



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.

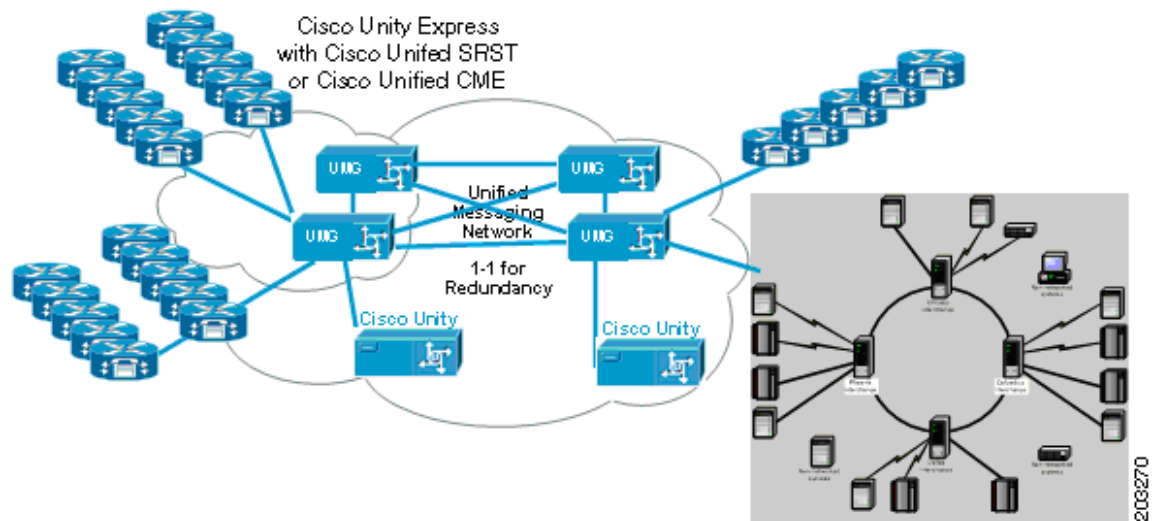
A Cisco UMG controlled messaging network is a mix of fully-meshed connections (between Cisco UMGs) and hub-and-spoke connections (between the Cisco UMG and its registered endpoints).



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.