher priority (primary Cisco UMG), If the primary Cisco UMG fails, DNS returns the secondary Cisco UMG IP address to the Cisco Unity node with a lower priority to route and deliver the messages.

See the *Cisco Unity System Administrator Guide* for detailed information about configuring the Domain Name Server.

Deployment Models for Cisco UMG

First Published: February 28, 2008

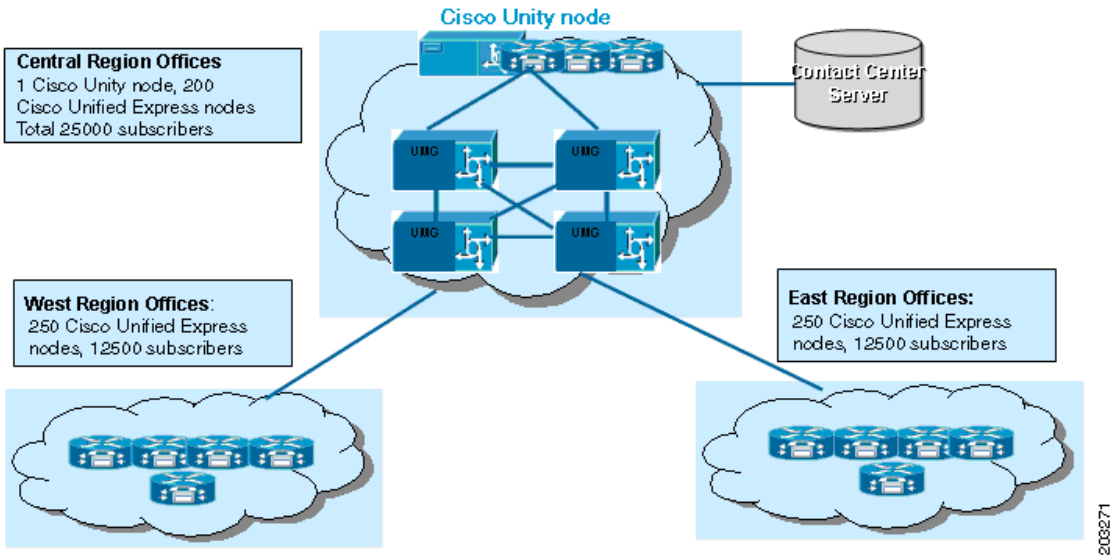
If a business wants to deploy a Cisco UMG controlled messaging network with multiple sites, one of the key network design decisions that you must make is whether the Cisco UMGs will be centralized at one site or distributed on multiple sites.

This chapter discusses the advantages and disadvantages of the various types of Cisco UMG deployments and contains the following sections:

Note The deployment scenarios in this chapter focus on medium to large enterprise businesses with at least 50 voicemail systems including Cisco Unity Express, Cisco Unity, and/or Avaya Interchange in the network.

Centralized Cisco UMG Deployment

Figure 1 Centralized Cisco Deployment Model



In the centralized Cisco UMG deployment model, all the Cisco UMGs are installed in one location (probably the company headquarters, labeled central region offices in Figure 1). Cisco Unity and Cisco Unity Express are used in the central region as voicemail systems. All branch offices in all regions (west and east in the figure) are equipped with Cisco Unity Express as voicemail systems. The WAN connections are setup between branches and the headquarters. The Contact Center Application is running in the central region.

The advantages of this model are:

- Easy installation on Cisco UMG hardware because all the Cisco UMGs are located in the same region.
- Directory exchange between Cisco UMGs does not consume the WAN bandwidth between remote branch offices (east and west regions) and the central region.
- Hardware cost is less when using Cisco UMG. A NME-UMG-EC can host up to 1000 nodes with one extra unit installed for failover scenario.

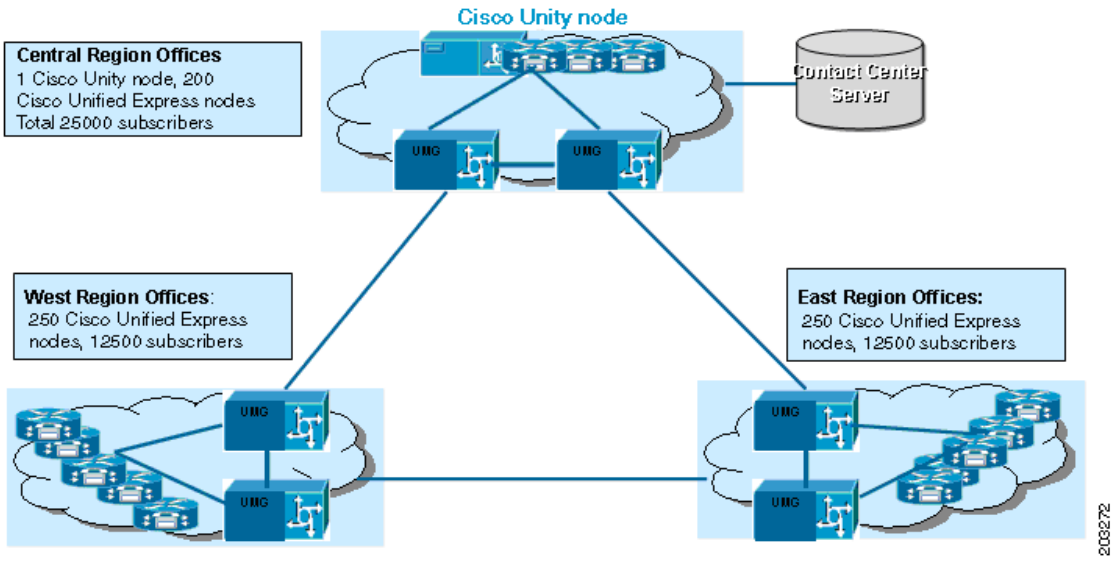
The disadvantages of this model are:

- No message survivability in the remote sites when the WAN link between remote branches and the central region is unreachable. In this messaging network, Cisco UMG is the proxy for any message sent between two nodes. If a WAN link is down, even in the same region, the subscriber cannot leave a message to any subscriber sitting on different Cisco Unity Express database.
- Increases the traffic load on the WAN link. For example, if a subscriber on CUE1 in the West Region is sending a message to a subscriber on CUE2 in the same region, CUE1 sends a VPIM message to the Cisco UMG across the WAN link, after the Cisco UMG searches its directory table to find a match, it delivers the message to the subscriber on CUE2 in the west region using the WAN link again. For every message within the same region, the same message must travel the WAN link twice and consume bandwidth.

- Extra WAN traffic load occurs between Cisco Unity Express nodes on the remote sites and the Cisco UMGs in the headquarters during directory exchanges and during Cisco Unity Express node remote lookups from any branch office to search remote subscribers.
- Limited network scalability especially when the remote office size grows. Although extra Cisco UMG units can be installed on the central site, the WAN link limitation between remote regions and the central site can impact how reliably messages are delivered.

Distributed Cisco UMG Deployment

Figure 2 Distributed Cisco Deployment Model



In the distributed Cisco UMG deployment model, every region has its own primary and secondary Cisco UMG. The Cisco Unity Express nodes on remote sites register with the local Cisco UMG instead of Cisco UMGs in the headquarters. The WAN link is used to connected remote sites to the central site and between remote branches.

The advantages of this model are:

- Full message survivability on the remote sites when the WAN link between the remote site and the central site is down. All the messages between different Cisco Unity Express mail systems within the same region do not have to be proxied by the Cisco UMG across the WAN link to the central site.
- Less network bandwidth is used on the WAN link. The local Cisco UMG can route and deliver the message within the region without utilizing the WAN link. Unlike the centralized model, every message between Cisco Unity Express nodes within a region must travel the WAN link twice. Because people work more closely within the same region, messages are delivered more frequently within the same region, saving more WAN bandwidth.
- Easily scaled on remote regions. On each remote site, a pair of Cisco UMGs (primary and secondary) can support up to 250 nodes with NME-UMG and up to 1000 nodes with NME-UMG-EC, without concern about WAN resource consumption during message delivery.

- No extra license cost compared to the centralized Cisco UMG model if the same number of nodes are deployed in the entire distributed Cisco UMG network. For example, as shown in Figure 2, the west region and the east region have 250 nodes each, and the central site has 201 nodes. So total number of licenses needed is 750, which can be either installed on the central site or distributed to multiple regions. For example, you can put 250 node licenses on the east region, 250 node licenses on the west region, and 250 node licenses on the headquarter.
- No traffic load on the WAN connection during directory exchanges between Cisco Unity Express nodes in remote regions and their hosting Cisco UMGs. Also no traffic is loaded on the WAN connection during remote lookups from the remote site Cisco Unity Express endpoints.
- Increased flexibility on feature management, such as spoken-name. Instead of turning on the feature on the central site Cisco UMG that includes all the nodes in the entire message network. The Cisco UMGs in each region can control the features based on resource availability.

Note The secondary Cisco UMG must purchase the same license as the primary Cisco UMG, in either the centralized or distributed model.

The disadvantages are:

- Extra Cisco UMG units must be purchased and installed on remote sites.
- During the directory exchange between Cisco UMGs, the traffic on the WAN connections may have spikes in volume. These bursts in traffic volume happen only when the Cisco UMG is inserted in to network for the first time and all endpoints register, or when out-of-sync directory information on the Cisco UMG is detected and is unrecoverable. After the system full directory exchange is complete, the subscriber informationis stable. In most cases, Cisco UMGs are capable of handling the small updates needed for out-of-sync directory information. The burst traffic that floods into the WAN connections is not significant if the system administrator installs and configures the Cisco UMGs during off-peak hours and verifies that the WAN bandwidth meets the requirement before installation. For slower links, consider turning off the spoken-name confirmation feature to reduce bandwidth usage.

WAN Bandwidth Requirement for Distributed Model

The following three examples use the West Region in Figure 2 as an example. This network information applies to all three examples:

- 250 Cisco Unity Express nodes in the West Region office
- 50 subscribers on each Cisco Unity Express node
- Total number of subscribers = 250 x 50 = 12500

No users have spoken-name turned on: Example 1

- SMTP message size during directory exchange: (assume a vCard size is about 180 bytes). smtpPsize= 180 x 12500 = 2250K bytes
- Add an extra 20%, total Bandwidth = 2250K x (1+20%) = 2.7M Bytes

20% of users have spoken-name turned on: Example 2

- The number of subscribers with spoken-name = 12500 x 20% = 2500
- The number of subscribers without spoken-name = 12500 x 80% = 10000

- Assume spoken-name is 2 second long at 32 Kbit/s exactly, SMTP message size for a vCard = 4K bytes x 2 = 8K bytes
- Bandwidth required for SMTP size = (8K x 2500) + (180 x 10000) = 18200K = 18.2M
- Add an extra 20%, total Bandwidth = 18.2M x (1+20%) = 22 MB
- The Cisco UMG provides the fragment mechanism when a directory exchange SMTP messaging is over 1 MB to avoid a huge package flood into the WAN link

All subscribers have spoken-name turned on: Example 3

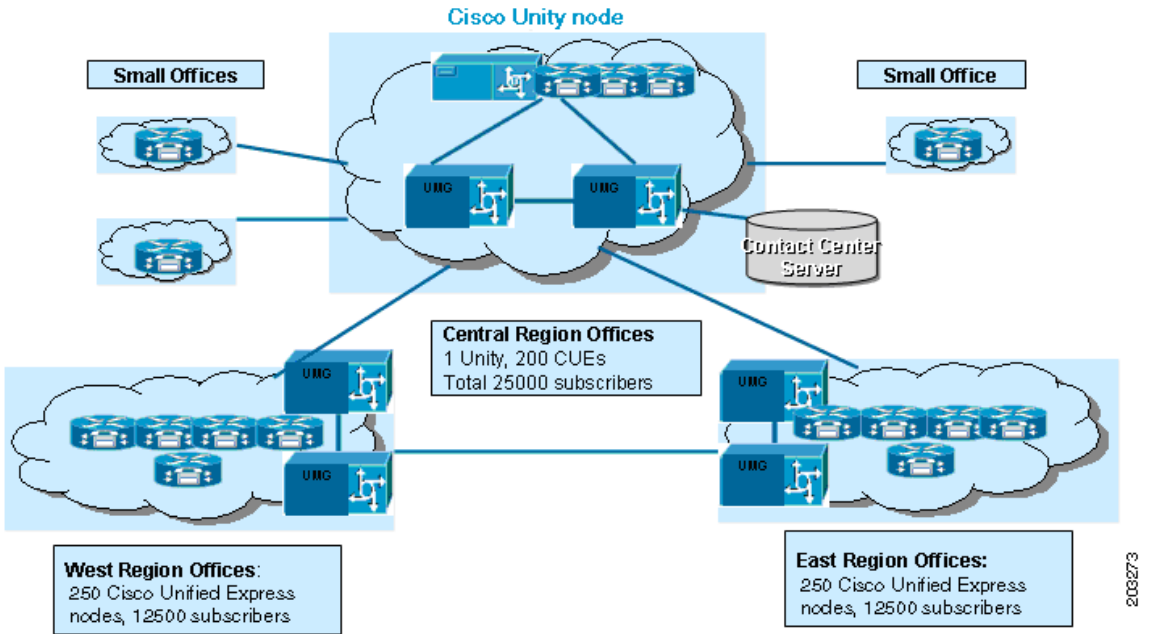
This scenario consumes a large amount of bandwidth. Carefully calculate the bandwidth requirement before deploying.

Additional Considerations

- The extra 20% in the previous estimates assume about 20% of the vCard traffic size is bigger than the average of 180 bytes.
- Fragmentation of SMTP messages to 1 MB units is implemented internally on the Cisco UMG. This is not user configurable.
- Directory-exchange traffic spikes most often during the first time sync-up between multiple regions. Thereafter, it really depends on how much the inter-region feature is used.
- Traffic for a Cisco UMG network is marked as best effort traffic. Therefore with QoS enabled network above traffic does not affect business critical or real time applications.

Hybrid Cisco UMG Deployment

Figure 3 Hybrid Cisco UMG Deployment Model



In this model, regions with a large number of subscribers on multiple Cisco Unity Express systems (east and west regions in Figure 3) are registered to the local Cisco UMGs, so that regions can take full advantage of the distributed Cisco UMG model. Remote office sites with a very small number of Cisco Unity Express installations (less than five), they can register with the Cisco UMGs in the central site to reduce hardware and license cost.

Note With the hybrid Cisco UMG deployment model, you must carefully estimate the bandwidth between the remote regions and the central site to ensure the WAN link can handle the extra traffic during message delivery.

Best Practices for Cisco UMG Deployment

In summary, the following best practices apply to the Cisco UMG deployment model.

- If the business infrastructure is the distributed with multiple regions, we recommend the distributed Cisco UMG model. However, you should carefully calculate the WAN bandwidth requirement. In general, the distributed Cisco UMG model provides more geographic scalability and the local message survivability.
- If the message flow is heavy in the remote sites across Cisco Unity Express units, we recommend the distributed model to reduce the WAN link usage during message route and delivery.
- Deploy the centralized Cisco UMG model if:
  - A business is mostly located in one central office.
  - The remote sites have only a few Cisco Unity Express units installed
  - The customer is willing to sacrifice message network survivability when the WAN link is down

  The customer must be aware that extra WAN bandwidth will be consumed even when messages are sent within the remote sites, if there are different mail systems. In general, we do not recommend this deployment.
- Deploy the hybrid Cisco UMG model for customers that have both large remote regional offices and some small offices in remote locations, if the overall topology of the business is centralized.

Migrating from the Fully-Meshed VPIM Network to a Cisco UMG Network

When migrating from the current messaging network to a Cisco UMG controlled messaging network, follow these recommendations:

- Upgrade Cisco Unity Express nodes to the version 3.1 to benefit from autoregistration. Earlier versions of Cisco Unity Express require manual provisioning on the Cisco UMGs.
- When registering the Cisco Unity Express nodes to the Cisco UMGs, Cisco Unity Express can keep all the existing VPIM network setup with remote network locations during the migration. The best practice is to:
  a. Verify the directory tables on the Cisco UMG to ensure the correct subscriber information are saved on the Cisco UMG database.

   b. Temporally remove the remote location IDs from the local Cisco Unity Express configuration and then confirm that messages are routed and delivered between the two nodes, both as originating and destination nodes.
   c. After verifying the successful message delivery between two nodes, remove the remote network location configuration from both Cisco Unity Express nodes.
   d. Complete the migration into the Cisco UMG controlled network.

- Do not allow Cisco Unity Express nodes to send VPIM traffic directly to other nodes. All VPIM message traffic must go through the Cisco UMG.
- For Cisco Unity endpoints, configure the Cisco UMG as the VPIM Delivery Location. We do not recommend setting up the Cisco UMG as the Cisco Unity Bridge because of the broadcast limitation of the Cisco Unity Bridge.
- For Cisco Unity customers that have setup all remote subscribers as VPIM remote subscribers, they can modify the remote VPIM subscriber configuration by replacing the VPIM location with the hostname of Cisco UMG, instead of pointing to the remote network location.
- For Cisco Unity customers that have their own messaging application to provide limited VPIM route and delivery functionality, they can do a partial migration with the following recommendations (although we recommend that you migrate all nodes in the entire network to the Cisco UMG controlled network):
   a. Keep the Cisco Unity side setup, but migrate all other nodes from remote offices into a Cisco UMG controlled network.
   b. On Cisco UMG, setup the customized messaging application on Cisco Unity as an endpoint with all required configurations. On the customized messaging application, configure VPIM parameters pointing to the Cisco UMG.
   c. Make sure all the messages between the Cisco UMG controlled network and the messaging application controlled domain have interaction between the Cisco UMG and the customer messaging application
   d. Do the interoperational testing between the Cisco UMG and the customized messaging application before the deployment. We are not responsible for your results.

Designing a Messaging Network Controlled by Cisco UMG

First Published: February 28, 2008

After completing chapter 3 and chapter 4, complete the following tasks:

- Use the analysis of the network traffic distribution pattern based on regions or areas on the messaging network to:
  - Decide which Cisco UMG deployment model to use.
  - Finalize the locations to install the Cisco UMGs.
  - Allocate the extra bandwidth for Cisco UMG to perform all required functions.
- Optionally extend or modify the network security and QoS mechanism on the current network for the new Cisco UMGs inserted into the network.
- Use the sizing and capability calculations for the Cisco UMG to select the correct hardware and licenses to purchase.
- Finalize which endpoint types and versions (Cisco Unity Express, Cisco Unity, and Avaya Interchange) to use
- Prepare the TFTP, FTP, NTP, and DNS servers for use in the Cisco UMG controlled messaging network

This chapter describes the following design guidelines based on the results from the above steps:

- Design a Cisco UMG network with unique location IDs for all entities including all endpoints and the Cisco UMGs.
- Design a Cisco UMG network with a consistent address scheme across all nodes in the network.
- Design reasonable timers and turn on/off features on the Cisco UMGs to optimize the network bandwidth.
- Design a secure Cisco UMG network from both network and application levels.
- Design the Cisco UMG failover scheme.
- Design the Cisco UMG back and restore options.

These guidelines are discussed in the following sections:

Design a Messaging Network with Unique Location IDs

In a Cisco UMG controlled network, the location ID for the Cisco UMG, Cisco Unity Express, Cisco Unity, and Avaya Interchange is used as an identifier for the location. The location IDs of an autoregistered endpoint (Cisco Unity Express 3.1 and later versions), and also the primary and/or the secondary Cisco UMG location IDs are included in the registration messages. The location IDs for manually provisioned endpoints (Cisco Unity Express prior to 3.1, Cisco Unity, and Avaya Interchange) are configured on the Cisco UMG using CLI commands and are shared between the Cisco UMGs during directory exchanges.

Location IDs of endpoints and Cisco UMGs are saved on the Cisco UMG directory table and used for the message routing. You must ensure that all of the Cisco Unity Express, Cisco Unity, and Avaya Interchange location IDs are unique across the entire Cisco UMG network. Without careful planning, it is possible to assign Location IDs that prevent the Cisco UMG from finding a message recipient at another location.

Guidelines for Assigning Location IDs

The numbering plan for assigning location IDs can affect how easily the Cisco UMG matches the number that a subscriber enters when addressing a message. We recommend following these guidelines:

- Establish a fixed length for location IDs, and if possible, a fixed length for extensions.
- Assign unique Location IDs. A Location ID must not be the same as any other Location IDs, system distribution list numbers, or any extension assigned to a subscriber. For example, when assigning a SDL list with number 1100, do not assign a location ID as 110. This results in a conflict during the Cisco UMG search and failure to invoke SDL 1100.
- Assign a numbering range for location IDs that extensions do not use. For example, you can assign Location IDs with leading zeros (0001, 0002, and so on).
- Make sure that the Location IDs you assign for all entities are at least three digits because this is required by the Cisco Unity Dial ID parameter.
- Make sure that the Location IDs for all entities are not more than seven digits because this is the maximum number of digits supported by Cisco Unity Express location IDs.
- If using variable-length location IDs and extensions, the location IDs should be in a different numbering range than the range for extensions. For example, if there is a local extension 527123, do not assign a location the location ID of 527 if there is a possibility that this location will have the extension 123.
- If using variable-length location IDs, the first digits of each location ID must be unique with respect to other location IDs. For example, if you have a location with an ID of 527, do not assign another location the ID of 5277. In this example, during a blind address search, Cisco Unity and Cisco Unity Express would always match the blind address entered by the subscriber to location 527 and fail to find location 5277.

- Follow Cisco Unity and Cisco Unity Express Design Guide regarding Dial ID and Location ID recommendations.
- Make sure that the Location ID you assing are digits only. We do not recommend using * or # for Location IDs.
- We recommend that you configure prefixes the same as the location ID for easier management and a nicer user experience.

Without following these guidelines, subscribers may encounter the following problems when addressing a message:

- A delay while the Cisco UMG searches for a match remote location
- Multiple matches for the number entered by a user
- Failure to find the recipient at another location

Designing an Address Scheme for Your Messaging Network

A subscriber, also referred as a mailbox user, is addressed with the format specified in the VPIM protocol. It consists of a local part and a domain part. The local part is used for the username or mailbox identification; and the domain part is used for the machine identification or domain name. For example, a subscriber with address of 4085550101@xyz.com is in the xyz domain and the mailbox number is 4085550101.

The Cisco UMG supports the following three address schemes for a subscriber or mailbox identification

- E.164 format, a 10-digit unique telephone number for each subscriber (for example, 4085550101@cue-sj.xyz.com)
- Node with primary extension (for example, 1001@cue-sj.xyz.com, on which 1001 is the extension and cue-sj.xyz.com is the node identifier)
- Flexible string lengths which are unique across the network. The exact form depends on the Cisco UMG network dial plan. (for example, 23019@cue-sj.xyz.com where 23019 must be a unique digit across the entire messaging network). The maximum string length is 15 digits based on the E.164 standard.

Guidelines for Choosing an Address Scheme

It is important that you design a Cisco UMG network with a consistent address scheme across all mail systems in the network.

- Choose only one address scheme from the above three addressing schemes to uniquely identify all mailbox users in the Cisco UMG network. The Cisco UMG does not support routing of mixture addressing schemes. (For example, one Cisco Unity Express sending VPIM messages using an E.164 format and another Cisco Unity Express sending VPIM messages using the node + extension address scheme).
- Ensure each endpoint is properly configured.
- Endpoints such as Cisco Unity Express and Cisco Unity can compose a VPIM message using one of the above addressing schemes. If the network is deployed with any combination of Cisco Unity or Avaya Interchange, you must choose E.164 or a unique digit as the address scheme.

Designing a Cisco UMG Controlled Network with Network Optimization

By the very nature of the VPIM protocol over SMTP and remote voice message delivery in general, voice message are not required to be delivered in real time. A voice mail subscriber is accustomed to certain delays in terms of hours between the time the sender sends the voice mail and the time the receiver gets the voice mail on the remote systems, such that no Cisco UMG specific QoS parameters must be setup on an existing network.

However, under certain circumstances on the Cisco UMG deployment, the network bandwidth consumption may be increased. The system administrator should examine the network resource availability and modify the network configuration accordingly.

Choosing Reasonable Timers on Cisco UMG Network

Use the following guidelines when choosing reasonable timers:

- Endpoint Registration Expiration Timer on the Cisco UMG — Because there is no keepalive between the endpoints and the UMG, reregistration HTTP messages are exchanged between the endpoints and the Cisco UMGs when the timer expires. The registration timer is the system parameter that is applied to all the nodes that register with the hosting Cisco UMG. The network traffic may have a burst of traffic from bulk endpoints. The default timer setting is 24 hours. A setting that is too short timer will consume extra network bandwidth but a setting that is too long timer may cause an out-of-sync status between endpoints and its hosting Cisco UMG. We recommend that you set up reregistration events during off peak hours or after hours.

Note The Cisco UMG limits the amount of processing power it spends on registration requests to give priority to forwarding voice mail messages. When many registrations occur simultaneously, some fail and automatically retry.

- Directory Exchange Interval on Cisco Unity Express — When subscriber information is updated on Cisco Unity Express, Cisco Unity Express accumulates the changes that happened within the interval, then sends out directory exchange updates to its hosting Cisco UMG when the timer expires. The default interval is two minutes. When a Cisco Unity Express is doing major imports or exports for subscribers, change the timer accordingly.
- Delayed Delivery Receipt (DDR) timeout and NonDelivery Receipt (NDR) timeout on the Cisco UMGs — By default, the DDR timeout value is one hour and the NDR timeout value is six hours. We recommend that you use consistent DDR and NDR timer settings across all Cisco UMGs in the network.

Choosing Cisco UMG Features Based on Network Resource Availability

- Cisco Unity Express Remote Lookup — When this feature is turned on, Cisco Unity Express invokes remote lookup through HTTP to query location and user information from the Cisco UMG and stores the result in its local cache for future reference. However, the cache size on Cisco Unity Express is limited. Any query that cannot find a match in the local cache consumes network bandwidth and system resources. We recommend that you use blind addressing instead of remote lookup if there are a large number of queries during peak hours without adequate bandwidth.

Note The Cisco UMG limits the amount of processing power it spends on remote lookup to give priority to forwarding of voicemail messages. When many remote lookups occur simultaneously, some lookups may be rejected.

- Spoken Name Confirmation — The spoken name is carried within a vCard during directory exchanges and saved in the Cisco UMG database. A typical vCard without spoken name is about 180 bytes, with spoken name (averaging two to three seconds at exactly 32 Kbps), it can easily exceed 10 KB on a single vCard. In extreme cases, such as 1000 Cisco Unity Express nodes with 50 subscribers on each node, the single SMTP size during the directory exchange between the Cisco UMGs will be tens of megabytes. To be consistent with the Cisco Unity implementation, Cisco UMG limits the maximum SMTP message size to 1 MB during directory exchanges. Therefore, for every SMTP package, the network is able to handle an extra 1 MB in addition to other traffic. We recommend that you disable spoken name using the CLI if the network links between Cisco UMGs are slow.
- System Distribution List — SDLs are shared among Cisco UMGs and can be managed on any Cisco UMG in a network. When exiting from list-management mode on one Cisco UMG, all SDL changes are shared with all other Cisco UMGs in the network. Again, there is a burst of network traffic when SDL synchronization happens between Cisco UMGs. However, you can control the extra traffic load by performing SDL synchronization during off peak hours.

Design a Secure Cisco UMG Network from Both Network and Application Levels

When addressing the security of a Cisco UMG controlled network, you must have a network security strategy that prevents unauthorized access to any Cisco UMG, and must configure the Cisco UMG security features on each node to complement existing network security infrastructure.

To prevent any unauthorized access to the Cisco UMG, the following topics are discussed:

System and Remote Access

No external interfaces are on the Cisco UMG hardware (physically there is an FE interface port, but it is disabled in software and unusable). All access must pass through the host Cisco ISR router and across the backplane to the NME-UMG and NME-UMG-EC.

Local Access

The only local access to a Cisco UMG is through the host router's console interface by using the following command to open a session to the Cisco UMG:

service-module integrated-service x/y session

Entering this command requires 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 UMG CLI, Cisco UMG has no password capability. Any network administrator with access to enable mode on the router, also can access the Cisco UMG CLI. There is no user ID or password control on the Cisco UMG CLI. Access is controlled via the router, and if logging is required, you must set up the router with AAA/RADIUS monitoring of login access.

Remote Access Using Telnet

Direct Telnet access to the Cisco UMG IP address is disabled by default and an error message of "Unable to connect to remote host: Connection Refused" is returned when access is attempted. Therefore, remote CLI access to the Cisco UMG is only possible by Telneting to the hosting router and then using the **session** command to get access to the Cisco UMG CLI. That way, all the security protections that are built into Telnet access to your router automatically also protect access to Cisco UMGs.

Telneting to the router using the IP address followed by the explicit TTY port number that is allocated to Cisco UMG is not blocked and can provide undesirable "direct" access to the Cisco UMG.

To protect against this type of access, configure a login and password on the TTY port. In this example, the Cisco UMG module is in slot 1/0 on a Cisco 2811 and has a TTY port of 2066 leading to Cisco UMG, as shown in the following configuration example:

```
line 66
 password mypass
 flush-at-activation
 no activation-character
 login
 no exec
 transport preferred none
 transport input all
```

Note Cisco UMG itself does not support SSH. Because all communication between the hosting router and the Cisco UMG module is through the router backplane, Cisco UMG is not exposed to any external interface on IP segments. SSH access to the router is sufficient to protect Telnet access to the Cisco UMG.

Application Environment

The Cisco UMG is an IP application and therefore communicates with its environment using various TCP and UDP protocols and ports, as listed in Table 1.

Note You must ensure all the required ports listed in Table 1 are not blocked for various entities in the Cisco UMG controlled messaging network.

Table 1 Cisco UMG Protocols and Port Numbers

Protocol	Cisco UMG Destination Port	Cisco UMG Source Port	Remote Port	Remote Device	Notes
SSH			22	Secure Shell Client	Not supported by Cisco UMG. Use SSH to the host router
Telnet		23		Telnet Client	
DNS		TCP/UDP 53		DNS servers	
TFTP		UDP 69		TFTP server	To load RAM Kernel
FTP		TCP 20/21		FTP server	To install, backup, and restore
HTTP		TCP 80		Endpoints	Registration and remote lookup
NTP		UDP 123		NTP server	To Synchronize Date/Time
SMTP		TCP 25		Cisco UMG/ Cisco Unity Express	Directory Exchange
VPIM		TCP25		Cisco UMG/ Cisco Unity Express	Message Networking
Syslog		TCP 514		Syslog Server	
SNMP					Cisco UMG itself does not support SNMP

Cisco UMG Access Control Guidelines

- Assign an enable password to the router hosting the Cisco UMG module.
- Restrict Telnet access to the hosting router.
- Enable login and password control on the router TTY port connecting to Cisco UMG.
- Configure an inactivity timeout on the router TTY port connecting to Cisco UMG.
- Enable SSH on the router to protect Telnet traffic; use only SSH-capable Telnet client software.
- Use Access Control Lists (ACLs) to close access to any ports that are not actively in use by Cisco UMG.
- Use ACLs to restrict traffic to and from Cisco UMG.
- 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.

Application Level Security Protection

This section discusses the following types of security that are supported on Cisco UMG:

- Security checks during endpoint registration
- End user validation during the messaging delivery
- SDL/SBM authorization
- NAT support

Secure Registration of Endpoints

The Cisco UMG supports the HTTP digest authentication mechanism with shared a registration username and password between the Cisco UMG and its endpoints. If the username or password does not match, the registration fails and gives the response “Unauthorized.”

If the registration to the primary Cisco UMG failed with this response, the endpoint does not register with the secondary Cisco UMG sequentially. The endpoint should only continue registration with the secondary Cisco UMG, if it registered with primary Cisco UMG successfully or it cannot reach the primary Cisco UMG and received a timeout response.

The Cisco UMG can prevent nodes from registering by enabling the blocking of CLI commands associated with endpoint location IDs. During the registration message exchange, if the a matching Blocking Location ID is found, the Cisco UMG rejects the registration and gives the response “forbidden” to the endpoints.

The Cisco UMG accepts only VPIM messages sent from the registered endpoints.

Note Blocking an endpoint from autregistration will have no impact on whether you can manually configure an endpoint with the same location ID.

System Distribution List and System Broadcast Message Endpoint Control

The Cisco UMG controls SDL and SBM through subscriber authorization during SDL and SBM creation. By default all subscribers in the list have permission to receive only. Only certain numbers with explicitly granted privileges are able to send SDL or SBM.

In the case of a nested distribution list, if the subscriber has privileges to send to that particular list, the message addressed to that list must be sent to all the members under that list regardless of whether or not that subscriber has privileges to send to any specific member of the list.

For example, a Cisco UMG node has the following SDLs configured:

- SDL0010, which contains subscriber1 who has sending privileges
- SDL0020, which contains subscriber2 who has sending privileges
- SDL0030, which does not have sending privileges

In this example, the following behaviors occur:

- When subscriber1 addresses an SDL message by dialing 0010, it sends the message to all other individual subscribers under SDL0010, and all subscribers under SDL0020 and SDL0030.
- When subscriber2 addresses an SDL message, it can only send the message to all the subscribers in SDL 0020 by dialing 0020. It cannot send the message to the members under SDL0030 or any individual subscribers under SDL0010.
- When subscriber2 addresses an SDL message by dialing 0010, the Cisco UMG rejects it, resulting in an NDR to subscriber2.
- All subscribers under SDL0030 only have receiving permit. They cannot send SDL messages to any SDL list.

Note The total number of SDL members (subscriber or nested lists) in any SDL list within the entire Cisco UMG network cannot exceed 10000.

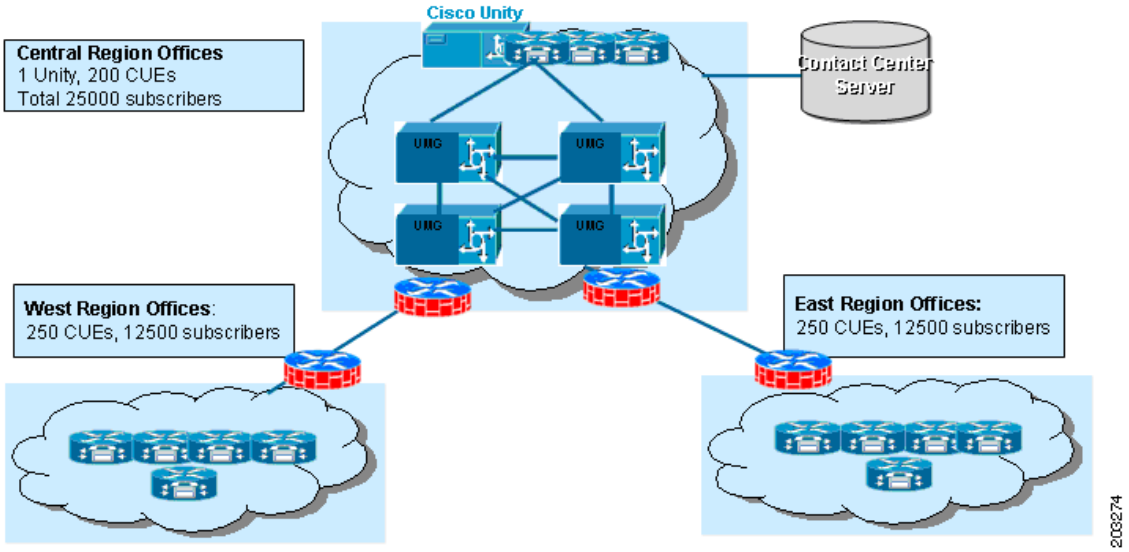
NAT Support on Cisco UMG

The Cisco UMG can be configured to use a NAT translation table to address NAT and firewall issues on the customer deployment environment. The NAT table consists of a list of internal IP address paired with the external IP address and ports. The Cisco UMG will look in this NAT table using the internal IP address to query the external IP address and port to determine the actual transport information.

In this section, the NAT examples use the Centralized Cisco UMG model and Distributed Cisco UMG model as reference to provide the recommendations.

Centralized Cisco UMG with NAT: Example

Figure 1 Centralized Cisco UMG Deployment with NAT



In this scenario, NAT blocks the following processes:

- Registration of the remote region Cisco Unity Express nodes on port 80
- Directory exchange between remote regions and the headquarters on port 25
- Message delivery to and from remote sites on port 25

To avoid these issues, we recommend that you:

- Configure the Firewall/NAT to statically open a pinhole on port 25 and port 80.
- Configure the Cisco Unity Express nodes on remote sites to register with the external IP address of the Cisco UMG on the headquarters NAT device. The NAT must be configured with a static mapping from the external IP address to the internal IP address of Cisco UMG.
- If multiple Cisco UMGs are behind the same NAT device (multiple Cisco UMGs may share the same external IP address), the endpoints on remote sites are able to communicate with Cisco UMGs using the different ports other than default 80/25. For example, the forwarding table on the headquarters NAT device may have a mapping table like this:

```
Forward 128.1.1.1:180 10.1.1.1:80  for UMG-1
Forward 128.1.1.1:181 10.1.1.2:80  for UMG-2
```

- On the remote site endpoint, the internal and external IP addresses must be configured on the Cisco UMG NAT table. The Cisco UMG looks in the NAT table to find the external IP address of the regional NAT device. The NAT device forwards it to the Cisco Unity Express after it maps the external IP address and the port to the internal IP and the port. For example, Cisco UMGs from the central site send VPIM message to remote region Cisco Unity Express with 128.1.1.3:126 instead of 10.1.1.3. The NAT table on the UMG might look like this:

Table 2 The NAT Table on the Cisco UMG at the Central Site

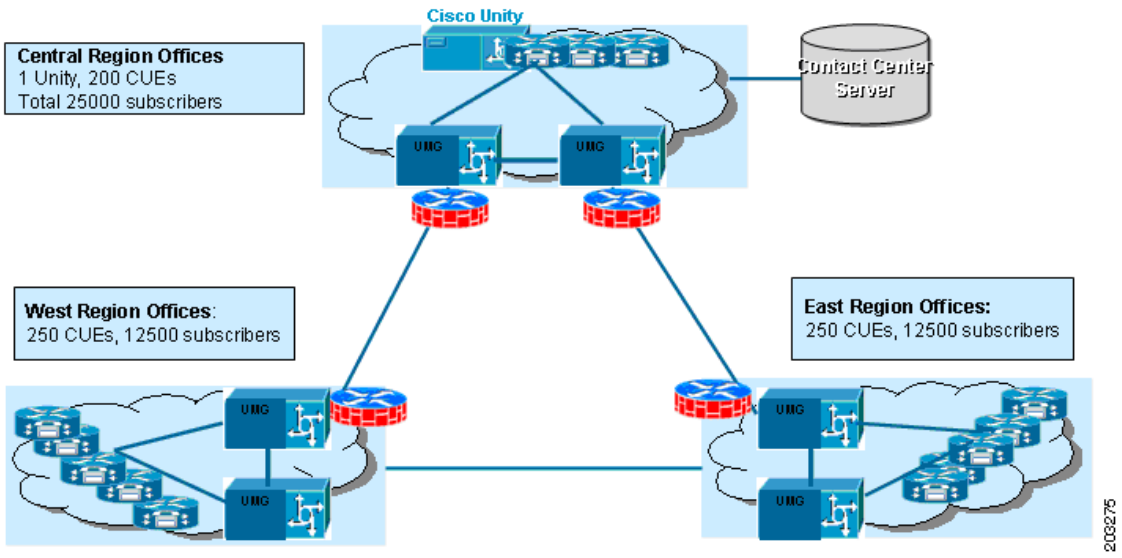
Peer	Internal IP Address	External IP Address	External HTTP Port	External SMTP Port
1001 (CUE-East-1)	10.1.1.3	128.1.1.3	1081	1026
1002 (CUE-East-2)	10.1.1.2	128.1.1.3	1082	1027
2001 (CUE-West-1)	10.1.1.1	128.1.2.3	1081	1026
2002 (CUE-West-2)	10.1.1.2	128.1.2.3	1082	1027

- If multiple Cisco Unity Express nodes sit behind the same NAT device, the Cisco UMG should be able to communicate with endpoints on different ports other than 25. Multiple endpoints can share the same external IP address. For example, the forwarding table on the region NAT device might have a mapping table like:

```
Forward 128.1.1.3:125 10.1.1.3:25  for CUE-1
Forward 128.1.1.3:126 10.1.1.4:25  for CUE-2
```

Distributed Cisco UMG Model with NAT: Example

Figure 2 Distributed Cisco UMG Deployment with NAT



In this example, NAT breaks both directory exchanges and message delivery because the routing table on the Cisco UMG will be built up with internal IP addresses which may not be reachable. The registration messages using HTTP port 80 are not blocked by the NAT devices in this scenario.

To avoid these issues, follow these guidelines:

- Configure the Firewall/NAT on both remote region and central sites to open a pinhole on port 25.
- Manually configure the NAT table on every Cisco UMG in the network to map the internal IP addresses to external IP addresses. The Cisco UMG will use the external IP addresses and the port numbers of its peer Cisco UMGs to exchange directory information and deliver the VPIM messages.
- If multiple Cisco UMGs are behind the same NAT device (multiple Cisco UMGs can share the same external IP Address), the Cisco UMG in other locations should be able to communicate with the Cisco UMGs on the different ports other than default 25. For example, the forwarding table on the headquarters NAT device might have the mapping table like this:

```
Forward 128.1.1.1:125 10.1.1.1:25  for UMG-1
Forward 128.1.1.1:126 10.1.1.2:25  for UMG-2
```

- The NAT on the headquarters Cisco UMG might have a mapping table like Table 3:

Table 3 The NAT Table on Central UMG

Peer	Internal IP	External IP	External SMTP Port
1101 (UMG-East-1)	10.1.1.10	128.1.1.3	1026
1102 (UMG-East-2)	10.1.1.11	128.1.1.3	1027
2101 (UMG-West-1)	10.1.1.10	128.1.2.3	1026
2102 (UMG-West-2)	10.1.1.10	128.1.2.3	1027

Designing the Fail Over Scheme in the Cisco UMG Network

As addressed earlier, the Cisco UMG supports a one-to-one active/standby fail over scheme. The secondary Cisco UMG does not have to be allocated in the same location as the primary Cisco UMG when the reliable IP connectivity is established between them.

The following points describe how Cisco UMG one-to-one failover support works:

- The failover can happen during endpoint registration, directory exchange, remote lookup, and message delivery. The Cisco UMGs must b e able to automatically detect and recover from a failover, including when the directory information is out-of-sync.
- For pairs of Cisco UMGs with one-to-one redundancy, the endpoints only send out directory updates to the primary Cisco UMG. The primary Cisco UMG publishes the information update to its all peer Cisco UMGs including its secondary Cisco UMG.
- If the endpoint cannot register with its primary Cisco UMG on the first attempt because of an unmatching username or password, it cannot register with its secondary Cisco UMG until the registration succeeds on its primary Cisco UMG.
- Because of the limitations of Avaya Interchange, only one Cisco UMG is allowed to send VPIM messages over it. Therefore, Avaya Interchange does not support failover on a Cisco UMG network.
- Because Cisco Unity does not support multiple VPIM endpoints pointing to the same remote user, or the multiple VPIM delivery locations pointing to the same remote location, the DNS must resolve IP addresses using the same hostnames that have different MX record priorities.
- For failover support on the older version Cisco Unity Express, the system administrator must manually provision it on the Cisco UMG endpoints.

Guidelines for Deploying Failover Support on the Cisco UMG Controlled Messaging Network

- Deploy dedicated primary and secondary Cisco UMGs; do NOT share the primary and secondary functionality on the any single Unit. For example, use UMG-1 as the primary Cisco UMG for the east region and UMG-2 as secondary. Do not use UMG-1 as secondary Cisco UMG for west region, and do not use UMG-2 as the primary Cisco MG for west region. Make sure you use the active/standby model, not the active/active load balancing model.
- Do not mix different Cisco UMG Hardware on the failover setup; always choose the same form of hardware for each Cisco UMG active/standby pair. For example if you use NME-UMG as the primary Cisco UMG, also use NME-UMG for the secondary. If you use NME-UMG-EC for the primary Cisco UMG, the secondary Cisco UMG must also use NME-UMG-EC to avoid causing the directory information to go out-of-sync because of a capacity mismatch.
- Because the Cisco UMG failover is transparent to the Cisco Unity, Cisco Unity must have DNS in order to resolve the primary and secondary Cisco UMG IP addresses from the single hostname into two MX records. We recommend that you set up MX records for both primary and secondary Cisco UMGs with different priorities.
- Ensure that endpoints can register with its primary Cisco UMG for the first time without any issues. Verify the IP connectivity and shared user name and password to avoid potential out-of-sync risk on directory information.
- We strongly recommend that you use the one-to-one full redundancy setup. Do not share the secondary Cisco UMG between different sets of endpoints. For example, set up UMG-1 as the primary Cisco UMG for the east region, and UMG-2 as the secondary Cisco UMG. Do not also use UMG-2 as secondary Cisco UMG for the west region. The west region should have its own primary and secondary pair of Cisco UMGs.

Designing the Backup and Restore on a Cisco UMG Controlled Network

A Cisco UMG uses the FTP server for backup and restore with two options:

- Configuration only backup and restore— Backs up all the system configuration including the peer gateways, manually configured endpoints (older version Cisco Unity Express, Cisco Unity, and Avaya Interchange), registration credentials, NAT configuration, default route, and other system configuration information as displayed by the **show startup-config** command.
- Configuration plus data backup and restore — In addition to backing up the entire system configuration, also backs up dynamic operational data that the Cisco UMG requires during runtime, such as auto-registered endpoint information, directory information from the local endpoints, and snapshots of the system distribution list and the system broadcast message.

Restrictions

- The directory and endpoint information advertised from the peer Cisco UMGs is not backed up.
- Backup and restore can only occur in offline mode.

Best Practices

The best practices with the Cisco UMG backup and restore are:

- We do not recommend performing data-only backups and restores. Performing data-only backup may introduce system inconsistencies because the conflicts the between existing configuration and the data being restored.
- Perform a **copy running-configuration startup-config** or **write memory** before the backup to ensure the system consistency across backup and restore.
- The snapshot information of the system distribution list and system broadcast message can be changed during backup and restore procedures. You should perform a manual synchronization of the SDL/SBM from/to the peer Cisco UMGs.
- Avoid security concerns by ensuring the appropriate secure tunnel is setup between the Cisco UMG host router and the FTP server.
- The storage of backup files is only as secure as the access to the FTP server. The files are not encrypted unless an offline utility is used to encrypt these files after Cisco UMG has completed its backup (and decrypt them again before attempting a restore operation).

Setting Up a Messaging Network Controlled by Cisco UMG Using a Distributed Model

First Published: February 28, 2008

This chapter describes how to set up a complete Cisco UMG controlled messaging network using a distributed model. The following topics are discussed:

Overview

In this messaging network, Cisco Unity Express, Cisco Unity, and Avaya Interchange are all present as endpoints, the Cisco UMGs are setup with full active-standby redundancy. Figure 1 shows a network diagram and Table 1, Table 2, Table 3, and Table 4 contain detailed information about the topology.

Figure 1 Cisco UMG Network Setup Case Study Topology

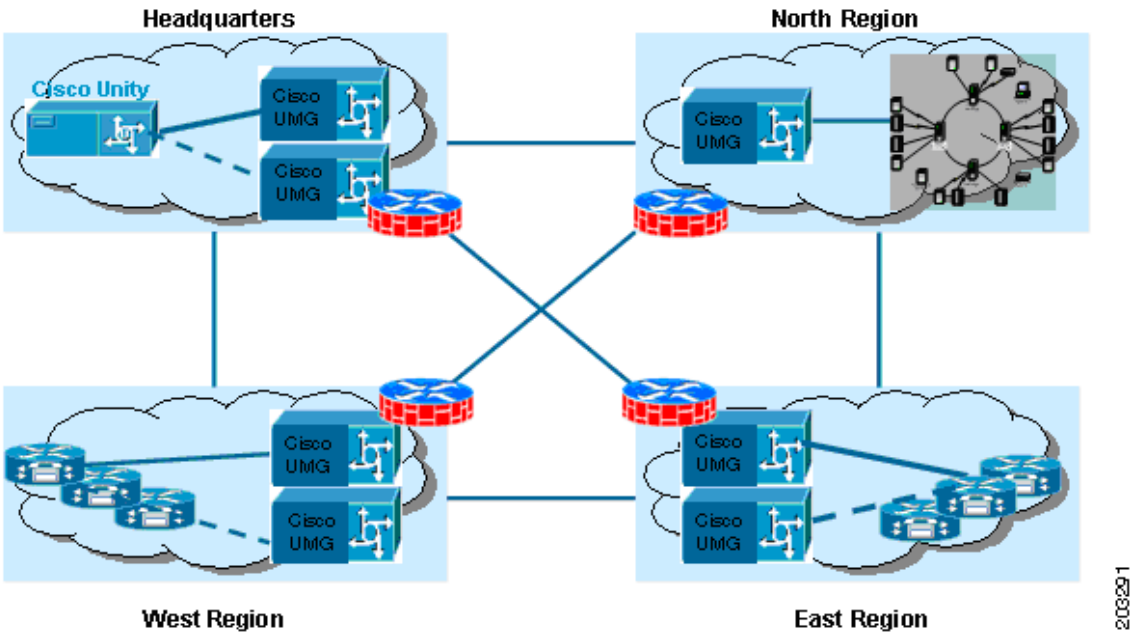


Table 1 Headquarters Information

Node	Location ID	IP Address	Host	Prefix	SMTP domain
Ump-P	500	10.60.80.200	Umgrtp	—	Umgrtp.headquarters.com
Umg-S	500	10.60.80.201	Umgrtp	—	Umgrtp.headquarters.com
Unity	510/511	10.60.80.11	HQunity	919/704	HQunity.headquarters.com
NTP	—	10.60.80.254	HQntp	—	—

Note For the west region, assume all the Cisco Unity Express nodes were upgraded to 3.1.

Table 2 West Region Information

Node	Location ID	IP Address	Name	Prefix
Umg-P	400	10.60.70.200		n/a
Umg-S	401	10.60.70.201		n/a
CUE-1	410	10.60.70.11		408
CUE-2	411	10.60.70.21		408
CUE-3	412	10.60.70.31		650
NTP	n/a	10.60.80.254	HQntp	n/a

Note For the east region, assume none of Cisco Unity Express nodes was upgraded to version 3.1.

Table 3 East Region Information

Node	Location ID	IP Address	Name	Prefix
Umg-P	300	10.60.30.200		n/a
Umg-S	301	10.60.30.201		n/a
CUE-1	310	10.60.30.11		716
CUE-2	311	10.60.30.21		716
CUE-3	312	10.60.30.31		917
NTP	n/a	10.60.80.254	HQntp	n/a

Table 4 North Region Information

Node	Location ID	IP Address	Host	Prefix	SMTP domain
Umg-P	600	10.60.60.200		N/A	
Interchange	610	10.60.60.11	interchange	203	Interchange.headquarters.com
NTP	n/a	10.60.80.254	HQntp	n/a	n/a

Note This document does not cover how to set up the domain and NTP. For information on this topic, see the *Cisco UMG System Administrator Guide*. Ensure the system time is synchronized in the Cisco network.

Building Up a Fully Meshed Network Between Cisco UMGs

The following example is for the west region Cisco UMG-P. The configuration for the other Cisco UMGs is similar.

```
umg-w-1(config)# network local messaging-gateway 400
```

Note Configure the network local ID on all the Cisco UMGs.

```
umg-w-1(config)# network messaging-gateway 401 10.60.70.201
umg-w-1(config)# network messaging-gateway 500 10.60.80.200
umg-w-1(config)# network messaging-gateway 501 10.60.80.201
umg-w-1(config)# network messaging-gateway 300 10.60.30.200
umg-w-1(config)# network messaging-gateway 301 10.60.30.201
umg-w-1(config)# network messaging-gateway 600 10.60.60.200
umg-w-1(config)#exit
```

To verify the full meshed network:

```
umg-w-1# show messaging-gateway
LocationID     Hostname                                  NAT
-----------------------------------------------------------
401            10.60.70.201                            disabled
500            10.60.80.200                            disabled
501            10.60.80.201                            disabled
300            10.60.30.200                            disabled
301            10.60.30.201                            disabled
600            10.60.60.200                            disabled

Local Gateway ID: 400
```

Managing Endpoints with One-to-One Cisco UMG Redundancy

Managing Cisco Unity 3.1 and Later Versions

Endpoint autoregistration involves configuration on both Cisco Unity Express and Cisco UMG. This example of the west region in this case, uses cue-w-1 as an example. The configurations for cue-w-2 and cue-w-3 are similar.

Registration Configuration on Cisco Unity Express

- Cisco Unity Express prerequisite configuration of the network Location ID

```
Cue-w-1(config)# network location id 410
Cue-w-1(config-location)# abbreviation cueW1
Cue-w-1(config-location)# email domain 10.60.70.11
cue(config-location)# voicemail phone-prefix 408
cue(config-location)# enable
cue(config-location)# exit

cue(config)# network local location id 410
```

```
Primary gateway IP address, registration listening port number, and username/password
       Cue-w-1(config)# messaging-gateway primary 400 10.60.70.200
       Cue-w-1(config-messaging-gateway)# username cue_410 password text pswd
       Cue-w-1(config-messaging-gateway)# exit
```

- Secondary gateway IP address and registration listening port number

```
Cue-w-1(config)# messaging-gateway second 401 10.60.70.201
Cue-w-1(config-messaging-gateway)# username cue_410 password text pw1
Cue-w-1(config-messaging-gateway)# exit
```

- Registration command that starts the process

```
cue(config)# messaging-gateway register
```

Corresponding Configurations on Cisco UMG

- Registration authentication username and password

```
Umg-w-1(config-reg)# username cue_410 password text pw1
Umg-w-1(config-reg)# username cue_410 password text pw1
Umg-w-1(config-reg)# exit
```

Note For other Cisco Unity Express endpoints in the west region, configure similar credentials.

For the secondary Cisco UMG in the west region, use to the same configuration.

- Block any Cisco Unity Express endpoint on the restricted list if any (optional). In this case, the Cisco UMG in the west region rejects all the Cisco Unity Express endpoints in the east region.

```
Umg-w-1(config-reg)> block location-id 310
Umg-w-1(config-reg)> block location-id 311
Umg-w-1(config-reg)> block location-id 312
```

Verifying Registration Status

```
umg-w-1# show registration users|status
umg-w-1# show endpoint local
    cue-w-1# show messaging-gateway
```

Managing Cisco Unity Express Versions Earlier Than 3.1

This scenario requires manual provisioning on Cisco UMG.

(The east region in this case, covers all three Cisco Unity Express configurations on UMG-e-1)

- Cisco Unity Express prerequisite configuration

  This example is for cue-e-1. The configurations for cue-e-2 and cue-e-3 are similar.

```
Cue-e-1(config)# network location id 310
Cue-e-1(config-location)# abbreviation cueE1
Cue-e-1(config-location)# email domain 10.60.30.11
Cue-e-1(config-location)# voicemail phone-prefix 716
Cue-e-1(config-location)# enable
Cue-e-1(config-location)# exit

Cue-e-1(config)# network local location id 310

Cue-e-1(config)# network location id 300
Cue-e-1(config)# email domain 10.60.30.200
Cue-e-1(config)# exit
```

- Configuration for cue-e-3 on umg-e-1

```
Umg-e-1(config)> endpoint 312 cue
Umg-e-1(config-endpoint)> broadcast-id 312
Umg-e-1(config-endpoint)> domain cue-e-1.cueE.headquarters.com
Umg-e-1(config-endpoint)> hostname 10.60.30.31
Umg-e-1(config-endpoint)> messaging-gateway secondary 301
Umg-e-1(config-endpoint)> prefix 917
Umg-e-1(config-endpoint)> enable
```

Note The domain on the above can be the IP address of Cisco Unity Express, in this case, 10.60.30.31.

- Configuration for cue-e-1 and cue-e-2 on umg-e-1

  Both cue-e-1 and cue-e-2 have the same prefix 716.

```
Umg-e-1(config)> endpoint 310 cue
Umg-e-1(config-endpoint)> broadcast-id 311
Umg-e-1(config-endpoint)> domain 10.60.30.11
Umg-e-1(config-endpoint)> hostname 10.60.30.11
Umg-e-1(config-endpoint)> messaging-gateway secondary 301
Umg-e-1(config-endpoint)> prefix 716 number-only
Umg-e-1(config-endpoint-extension)> extension 8561001
Umg-e-1(config-endpoint-extension)> extension 3241002
Umg-e-1(config-endpoint)> enable

Umg-e-1(config)> endpoint 311 cue
Umg-e-1(config-endpoint)> broadcast-id 311
Umg-e-1(config-endpoint)> domain 10.60.30.21
Umg-e-1(config-endpoint)> hostname 10.60.30.21
Umg-e-1(config-endpoint)> messaging-gateway secondary 301
Umg-e-1(config-endpoint)> prefix 716 number-only
Umg-e-1(config-endpoint-extension)> extension 1241001
Umg-e-1(config-endpoint-extension)> extension 5321002
Umg-e-1(config-endpoint)> enable
```

Note For older versions of Cisco Unity Express, you must enter prefix-number-only mode with extension information only if multiple endpoints are sharing the same prefix.

- Check the registration information on umg-e-1:

```
umg-e-1> show endpoint local
A total of 3 local endpoint(s) have been found:
Location    Location          Endpoint     Endpoint    Primary     Secondary
ID          Prefix            Type         Status      Gateway     Gateway
-------------------------------------------------------------------------------------------
310             716            CUE             Enabled   300         301
311             716            CUE             Enabled       300          301
312             917            CUE             Enabled   300          301

umg-e-1> show mailbox 311
2 mailbox(s) has been found for location 311
7161241001
7165321002

umg-e-1> show mailbox 310
2 mailbox(s) has been found for location 310
7165550111
7165550112

umg-e-1> show mailbox 312
No mailbox has been found for location 312
```

Note Only those manual endpoints with prefix-number-only extension configured have subscriber information on Cisco UMG's directory database.

Managing Cisco Unity and Manually Provisioning Cisco UMG

Note Manually provision Cisco UMG only if needed.

In this example of the headquarters configuration, Cisco Unity has multiple prefixes. This example includes the configuration for both Cisco UMG and Cisco Unity.

Configuration for HQunity on umgrtp

```
Configure  on umgrtp-1:
Umgrtp-1(config)> endpoint 510 unity
Umgrtp-1(config-endpoint)> domain headquarters.com
Umgrtp-1(config-endpoint)> hostname HQunity.headquarters.com
Umgrtp-1(config-endpoint)> messaging-gateway secondary 501
Umgrtp-1(config-endpoint)> prefix 919
Umgrtp-1(config-endpoint)> enable

Umgrtp-1(config)> endpoint 511 unity
Umgrtp-1(config-endpoint)> domain headquarters.com
Umgrtp-1(config-endpoint)> hostname HQunity.headquarters.com
Umgrtp-1(config-endpoint)> messaging-gateway secondary 501
Umgrtp-1(config-endpoint)> prefix 714
Umgrtp-1(config-endpoint)> enable
```

Note Every prefix on Cisco Unity is counted as an individual endpoint on Cisco UMG, which means you must assign different Location ID.

Configuration for Cisco Unity

Defining the Cisco UMG Host Information on Cisco Unity DNS Server

Figure 2 Configuring the Cisco UMG Host (umgrtp) with a Primary IP Address (10.60.80.200)

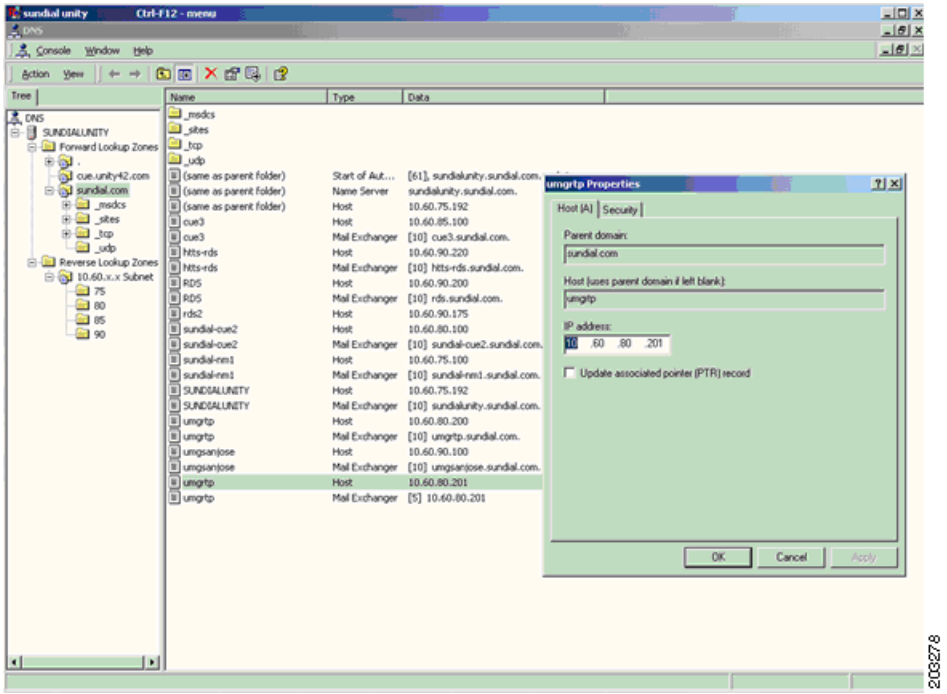
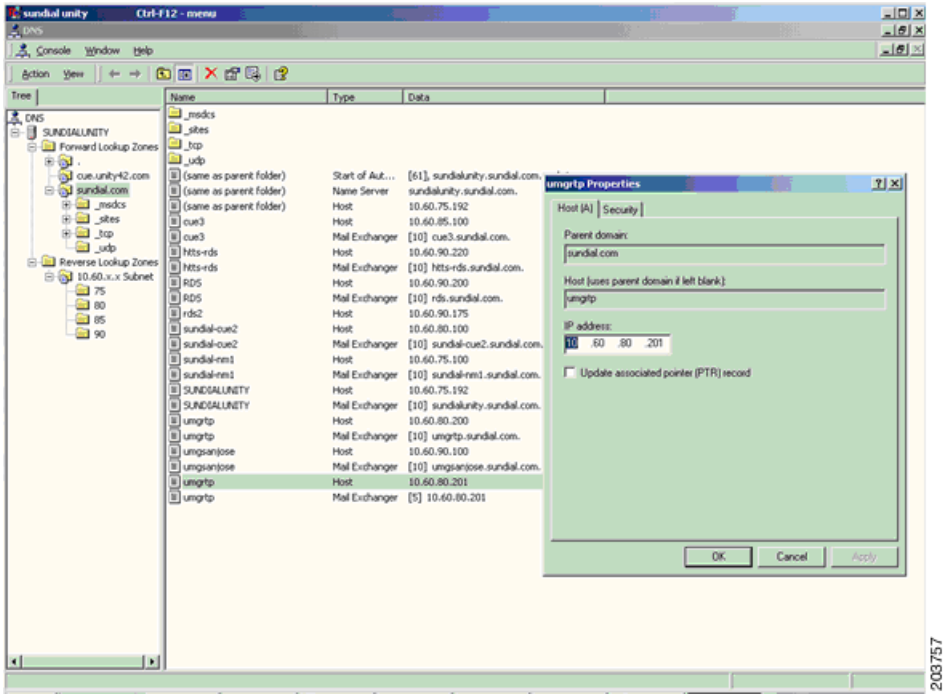


Figure 3 Configuring the Cisco UMG Host (umgrtp) with a Secondary IP Address (10.60.80.201)



Creating a Mail Exchange Record on Cisco Unity for Cisco UMG 1-1 Redundancy

Figure 4 Create MX Record for Primary Cisco UMG with Priority 10

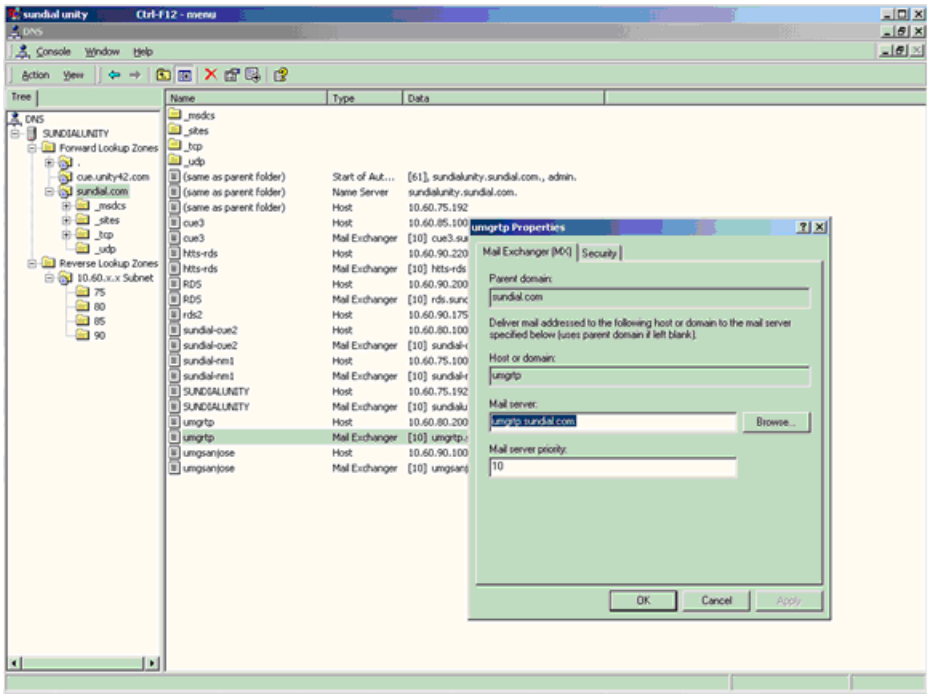
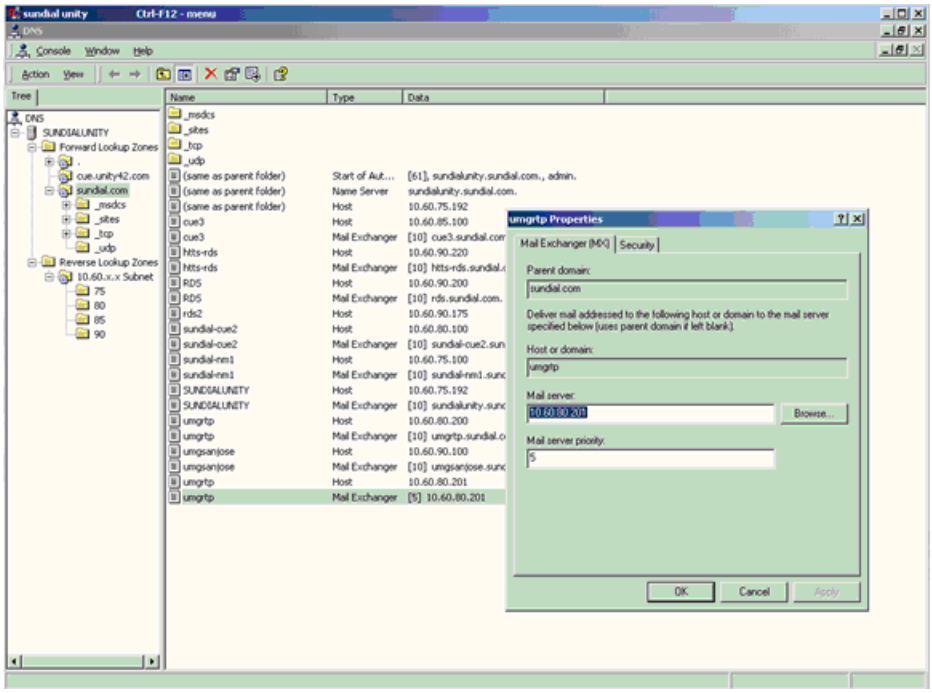
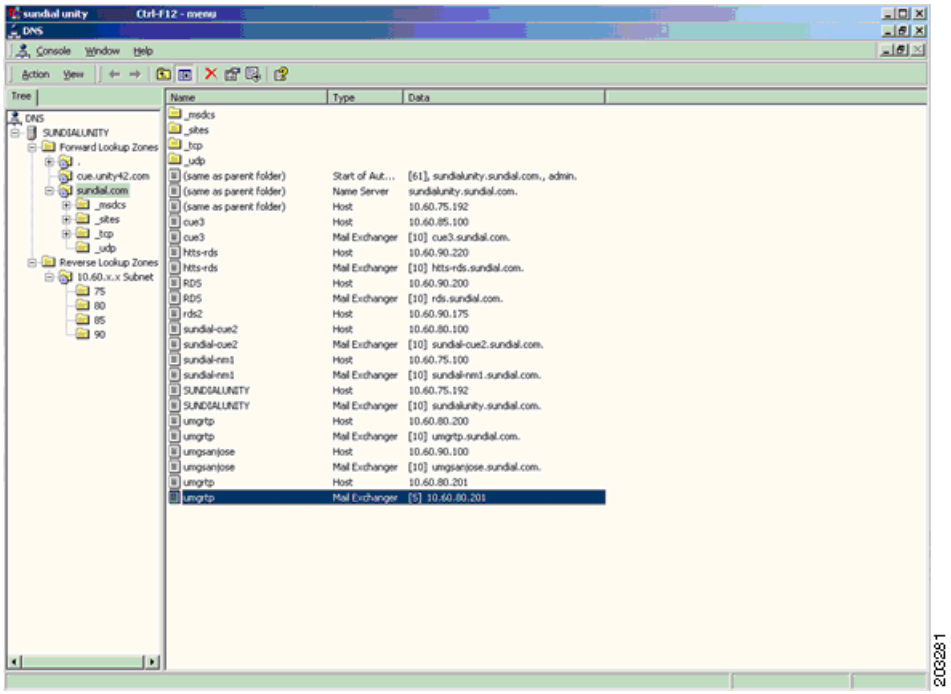


Figure 5 Create MX Record for Secondary Cisco UMG with Priority 5



Note Cisco UMG redundancy is transparent for Cisco Unity. Cisco Unity relies on the DNS server to map the primary or secondary Cisco UMG host to the IP address depending on the Cisco UMG status and priority setup. (See Figure 6)

Figure 6 MX-records from Cisco Unity with Primary and Secondary Cisco UMG Information



Setting Up Cisco UMG on Cisco Unity as a Delivery Location with a Dial-ID

Figure 7 Add the Delivery Location on Cisco Unity to umgrtp

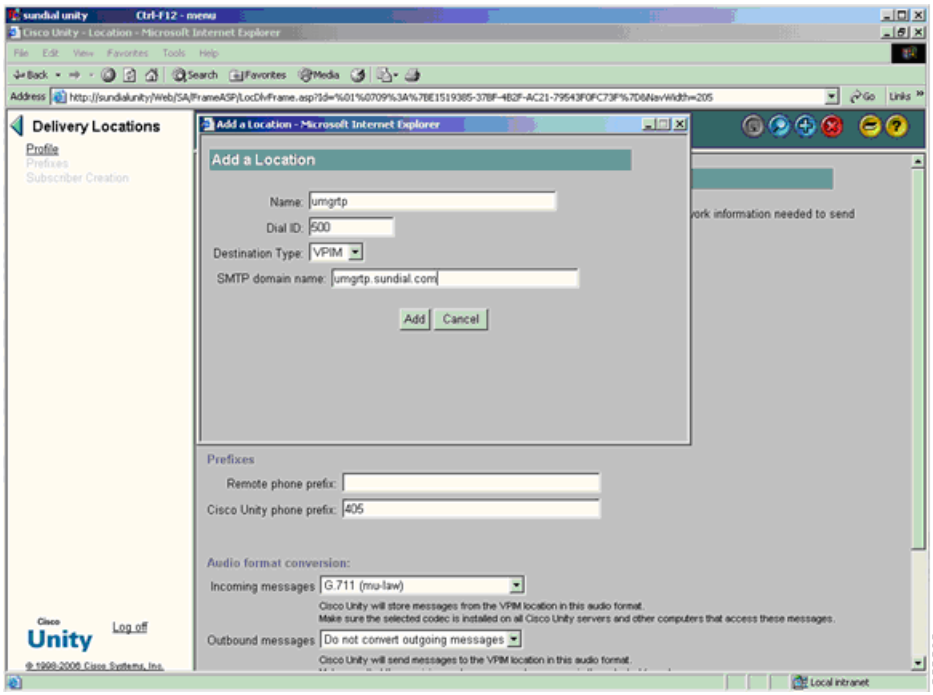
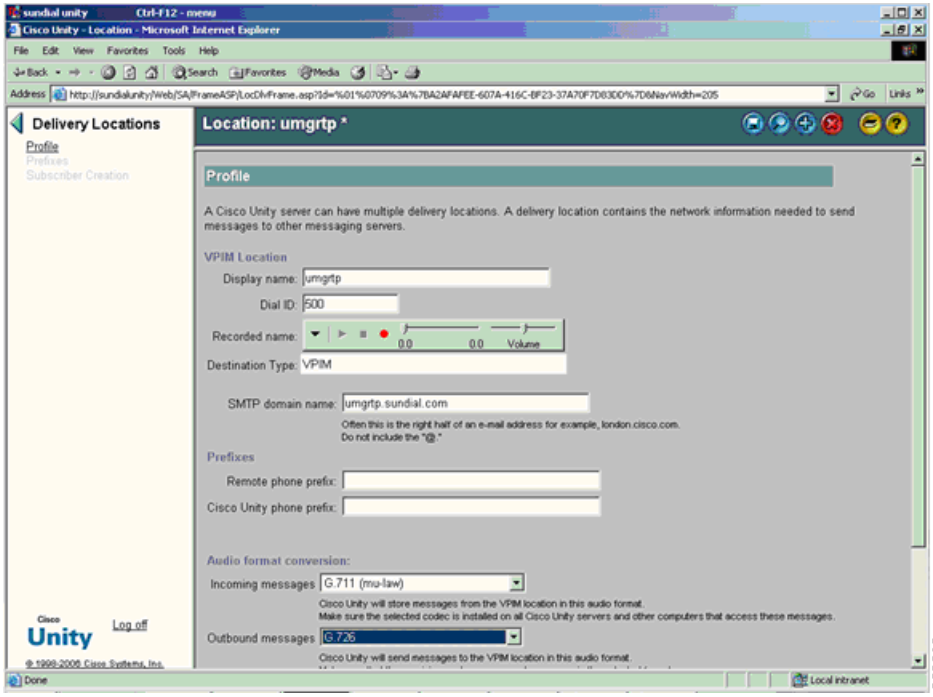


Figure 8 Delivery Location Setup with Other Parameters

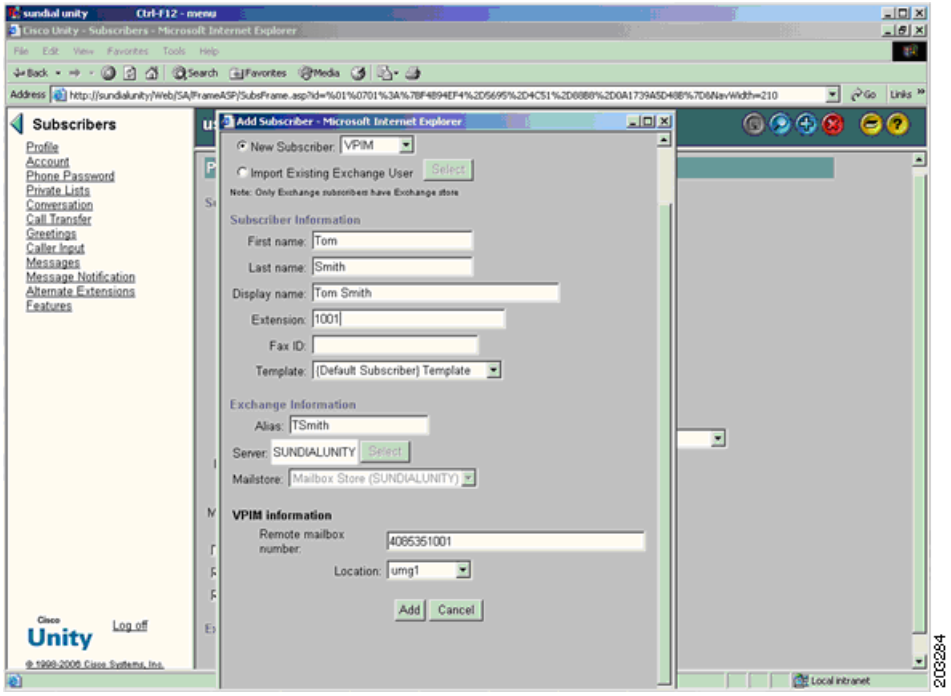


Note When adding the Cisco UMG host as the Delivery location, the Dial ID field on Cisco Unity is the Location ID of the Primary Cisco UMG to which Cisco Unity registered. Leave the Remote Phone Prefix field empty to indicate that any subscriber on Cisco Unity can dial any number outside by dialing the dial_ID followed with the real remote number. Depending on the Cisco Unity dial plan, you can leave the Cisco Unity Phone Prefix field empty or enter the prefix of the Cisco Unity endpoint on Cisco UMG.

Optionally Deploying VPIM Network Using Remote VPIM Subscribers Instead of Delivery Location

In this model, the customer has imported all the remote subscriber information into the Cisco Unity database. When Cisco UMG is inserted into the VPIM network with all remote subscribers registered, the customer can either move from a Remote VPIM subscriber setup to a delivery location setup or stay with a Remote VPIM subscriber setup by setting the VPIM location to the primary Cisco UMG Location ID.

Figure 9 Remote Subscriber VPIM Location Setup on Cisco Unity



Note The deployment involves the information change on every remote VPIM subscriber's setup.

Verifying the Cisco Unity Endpoints on Cisco UMG

```
umgrtp-1> show endpoint local
A total of 2 local endpoint(s) have been found:
Location    Location          Endpoint           Endpoint    Primary     Secondary
ID          Prefix            Type               Status      Gateway     Gateway
-------------------------------------------------------------------------------------
510             919           Unity              Enabled   500         501
511             704           Unity              Enabled   500         501
```

Managing the Avaya Interchange Endpoint on Cisco UMG with Manual Provisioning

The following example is for the north region.

Configuration on umg-n-1

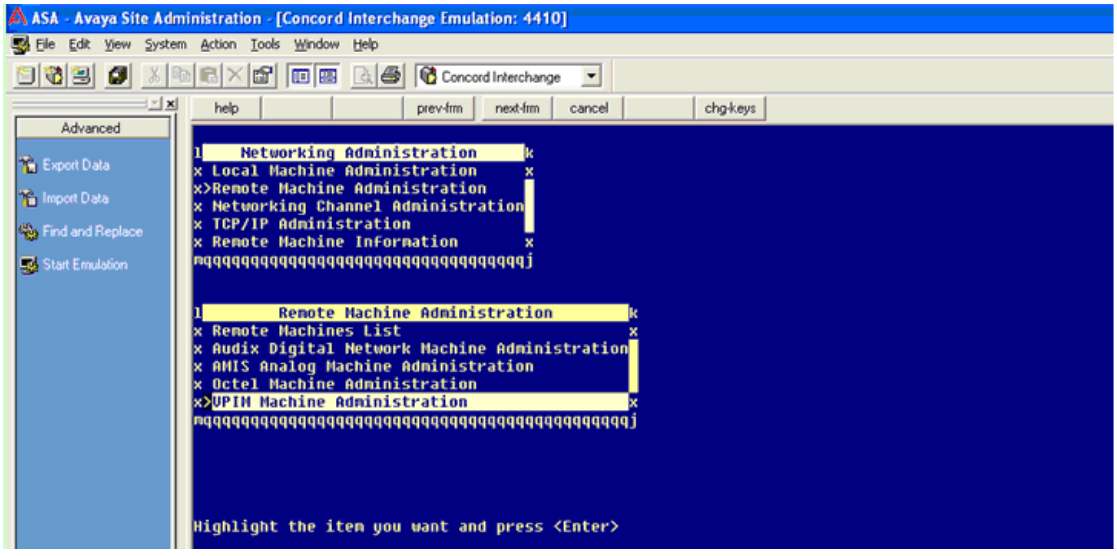
In this example, there is only one Cisco UMG connected to Avaya Interchange, no failover is supported with Avaya Interchange because of the limitation on Avaya Interchange VPIM support.

```
Umg-n-1(config)> endpoint 610 unity
Umg-n-1(config-endpoint)> domain avaya.headquarters.com
Umg-n-1(config-endpoint)> hostname interchange.headquarters.com
Umg-n-1(config-endpoint)> prefix 203
Umg-n-1(config-endpoint)> enable
```

Configuration on Avaya Interchange

Step 1 From the Avaya Interchange Main Menu, choose **Network Administration > Remote Machine Administration > VPIM Machine Administration**.

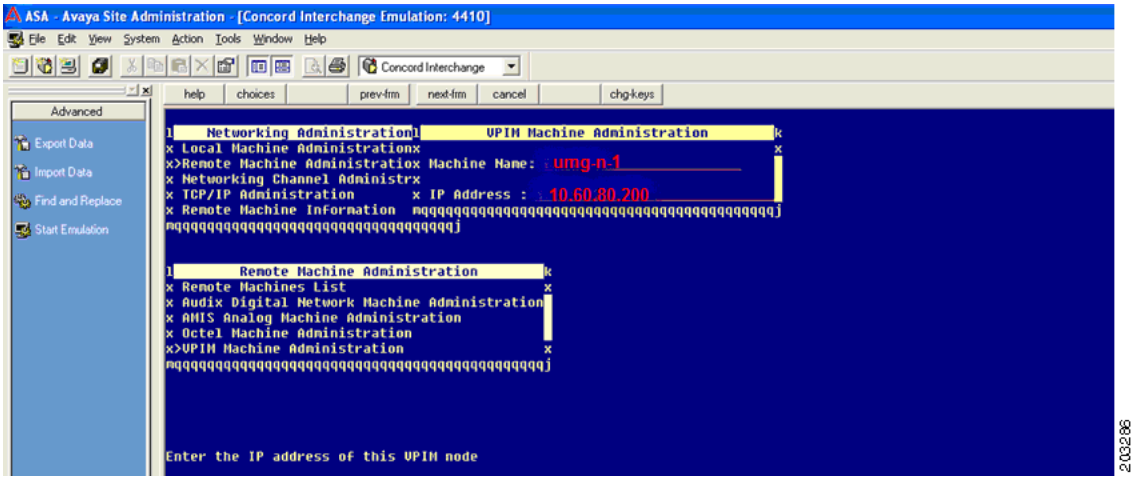
Figure 10 VPIM Machine Admininstration Mode



Step 2 On the VPIM machine administration screen, insert the Cisco UMG host name and IP address

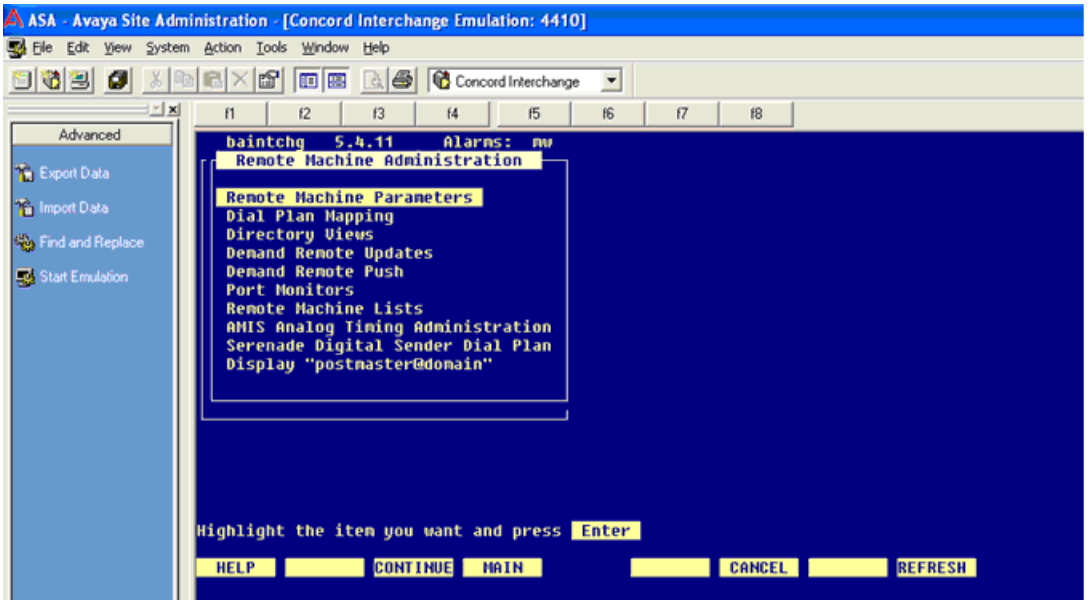
In this example, the Machine Name could be umg-n-1 and the IP address should be 10.60.60.200.

Figure 11 Cisco UMG Configuration on Remote-Machine Configuration Window



Step 3 From the Avaya Interchange Main menu, choose **Interchange Administration** > **Remote Machine Administration** > **Remote Machine Parameters**.

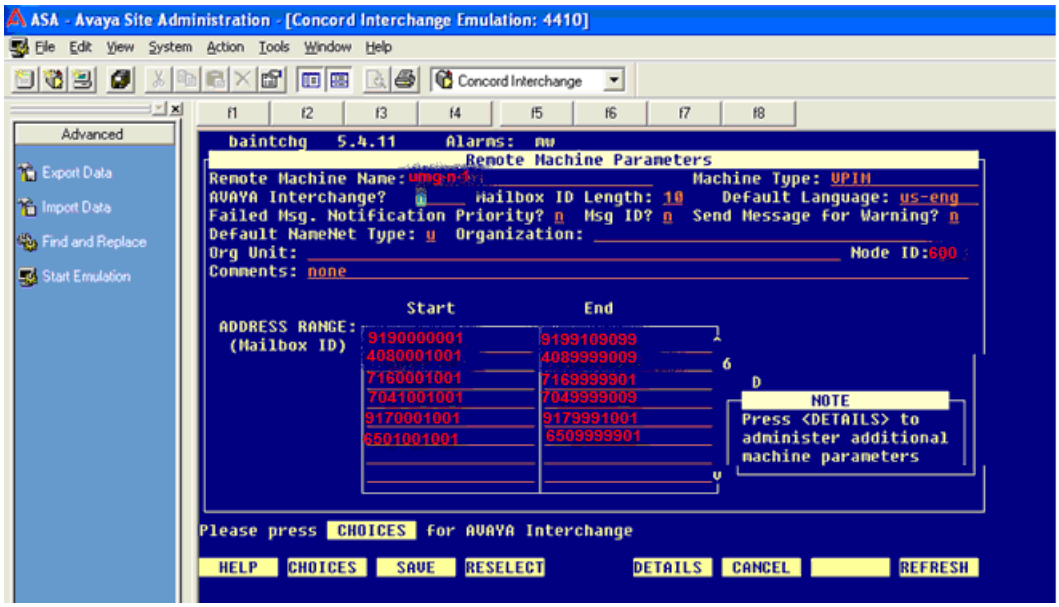
Figure 12 Remote Machine Parameter Configuration Mode



Step 4 On the Remote Machine Parameters screen configure the following:

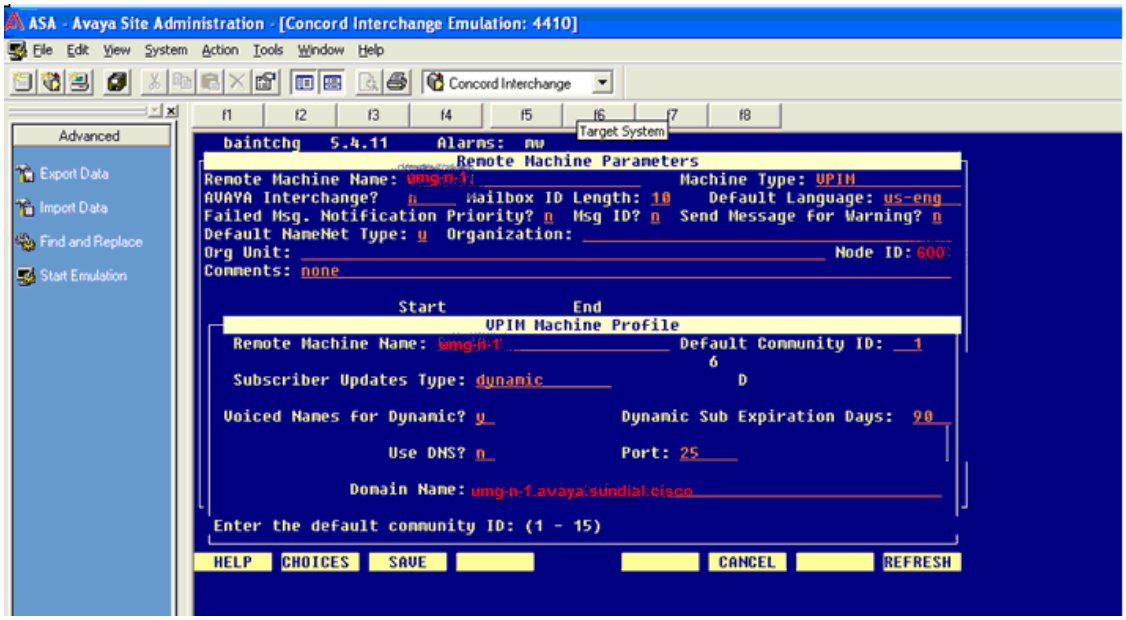
- Cisco UMG name
- Location ID
- E164 numbers.

Figure 13 Basic Remote Machine Parameters Configuration



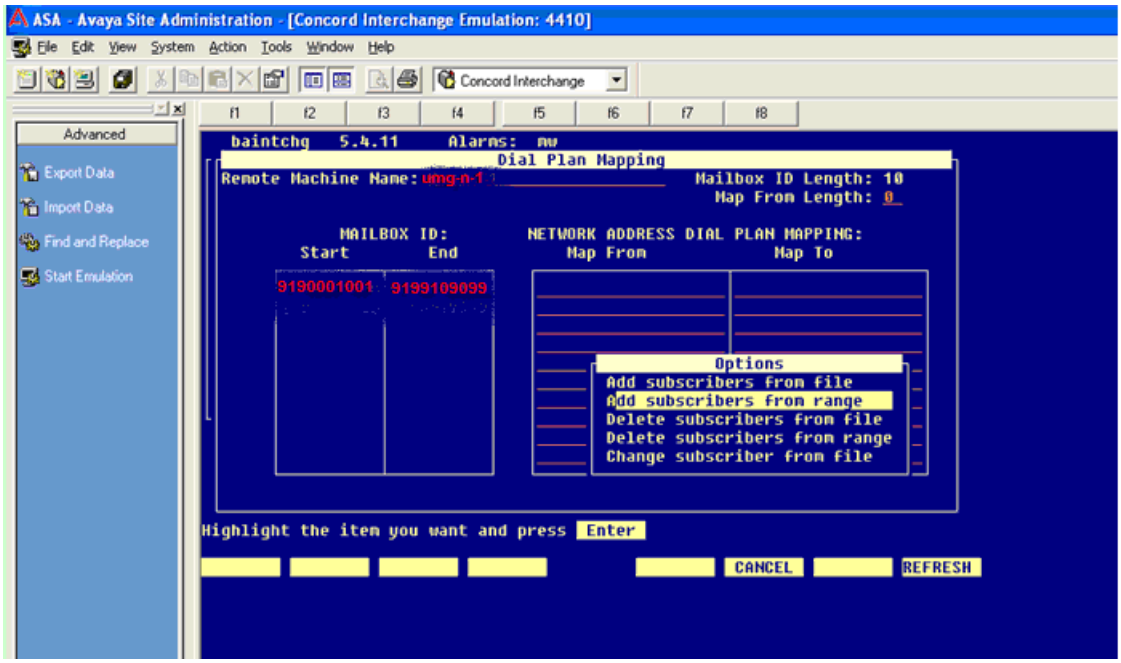
Step 5 Continue on the Remote Machine Parameters screen.

Figure 14 Detailed Remote Machine Parameters Configuration



Step 6 If you must map the dial plan with network dial plan, exit from the Remote Machine Parameters screen and choose **Interchange Administration** > **Remote Machine Administration** > **Dial-Plan Mapping**.

Figure 15 Dial-Plan Mapping Configuration



Note The configuration of other Customer Service parameters, such as Queue and CDR, is not within the scope of this document.

Verifying from umg-n-1

```
Umg-n-1> show endpoint local
A total of 1 local endpoint(s) have been found:
Location    Location          Endpoint          Endpoint    Primary     Secondary
ID          Prefix            Type              Status      Gateway     Gateway
-------------------------------------------------------------------------------------
510           919           Interchange       Enabled     600         N/A
```

Monitoring and Manually Synchronizing Cisco UMG Directory Exchange

The Cisco UMG is an intelligent agent that handles directory information exchange automatically without any manual provisioning effort. The directory exchange can happen between:

- Multiple Cisco UMGs
- Cisco UMG and Cisco Unity Express systems

However, the directory exchange is limited with the autoregistered endpoints, so the directory exchange on Cisco Unity, Cisco Unity Express earlier than version 3.0, and Avaya Interchange is not supported. If you want subscriber level information on the Cisco UMG for those manual endpoints, you can configure the Cisco UMG to use prefix-number-only mode.

During a directory exchange, the following events will occur:

- When the Cisco UMG is first time inserted into a Cisco UMG-controlled messaging network, a full directory exchange is triggered between Cisco UMGs.
- When a Cisco Unity Express first time registers with its primary Cisco UMG, a full directory exchange is triggered between the Cisco Unity Express and its primary Cisco UMG. The secondary Cisco UMG gets information updates from the primary Cisco UMG.
- When any subscriber information is changed on Cisco Unity Express, a directory update occurs between Cisco Unity Express and its primary Cisco UMG. Next a directory exchange occurs between the primary Cisco UMG and all its peer gateways through the fully meshed unicast network.
- When Cisco Unity Express or Cisco UMG goes down and comes back online, a directory exchange is triggered on Cisco Unity Express and Cisco UMG, and across all the Cisco UMGs in the network.
- When a Cisco UMG detects out-of-sync data either from its endpoints or its peer Cisco UMGs, it tries to perform a directory update to recover. If it cannot recover, a full directory exchange is triggered.

Although the Cisco UMG can synchronize the directory information across your entire network, a set of CLI commands for Cisco Unity Express 3.1 and Cisco UMG 1.0 enable you to manually perform a directory exchange if the automatic resynchronization takes too long or is not invoked.

To manually perform a directory exchange, configure both Cisco Unity Express and the Cisco UMG as described below.

Manually Synchronizing Cisco UMG Directory Exchange on Cisco Unity Express

To synchronize directory exchange for Cisco Unity Express, use the following command:

```
messaging-gateway directory exchange [full | update]
```

Manually Synchronizing Cisco UMG Directory Exchange on Cisco UMG

To synchronize directory exchange on Cisco UMG, use the following commands:

```
directory exchange endpoint request [full | update]
directory exchange endpoint request [full | update] LOCATIONID
directory exchange messaging-gateway request [full | update]
directory exchange messaging-gateway request [full | update] LOCATIONID
directory exchange messaging-gateway send [full | update]
directory exchange messaging-gateway send [full | update] LOCATIONID
```

Note Use the manual directory-exchange only when out-of-sync directory information cannot be fixed by the automatic directory-exchange processes.

When applying the CLI commands shown above, examine the available bandwidth before flooding all the directory exchange information to endpoints or Cisco UMGs. If possible, use the commands only for certain nodes, during off-peak hours.

Verifying the Directory Information Exchange on the Cisco UMGs in the Network

Verifying the Endpoint

This example is for the Cisco UMG on East Region, umg-e-1.

```
umg-e-1> show endpoint local
    A total of 3 local endpoint(s) have been found:
    Location    Location          Endpoint          Endpoint    Primary     Secondary
    ID         Prefix            Type              Status      Gateway     Gateway
-------------------------------------------------------------------------------------
    310             716           CUE             Enabled   300        301
    311             716           CUE             Enabled   300         301
    312             917           CUE             Enabled   300         301

umg-e-1> show endpoint network
    A total of 6 network endpoint(s) have been found:
    Location   Location            Endpoint     Primary     Secondary
    ID         Prefix              Type         Gateway     Gateway
-------------------------------------------------------------------------------------
    510            919               Unity          500   501
    511            704              Unity         500      501
    410            408              CUE            400    401
    411            408              CUE             400     401
    412            650              CUE             400     401
    610            203              Interchange      600  n/a
```

Verifying the Subscriber

This example is for umg-e-1 and umg-w-1.

```
Umg-e-1# show mailbox 410
2 mailbox(s) has been found for location 410

4085550101
4085550102
```

The two subscriber numbers are exchanged from automatic directory exchange.

```
Umg-w-1# show mailbox 310
2 mailbox(s) has been found for location 310

7165550101
7165550102
```

The 2 subscriber numbers are exchanged by manual provisioning.

```
Umg-w-1# show mailbox 510
No mailbox has been found for location 510
```

No automatic directory exchange and manual provisioning.

Note All the Cisco UMGs in the network must have identical directory tables.

For autoregistered endpoints, the directory table contains the subscriber level information.

For manually provisioned endpoints, the directory table contains the subscriber level information only if prefix-number-only mode is enabled and the extensions are manually configured.

For manually provisioned endpoints without prefix-number-only sub mode enabled, no subscriber level information is in the directory table.

Message Routing and Delivery on Cisco UMG

The Cisco UMG (primary or secondary) that hosts an endpoint is responsible for routing the messages from that endpoint. The Cisco UMG utilize information from the directory table to route messages. Messages are routed differently, depending on the registration method of the destination endpoint.

If the destination endpoint is an autoregistered endpoint, the Cisco UMG routes on the subscriber level, which means the Cisco UMG searches for the destination number in its directory table to find the termination node.

If the destination endpoint is a manually provisioned endpoint, the Cisco UMG first routes using the prefix. If only one location with the prefix is found in the directory table, the routing is complete. If more than one location is found with the prefix, the Cisco UMG next looks at the prefix + extension level, which is configured under prefix-number-only mode.

For any VPIM message received on the Cisco UMG, the message destination “To” field could be a System Distribution List (SDL), SBM, or a subscriber number (E.164 phone number scheme). SDLs are matched first. If an SDL overlaps any other number, the SDL masks that number. All SDLs must begin with a numerical sequence that is unique to the system.

The Cisco UMG resolves the destination in the precedence of SDL, SBM, and subscribers. If the message destination does not match any of the existing SDLs, the Cisco UMG searches for a match in the list of configured broadcast endpoints. If no match is found, the Cisco UMG tries to resolve the message destination as a subscriber. If a match is still not found, the message is dropped, resulting in a Non-Delivery-Receipt (NDR).

You can configure a default route on Cisco UMG in case no destination is matched in Cisco UMG's database. For example, in the west region, the default route can be set up to point to cue-w-1, as shown below:

```
Umg-w-1(config)# network default-route 410
Umg-w-1> show network default-route
```

Note In Cisco UMG 1.0, The default route can be a local endpoint or a peer Cisco UMG. However, to avoid looping, there must be a default route plan, such that no message ever gets passed to more than two Cisco UMGs. In other words, if at any time an originating Cisco UMG specifies another Cisco UMG as a default route, that Cisco UMG must be the terminating Cisco UMG and therefore should have its default route set to a local endpoint.

When the address and route are resolved, the message is inserted into delivery queue and is ready to deliver. You can configure DDR and NDR timers to handle any delivery retry and failure cases.

Table 5 lists the DDR reason codes from Cisco UMG 1.0:

Table 5 Cisco UMG NDR reason codes

NDR Code	Cisco Unity Express	Cisco Unity
4.2.1	The remote voice mail system did not accept the message	The recipient's mailbox is not accepting network messages.
4.2.2	The recipient's mailbox is full	The message format is not allowed for delivery to the remote voice mail system.
4.3.1	The remote voice mail system did not accept the message	The message format is not allowed for delivery to the remote voice mail system.
4.3.2	The remote voice mail system did not accept the message	The recipient's mailbox is not accepting network messages.
5.1.1	The recipient's mailbox does not exist	The remote voice mail system was not able to accept the message.
5.2.0	The message format was not accepted by the remote voice mail system	Network problems prevented routing to the remote voice mail server
5.3.2	Networking is disabled	The recipient's mailbox is not accepting network messages.
5.4.1	Could not contact the remote voice mail system	The remote voice mail system could not be contacted.
5.7.9	The message format was not accepted by the remote voice mail system	The message format was not accepted by the remote voice mail system

To check the Cisco UMG messaging routing and delivery statistics, use the **show statistics** command on the Cisco UMG, as shown below:

```
Umg-w-1> show statistics

SMTP Receive Failure:          0
SMTP Sent Failure:             0
SMTP Rejected:                 2
NDR Message Generated:         0
DDR Message Generated:         0
Number of Lookup Request:      0
SDL Message Received:          0
SDL Message Sent:              0
SBM Message Received:          0
DirEx Message Received:        14
DirEx Message Send:            12
VPIM Message Received:         0
VPIM Message Sent:             0
Total SMTP Message Received:   14
Total SMTP Message Sent:       12
```

Setting Up Directory Lookup with TUI or VVE Interface

In Cisco UMG 1.0, a global search option is available to the end users when no match is found in the endpoint's local database (Cisco Unity Express).

You must enable the feature on the endpoint during the registration process. After configuring the hosting message gateway username and password, use the following command before starting the registration process.

```
cue(config)# messaging-gateway directory lookup tui-prompt
```

To check the feature's availability on the endpoint:

```
cue# show messaging-gateway
Messaging gateways:

AutoRegister to gateway(s) : Enabled
Remote directory lookup : Enabled (with TUI prompt)
```

Note To use the Cisco VVE interface, VoiceView Service must be enabled on Cisco Unity Express and a URL must be defined on the Cisco Unified CME telephony-interface. For detailed configuration information, see the *Cisco Unified CME System Administrator's Guide* and the *Cisco Unity Express Administrator's Guide*.

Directory lookup can be enabled with or without TUI confirmation.

Setting Up Spoken-Name Confirmation Across AutoRegistered Cisco Unity Express Endpoints

By default, spoken name is disabled on the Cisco UMG, which means that the spoken names received from Cisco Unity Express endpoints are not stored in the Cisco UMG directory database, and the spoken name are not part of the directory exchange with its peers. When this feature is enabled, Cisco Unity Express caches the location spoken names and plays them back to the end user.

To invoke this feature, you must configure both Cisco Unity Express and Cisco UMG:

On Cisco Unity Express:

```
Cue-w-1(config)# remote cache enable
```

Note Remote cache is mandatory for the Cisco UMG spoken-name feature.

On Cisco UMG

```
umg-w-1(config)# spoken-name enable

umg-w-1# show spoken-name
Spoken name is enabled.
```

If Cisco Unity Express already registered with the Cisco UMG before spoken-name is enabled, you must use the following CLI to trigger directory exchange to update spoken-name information:

```
Cue-w-1(config)# no messaging-gateway registration
Cue-w-1(config)# messaging-gateway registration
```

If spoken-name is already stored in the Cisco UMG database, disabling spoken-name does not delete the entry from the directory table until the new directory updates occurs.

Using System Distribution Lists Across Cisco Unity Express Systems

System Distribution Lists (SDLs) are created and managed in EXEC mode, not configuration mode. Each SDL can have one or more members, each of which could be one of the following entities:

- A subscriber
- Another SDL list

SDLs are shared among Cisco UMGs and can be managed on any Cisco UMG in a network. SDLs are created and edited in list-management mode, which is the submode of EXEC mode. When list-management mode is exited on one Cisco UMG, all SDL changes are pushed out to all other Cisco UMGs in the network. At any time, only one Cisco UMG can manage the SDL information. Other Cisco UMGs are not able to enter list-management mode to manage SDLs until the Cisco UMG that was in the list-management mode exits from that mode or a 5-minute timeout when there is no exit request from the Cisco UMG that is currently in list-management mode.

As an example, the following sections show how to create three SDLs. These SDLs are for:

- West region
- East region
- Both west region and the east region

In this example, umg-w-1 is the master Cisco UMG.

Creating an SDL with Privileges

```
umg-w-1# list-manager
Locking system distribution lists...[OK]--> The umg-w-1 declare itself as the master UMG

## The following is the SDL list of the west region ##
Umg-w-1(listmgr)# list number 900    --> The list number must be a unique number
Umg-w-1(listmgr-edit)# name SDL_WEST

umg-w-1(listmgr-edit)# member 4085550101 type sub
umg-w-1(listmgr-edit)# member 4085550102 type sub
umg-w-1(listmgr-edit)# member 4085550001 type sub
umg-w-1(listmgr-edit)# member 4085550003 type sub

umg-w-1(listmgr-edit)# privilege 4085550101 --> Assign the authority to 2 members
umg-w-1(listmgr-edit)# privilege 4085550001

## The following is the SDL list of the east region ##
Umg-w-1(listmgr)# list number 910    --> The list number must be a unique number
Umg-w-1(listmgr-edit)# name SDL_EAST

umg-w-1(listmgr-edit)# member 7165550021 type sub
umg-w-1(listmgr-edit)# member 7165550042 type sub
umg-w-1(listmgr-edit)# member 7165550061 type sub
umg-w-1(listmgr-edit)# member 7165550082 type sub

umg-w-1(listmgr-edit)# privilege 7165550021 --> Assign the authority to 2 members
umg-w-1(listmgr-edit)# privilege 7165550082

## the following is the SDL list of west and east regions

Umg-w-1(listmgr)# list number 999    --> The list number must be a unique number
Umg-w-1(listmgr-edit)# name SDL_E_W

umg-w-1(listmgr-edit)# member 900 type list
umg-w-1(listmgr-edit)# member 910 type list

umg-w-1(listmgr-edit)# privilege 7165550021 --> Assign the authority to 2 members
umg-w-1(listmgr-edit)# privilege 4085550101
```

Publishing the SDLs to All Peer Cisco UMGs in the Network

Use either the manual **list publish** command or exit from SDL configuration mode.

```
umg-w-1(listmgr)# list publish     --> This is optional CLI, SDL will get automatically
published when exiting from listmgr mode
LocationID        Status          Description
-----------------------------------------------------------
500               Published
501               Published
401               Published
300               Published
301               Published
600               Published
601               Published

# of network gateways published:        7
# of network gateways failed to publish:0
```

Unlocking the SDL Configuration

```
umg-w-1(listmgr-edit)# exit
umg-w-1(list)# exit
auto publishing to all ...
LocationID        Status          Description
500               Published
501               Published
401               Published
300               Published
301               Published
600               Published
601               Published

# of network gateways published:        7
# of network gateways failed to publish:0
```

Verifying the SDL Configuration on Any Cisco UMG in the System

```
umg-e-1(listmgr)# show list 900
Extension:   000
Name:        SDL_WEST
Member(s):   4085550101 (subscriber)
             4085550102 (subscriber)
             4085550001 (subscriber)
             4085550003 (subscriber)
             -----
             # of members: 4

umg-e-1# show list 900 privilege --> Under UMG exec mode
2 authorized sender(s) has been found for system distribution list 900:

4085550101
4085550001
```

Verifying that SDL is Synchronized Between Cisco UMGs

Use these commands to check the SDL versions on Cisco UMGs and verify that SDL is synchronized:

```
Umg-e-1 > show list tracking version
The version of system distribution list is 70173_04062007030517.

Umg-w-1 > show list tracking version
The version of system distribution list is 70173_04062007030517.
```

Note In a Cisco UMG network, only one Cisco UMG can create, modify, or delete the SDL at any time. When you enter list-manager mode, the SDL is automatically locked and it cannot be managed by other Cisco UMGs. The **exit** command from list-management mode automatically enables other Cisco UMGs in the network to access SDL list-management mode for SDL creation/Modification/Deletion.

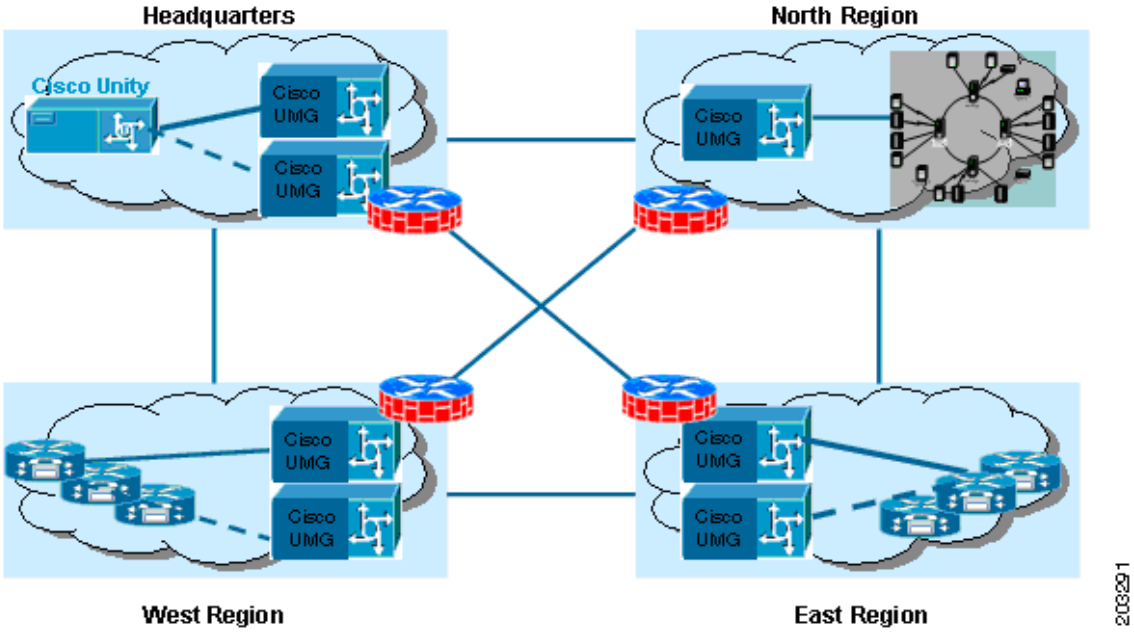
The SDL information is published across all Cisco UMGs in the network when the Cisco UMG that manages the SDLs exits from list-management mode.

Subscribers of SDLs must have the correct privileges setup to send SDL messages. A subscriber without a correct SDL privilege receives a NDR from the Cisco UMG when sending out an SDL message.

Setting Up NAT Tables on Cisco UMG

Figure 16 shows an example of a Network Address Translation (NAT) device used on the edge of every region. In this example, the NAT is required during directory exchange between Cisco UMGs and message delivery across the regions.

Figure 16 NAT Configuration Example in a Cisco UMG Network



The headquarters Cisco UMG and west region Cisco UMG are used as the sample configuration here.

```
On umg-h-1:
Umg-h-1(config)> nat location 400
Umg-h-1(config-nat)> vpim external 128.1.2.3 26
Umg-h-1(config)> nat location 401
Umg-h-1(config-nat)> vpim external 128.1.2.3 27
```

Table 6 shows what the NAT table may look like on the headquarters Cisco UMG.

Table 6 NAT Table on Central Cisco UMG

Peer	Internal IP	External IP	External SMTP Port
400 (UMG-W-1)	10.60.70.200	128.1.2.3	26
401(UMG-W-2)	10.60.70.201	128.1.2.3	27

Note On the umg-h-2, the same NAT configuration must be duplicated.

The VPIM port 26 and 27 are specified to umg-w-1 and umg-w-2, because they share the same external IP address: 128.1.2.3.

The above configuration is the NAT table for only the west region configured on UMG-H-1, the rest of regions are not covered.

The forwarding table on the headquarters NAT device might have a mapping table like this:

```
    Forward 128.1.1.3:26 10.60.80.200:25  for UMG-H-1
    Forward 128.1.1.3:27 10.60.80.201:25  for UMG-H-2
On umg-w-1:
Umg-w-1(config)> nat location 500
Umg-w-1(config-nat)> vpim external 128.1.1.3 26
Umg-w-1(config)> nat location 501
Umg-w-1(config-nat)> vpim external 128.1.1.3 27
```

Table 7 shows what the NAT table might look like on the headquarters Cisco UMG.

Table 7 NAT Table on the West Region Cisco UMG

Peer	Internal IP	External IP	External SMTP Port
500 (UMG-h-1)	10.60.80.200	128.1.1.3	26
501(UMG-h-2)	10.60.80.201	128.1.1.3	27

Note On the umg-w-2, the same NAT configuration must be duplicated.

The VPIM port 26 and 27 are specified to umg-h-1 and umg-h-2, since they share the same external IP address: 128.1.1.3.

The above configuration is the NAT table for the headquarters on UMG-w-1 only. The rest of regions are not covered.

The forwarding table on the west region NAT device might have the mapping table like this:

```
Forward 128.1.2.3:26 10.60.70.200:25  for UMG-W-1
Forward 128.1.2.3:27 10.60.70.201:25  for UMG-W-2
```

Setting Up Backup and Restore for Cisco UMG

In this example, configuration and data backup is configured on umg-w-1. We do not recommend data-only backup and restore.

Ensuring the System Consistency Across Backup and Restore

Use the **copy running-config startup-config** command to write to memory before backup:

```
Umg-w-1> copy running-config startup-config
```

Setting Up the Backup Version and FTP server

```
Umg-w-1(config)> backup server url ftp://10.60.70.100/umg-backup username test password
test
Umg-w-1(config)> backup revisions 1
```

Take the Cisco UMG Offline and Choose Backup Category All

Note The backup and restore must be done in offline mode!

```
Umg-w-1(config) > offline
!!!WARNING!!!: If you are going offline to do a backup, it is recommended that you save
the current running configuration using the 'write' command, prior to going to the offline
state.
Putting the system offline will terminate all end user sessions.
Are you sure you want to go offline[n]? : y
UMG(offline) > backup category all
```

Check the Backup_ID to Decide which Revision to Restore

Go to the backup location on the FTP server and verify that the backup files are there. You can retrieve the backup ID using the **show backup server** command which lists all available back copies on the remote backup server.

Take the Cisco UMG Offline and Choose Backup_ID to Complete the Restore

```
UMG(config) > offline
!!!WARNING!!!: If you are going offline to do a backup, it is recommended that you save
the current running configuration using the 'write' command, prior to going to the offline
state.
Putting the system offline will terminate all end user sessions.
Are you sure you want to go offline[n]? : y
UMG(offline) > restore id data1 category all
UMG(offline) > continue
```