



# CHAPTER 16

## Cisco Unified MeetingPlace Express

---

Last revised on: February 13, 2008

Cisco Unified MeetingPlace Express is a rich-media appliance for voice and web collaboration. This chapter addresses system-level design considerations. For detailed product information, refer to the product documentation available on

<http://www.cisco.com>

### Deployment Models

This section describes design recommendations for integrating Cisco Unified MeetingPlace Express with the following major IP Telephony deployment models:

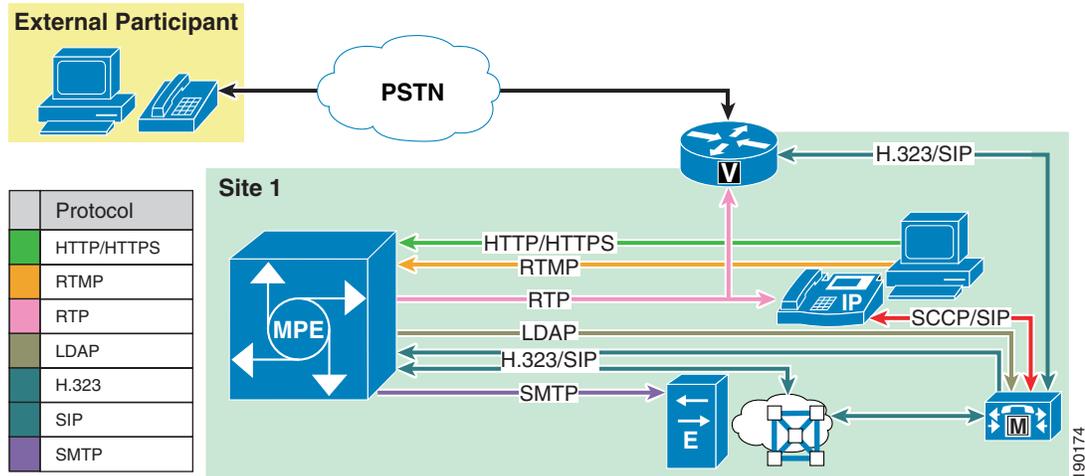
- [Single Site, page 16-2](#)
- [Multisite WAN with Centralized Call Processing, page 16-3](#)
- [Multisite WAN with Distributed Call Processing, page 16-4](#)
- [Clustering Over the WAN, page 16-5](#)

In addition to these deployment models, this section covers deployments based on a demilitarized zone (DMZ). The DMZ deployment is treated separately and is applicable to each of the IP Telephony deployment models listed above. (See [Security and DMZ Deployment, page 16-5](#).)

## Single Site

In a single-site deployment, all call processing is local and all participants are local as well. Bandwidth is usually not a concern, as it would be in multisite configurations. In this model, the Cisco Unified MeetingPlace Express server connects to Cisco Unified CallManager through a gatekeeper, H.323 trunk, or SIP trunk. (See [Figure 16-1](#).)

**Figure 16-1** Single-Site Deployment

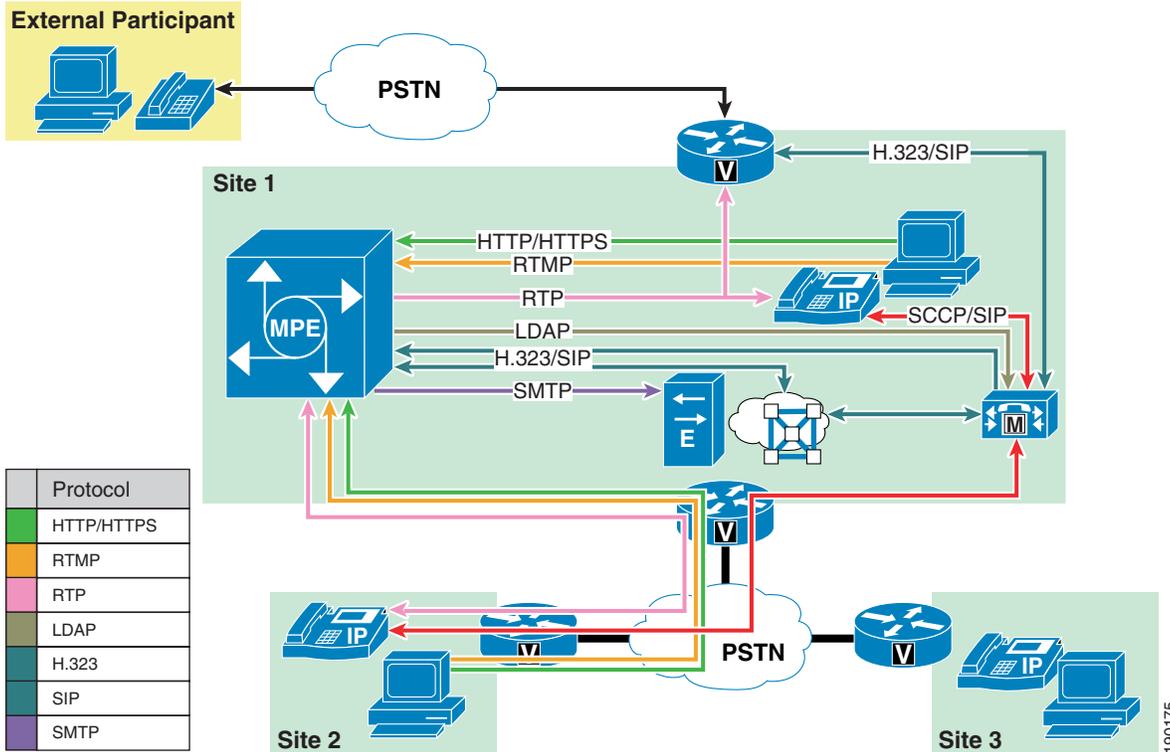


The general design considerations presented in the remaining sections of this chapter apply to this basic deployment model.

## Multisite WAN with Centralized Call Processing

In a multisite WAN deployment with centralized call processing, the Cisco Unified MeetingPlace Express server is usually located in the central site, where all call processing occurs. (See [Figure 16-2](#).)

Figure 16-2 Multisite WAN Deployment with Centralized Call Processing



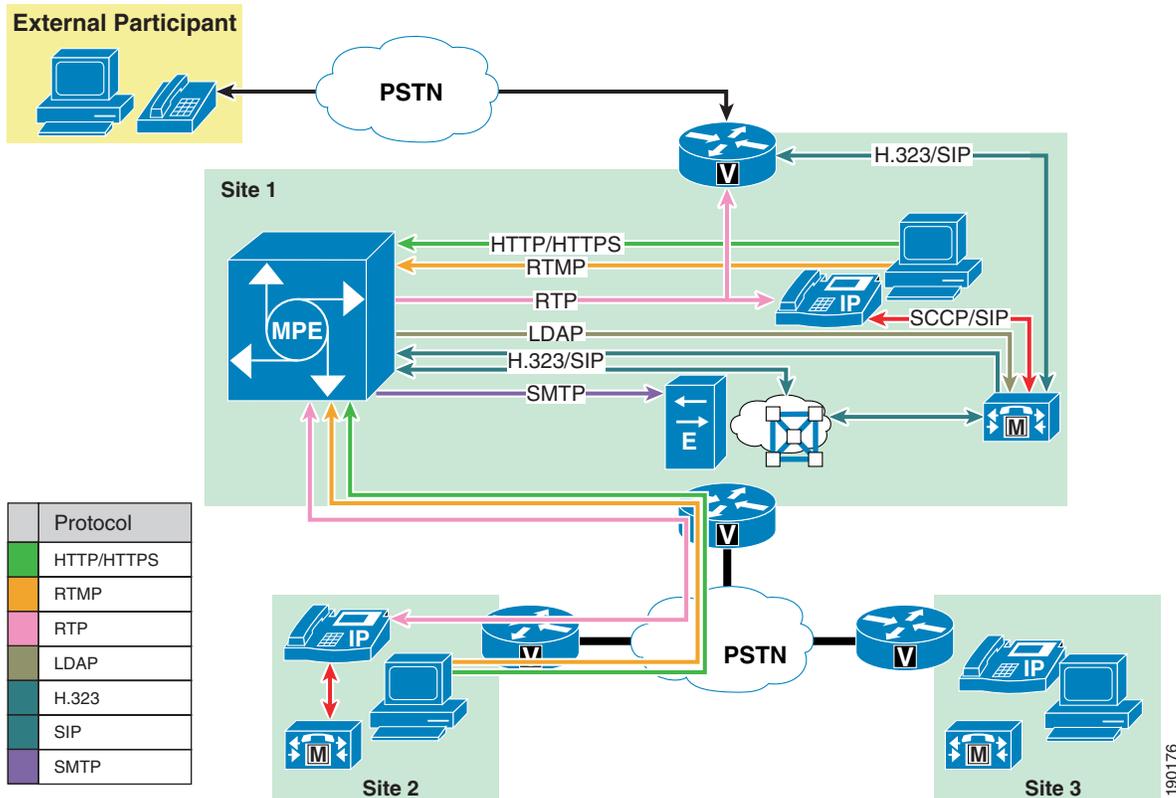
In this deployment, participants in the central site have no special considerations, but participants at remote sites require the following additional considerations:

- Cisco Unified MeetingPlace Express supports only G.711. Transcoders at the central site must be used for all remote calls other than G.711.
- Web collaboration requires significant bandwidth that must be provisioned. (See [Bandwidth Considerations for Web Applications and Screen Sharing](#), page 16-7.)
- The same QoS and call admission control mechanisms used for the existing IP Telephony deployment are required. For purposes of call admission control, the Cisco Unified MeetingPlace Express server should be treated as a telephony endpoint in the central site.

## Multisite WAN with Distributed Call Processing

In a multisite WAN deployment with distributed call processing, the Cisco Unified MeetingPlace Express server is usually located in a single site local to Cisco Unified CallManager, similar to a multisite WAN deployment with centralized call processing. [Figure 16-3](#) depicts an example of a multisite WAN deployment with distributed call processing.

**Figure 16-3** Multisite WAN Deployment with Distributed Call Processing



This deployment differs from a multisite WAN deployment with centralized call processing because the call processing is distributed to multiple sites. These sites may use Cisco Unified CallManager, Unified CallManager Express, or other methods of call processing. Because Cisco Unified MeetingPlace Express is a single server with no cascading, mirroring, or redundancy capabilities, a single active server at a single site would be typical. An additional server as a secondary active server may be deployed at a separate site but would not allow for a true failover environment. See [Redundancy](#), page 16-12, for more information.

To have a multisite redundant and distributed collaboration system, consider Cisco Unified MeetingPlace as an option. See the chapter on [Cisco Unified MeetingPlace Integration](#), page 15-1, for more information.

### Design Considerations

In this deployment, participants local to the Cisco Unified MeetingPlace Express server have no special considerations, but participants remote from the Cisco Unified MeetingPlace Express server require the following additional considerations:

- Cisco Unified MeetingPlace Express supports only G.711. Transcoders at the site containing the Cisco Unified MeetingPlace Express server must be used for all remote calls other than G.711.
- Web collaboration requires significant bandwidth that must be provisioned. (See [Bandwidth Considerations for Web Applications and Screen Sharing, page 16-7](#).)
- The same QoS and call admission control mechanisms used for the existing IP Telephony deployment are required. For purposes of call admission control, the Cisco Unified MeetingPlace Express server should be treated as a telephony endpoint in its local site.
- The Cisco Unified CallManager cluster at the remote site (Site 2 in [Figure 16-3](#)) can directly route calls to Cisco Unified MeetingPlace Express located at the central site (Site 1) by defining an H.323 gateway or SIP trunk directly on the remote cluster. This practice is not recommended due to its potential impact on call admission control. Routing calls directly to MeetingPlace and not through the central cluster via an intercluster trunk or through gatekeeper can cause calls not to be accounted for in call admission control measurements.

## Clustering Over the WAN

In a deployment with clustering over the WAN, the Cisco Unified CallManager cluster is split across one or more locations separated by high-capacity and high-speed WAN or MAN links. Cisco Unified MeetingPlace Express does not have any server-to-server redundancy and cannot fully utilize the redundant nature of this model. An additional server as a secondary active server may be deployed at the alternate site but would not allow for a true failover environment. See [Redundancy, page 16-12](#), for more information.

Placement and design considerations would be identical to the previous deployment model, [Multisite WAN with Distributed Call Processing, page 16-4](#).

To have a multisite redundant and distributed collaboration system, consider Cisco Unified MeetingPlace as an option. See the chapter on [Cisco Unified MeetingPlace Integration, page 15-1](#), for more information.

## Security and DMZ Deployment

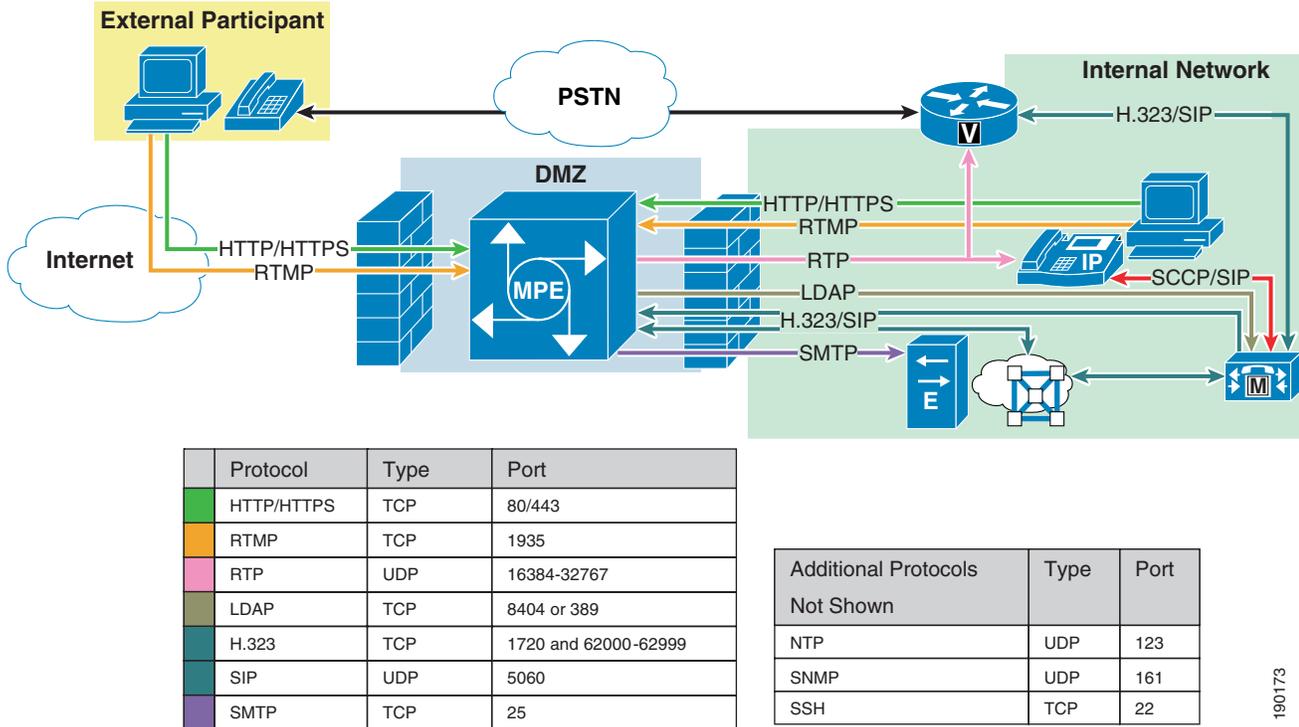
Cisco Unified MeetingPlace Express may be placed in a demilitarized zone (DMZ), although there is no mechanism to allow internal and external applications because it is a single server. All internal and external web collaboration and telephony calls must reach the Cisco Unified MeetingPlace Express server in the DMZ.

External telephony calls would come into a gateway inside the firewall and be treated the same as internal calls being sent into the DMZ to connect to the Cisco Unified MeetingPlace Express server.

External web collaboration would come into the DMZ from outside the firewall, and internal from inside.

[Figure 16-4](#) illustrates communication between the Cisco Unified MeetingPlace Express server in the DMZ and the internal and external networks.

Figure 16-4 DMZ Deployment



190173

### Design Considerations for DMZ Deployment

- If port 1935 is not configured in the firewall access control list (ACL), Real Time Messaging Protocol (RTMP) traffic will tunnel over port 80 with a small performance hit.
- If Network Time Protocol (NTP) is to be used, connectivity internally or externally to an NTP source over port 123 is needed.
- Secure Shell (SSH) access over port 22 to the server from the internal network might be needed. Cisco Technical Assistance Center (TAC) might require SSH access to support Cisco Unified MeetingPlace Express properly.
- Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP) ports are required for voice termination on the Cisco Unified MeetingPlace Express server. With Cisco firewall devices, RTP ports will be opened dynamically to allow the correct traffic flows through the firewall based on the H.323 or SIP call setup. Therefore, it is not necessary to open a range of ports on the firewall.

# Call Admission Control, Bandwidth, and QoS

This section describes important call admission control, bandwidth, and QoS considerations for Cisco Unified MeetingPlace Express deployments.

## Call Admission Control

Cisco Unified MeetingPlace Express should be treated as a local voice gateway for purposes of call admission control. For additional guidance on call admission control, see the chapter on [Call Admission Control, page 9-1](#).

## Bandwidth Considerations for Web Applications and Screen Sharing

Screen sharing consumes large amounts of bandwidth, on the order of 2 Mbps per user in the worst case. Because of the excessive bandwidth and bursty nature of screen sharing, the following design considerations must be observed.

### Design Considerations

Use of 100 Mbps for LAN connectivity will limit the number of concurrent web collaboration sessions. When possible, use 1 Gbps connections.

Users at remote sites that cause web collaboration to traverse a WAN will require special consideration. The client flash session bandwidth or room bandwidth setting for these users should be lowered, reducing the load across the WAN. Because web collaboration data is delivered unicast, the largest burst of data should be multiplied by the number of clients at a remote site. For example, assume a remote site has 100 users, 10 of which are on a web collaboration session at any one time. If bursts of 2 Mbps occur in the data from the remote server to each user, 20 Mbps bursts can be experienced across the WAN connection.

When WAN links become congested from excessive web collaboration data or other sources, the degradation of all traffic is compounded by packet loss, retransmissions, and increased latency. Sustained congestion will have a sustained degrading impact on all remote collaboration sessions.

The following settings on the client web collaboration sessions control the rate at which the participant receives data as well as the rate at which the presenter sends data:

- **Modem** — Bandwidth limited to 64 kbps
- **DSL** — Bandwidth limited to 640 kbps
- **LAN** — Bandwidth up to 3,000 kbps (Bandwidth bursts above 3,000 kbps are possible if high-resolution images or photos are shared. Sharing normal to complex presentations or document should not generate bursts above 3,000 kbps unless large complex images are embedded.)

Bandwidth settings are not automatically adjusted when congestion occurs; they must be adjusted manually. Bandwidth settings default to LAN and must be set at the initialization of each collaboration session. A new session is set to LAN regardless of previous settings.

Bandwidth settings can be adjusted in the following locations in the web collaboration client screen:

- My Connection Speed
  - Limits the speed data is delivered to an individual user from the Cisco Unified MeetingPlace Express server.

- Limits the speed data is sent from the presenter to the Cisco Unified MeetingPlace Express server.
- Presenter speed does not limit the rate at which participants receive data.
- Optimize Room Bandwidth
  - Limits the rate data is delivered to all users.
  - Currently has data burst issues and might impact WAN bandwidth utilization.

**Note**

The setting for My Connection Speed on the client web interface for the presenter and participant are independent of each other. Presenter speed does not limit the rate at which participants receive data. If the presenter is set to send data to Cisco Unified MeetingPlace Express at Modem speed (70 kbps) and a participant is set to receive data at LAN speed (3,000 kbps), the participant will still receive data up to 3,000 kbps.

**Note**

While the Optimize Room Bandwidth setting does reduce the rate data is sent to users, bursts in the delivery of that data still occur and can congest WAN links. Changing My Connection Speed on the participant's client eliminates bursts and delivers data to the client at a steady rate. The burst issues with the Optimize Room Bandwidth setting will be addressed in future releases.

The client resolution setting also impacts the bandwidth used by limiting the bits per image. A meeting room set at 640x480 pixels will typically generate less than one-third of the traffic compared to a setting of 1280x1024 pixels.

**Design Recommendations Summary**

- Connect both Cisco Unified MeetingPlace Express server interfaces to the LAN with 1 Gbps connections.
- For meetings involving remote users, have the remote users set their My Connection Speed to **DSL**. If congestion issues occur, lower the setting to **Modem**, or lower the screen resolution settings.

## QoS

Quality of Service (QoS) considerations encompass the following topics.

**Traffic Classification or Markings**

Traffic classification or markings from the Cisco Unified MeetingPlace Express server are as follows:

- SIP, H.323, and call control — Not marked
- Voice media (RTP) — Marked EF (DSCP 46)
- Web traffic (HTTP and HTTPS) — Not marked
- Flash web collaboration (RTMP) — Not marked

**Voice and Call Control Traffic**

Voice and call control traffic should be classified with the standard classifications as described in the chapter on [Network Infrastructure, page 3-1](#). If the connection between the Cisco Unified MeetingPlace Express server and the gatekeeper or Cisco Unified CallManager extends over a WAN connection, call control traffic should be re-marked to CS3 (DSCP 24).

**Web Interface Traffic**

No prioritization is recommended for the main web interface. Web traffic to the Cisco Unified MeetingPlace Express server should be treated the same as traffic to other internal web application servers.

**Flash Web Collaboration Traffic**

Because of the large amounts of bandwidth consumed and the bursty nature of this data, as described in the previous section, prioritization of web collaboration traffic across the WAN is difficult. If you attempt to prioritize the web collaboration traffic, classify it separately and lower than other prioritized data.

## Directory Integration

Cisco Unified MeetingPlace Express integrates directly with Cisco Unified CallManager 4.x. For third-party directory integration, a plug-in is required. Cisco Unified MeetingPlace Express supports Microsoft Active Directory, Sun One LDAP, and Netscape/iPlanet LDAP.

Cisco Unified MeetingPlace Express also integrates directly with Cisco Unified CallManager 5.x via Cisco AVVID XML Layer (AXL) Simple Object Access Protocol (SOAP). Third-party directory integration in a Cisco Unified CallManager 5.x environment requires Cisco Unified MeetingPlace Express to point to Cisco Unified CallManager only.

For more information, refer to the *Administrator's Configuration and Maintenance Guide for Cisco MeetingPlace Express*, available at

<http://www.cisco.com>

## H.323 and SIP Direct Integration

Integration with Cisco Unified CallManager can be accomplished by several methods. This section examines two of those methods, H.323 and SIP direct integration, while the third (H.323 via gatekeeper) is examined in the next section.

### H.323 Gateway

The simplest integration option is to define Cisco Unified MeetingPlace Express as an H.323 gateway in Cisco Unified CallManager. You must also configure route patterns in Cisco Unified CallManager that point to the defined gateway. Cisco Unified CallManager 4.1, 4.2, and 5.0, as well as Cisco Unified CallManager Express, all support this option.

## SIP Trunk

Using a SIP trunk to connect to Cisco Unified MeetingPlace Express has some conditions and version dependencies. The following current combinations are supported between Cisco Unified CallManager and Cisco Unified MeetingPlace Express.

### Cisco Unified MeetingPlace Express 1.1.1 and Cisco Unified CallManager 5.x

With this combination, a SIP trunk can be defined directly from Cisco Unified CallManager to Cisco Unified MeetingPlace Express. The following design rules apply to this integration:

- A separate SIP Security Profile must be created and associated with the SIP trunk to Cisco Unified MeetingPlace Express. This security profile must have the transport set to UDP. The default setting is TCP, which will not work with Cisco Unified MeetingPlace Express.
- The SIP trunk configuration must have **MTP Required** checked and must have MTP resources available. MTPs will be invoked for each call to Cisco Unified MeetingPlace Express for the entire duration of the call. This requirement does not apply to Cisco Unified MeetingPlace Express 1.1.2 and higher.

### Cisco Unified MeetingPlace Express 1.1.2 and Cisco Unified CallManager 5.x

With this combination, a SIP trunk can be defined directly from Cisco Unified CallManager to Cisco Unified MeetingPlace Express. The following design rules apply to this integration:

- Cisco Unified CallManager 5.0.4 or higher is required for Cisco Unified MeetingPlace Express 1.1.2. Prior Cisco Unified CallManager 5.0 versions are not supported.
- A separate SIP Security Profile must be created and associated with the SIP trunk to Cisco Unified MeetingPlace Express. This security profile must have the transport set to UDP. The default setting is TCP, which will not work with Cisco Unified MeetingPlace Express.
- The SIP trunk does not require MTPs because Cisco Unified MeetingPlace Express 1.1.2 supports enhanced SIP capabilities. Do not check the MTP Required option on the SIP trunk.
- Ensure that MTPs are available in the associated media resource group list. Some endpoints may cause an MTP to be invoked dynamically when completing a call to Cisco Unified MeetingPlace Express.

### Cisco Unified MeetingPlace Express 1.1.x and Cisco Unified CallManager 4.1 and 4.2

With this combination, a SIP trunk can be defined directly from Cisco Unified CallManager to Cisco Unified MeetingPlace Express. The following design rules apply to this integration:

- Outgoing transport must be set to UDP. The default setting is TCP, which will not work with Cisco Unified MeetingPlace Express.
- The SIP trunk configuration must have **MTP Required** checked and must have MTP resources available. MTPs will be invoked for each call to Cisco Unified MeetingPlace Express for the entire duration of the call. This requirement will not be removed in future releases of Cisco Unified MeetingPlace Express due to the requirements of Cisco Unified CallManager 4.x.

# Gatekeeper Integration

Cisco Unified MeetingPlace Express can be integrated into a gatekeeper environment in accordance with the design considerations presented in this section. Integration as an H.323 gateway or via SIP trunk directly from Cisco Unified CallManager is still an option in a gatekeeper environment. The gatekeeper registration method is as a gateway, using a single E.164 address with the registration. The following design considerations must be taken into account when designing for use in a gatekeeper environment.

## Design Considerations



### Note

Cisco Unified MeetingPlace Express will not register into a specific zone. The default, or first, local zone is always used when multiple local zones exist.

To force Cisco Unified MeetingPlace Express to use a specific local zone, use the **no zone** command on all zones where you do not want Cisco Unified MeetingPlace Express to register. For example, the following commands force Cisco Unified MeetingPlace Express (with address 10.20.110.50) to register to testzone2:

```
gatekeeper
  zone local mp2-gk1 mp2.com 10.20.105.50
  zone local testzone2 mp2.com
  no zone subnet mp2-gk1 10.20.110.50/32 enable
```



### Note

The Cisco Unified MeetingPlace Express direct meeting dial-in feature requires additional gatekeeper configuration.

Cisco Unified MeetingPlace Express registers as a single E.164 address, so extensions for direct meeting dial-in cannot be reached through a gatekeeper without adding manual entries to the gatekeeper by one of the methods shown in the following examples.

#### Option 1: Use Zone Prefix to Route (Recommended)

This example routes extensions 1000 through 1009 to the Cisco Unified MeetingPlace Express server.

```
gatekeeper
  zone local mp2-gk1 mp2.com 10.20.105.50
  zone prefix mp2-gk1 100.
  gw-type-prefix 1#* default-technology gw ipaddr 10.20.110.50 1720
```

#### Option 2: Use Static E.164 Addresses (Not Recommended)

```
gatekeeper
  alias static 10.20.110.50 1720 gkid mp2-gk1 gateway voip ras 10.20.110.50 62675 e164
  1005 e164 1008 e164 1007 e164 1006
```

```
show gatekeeper endpoints
```

CallSignalAddr	Port	RASSignalAddr	Port	Zone Name	Type	Flags
10.20.110.50	1720	10.20.110.50	62675	mp2-gk1	UNKN-GW	S
E164-ID: 1000						
H323-ID: MeetingPlace						

```
E164-ID: 1005 (static)
E164-ID: 1008 (static)
E164-ID: 1007 (static)
E164-ID: 1006 (static)
```

## Redundancy

This section describes the following types of redundancy:

- [Cisco Unified MeetingPlace Express Server Redundancy, page 16-12](#)
- [Physical Network Redundancy, page 16-12](#)
- [Redundancy Using a Gatekeeper, page 16-12](#)
- [Redundancy Using H.323 Gateway Integration, page 16-13](#)
- [Redundancy Using SIP Trunk Integration, page 16-13](#)

## Cisco Unified MeetingPlace Express Server Redundancy

Cisco Unified MeetingPlace Express is a standalone server with no redundancy built in, except for some server components which are themselves redundant. Mirrored drives, dual power supplies, redundant fans, and so forth, give a high level of internal server redundancy and availability. Other methods outside of the server may be incorporated to enhance redundancy characteristics for calls sent from or delivered to Cisco Unified MeetingPlace Express.

Although Cisco Unified MeetingPlace Express is a standalone server, multiple Cisco Unified MeetingPlace Express servers can be deployed using the same Cisco Unified CallManager directory. This configuration enables users to log into an alternate server, via the common directory, and quickly reschedule meetings if the server they were originally using should fail. Two or more fully licensed Cisco Unified MeetingPlace Express servers are needed for this option.

## Physical Network Redundancy

Cisco Unified MeetingPlace Express has two Ethernet ports that are utilized for different purposes, one for call control, web interface, and media, and the other for web collaboration. While traffic rerouting should occur, these ports cannot be relied upon for redundancy. If one port on the server or switch (or the cable between them) fails, the server might not operate properly.

## Redundancy Using a Gatekeeper

### Inbound Calls

The only other redundancy with respect to inbound calls is gatekeeper redundancy, which would apply to outbound calls as well. You can implement gatekeeper redundancy by either of the following methods:

- Alternate gatekeeper

In this method, gatekeepers are set up in a redundant gatekeeper cluster. Cisco Unified MeetingPlace Express registers with its defined gatekeeper. Upon registration, the gatekeeper informs Cisco Unified MeetingPlace Express of an alternate gatekeeper in the cluster for use in the event of a failure.

- Gatekeeper Hot Standby Router Protocol (HSRP)

In this method, two gatekeepers share a single HSRP IP address. In the case of failure, Cisco Unified MeetingPlace Express registers to the secondary gatekeeper using the same gatekeeper IP address.

**Note**

Because the alternate gatekeeper information is delivered during registration and is not permanently stored in Cisco Unified MeetingPlace Express, booting or rebooting of the server when the primary gatekeeper is inaccessible will prevent Cisco Unified MeetingPlace Express from registering with the alternate gatekeeper.

Detailed information about gatekeeper redundancy can be found in the section on [Gatekeeper Redundancy, page 8-18](#).

**Outbound Calls**

Multiple Cisco Unified CallManager servers in a single cluster can register to a gatekeeper for redundancy. The gatekeeper will choose an active Cisco Unified CallManager to complete an outdial from Cisco Unified MeetingPlace Express.

Gatekeeper redundancy as described in the previous section ([Inbound Calls, page 16-12](#)) applies to outbound calls as well.

## Redundancy Using H.323 Gateway Integration

**Inbound Calls**

If you integrate Cisco Unified MeetingPlace Express as an H.323 gateway, inbound calls will be sent from an available Cisco Unified CallManager server within a cluster. If the server fails, inbound calls will automatically be sent from another server in the cluster.

**Outbound Calls**

Cisco Unified MeetingPlace Express allows definition of multiple outbound Cisco Unified CallManagers for outbound call resolution. Should one fail, the next one is used.

## Redundancy Using SIP Trunk Integration

**Inbound Calls**

If you integrate Cisco Unified MeetingPlace Express using a SIP trunk, inbound calls will be sent from an available Cisco Unified CallManager server within a cluster. If the server fails, inbound calls will automatically be sent from another server in the cluster.

**Outbound Calls**

Cisco Unified MeetingPlace Express allows definition of multiple outbound Cisco Unified CallManagers for outbound call resolution via SIP trunk. Should one fail, the next one is used.

# Other Important Design Considerations

This section lists other important design considerations not covered previously in this chapter.

## Network Connectivity

- Cisco Unified MeetingPlace Express uses two network interface cards (NICs) for connectivity. At this time, both NICs must be placed in the same subnet with a common default gateway. Connectivity issues will arise if the NICs are placed in separate subnets.
- Changing the IP addresses of the Cisco Unified MeetingPlace Express server must be done through the **net** command by connecting to the server via SSH and using the **mpxadmin** login. Changing the IP address through other means will not properly change the configuration of Cisco Unified MeetingPlace Express and will cause configuration issues.

## IP Telephony Gateways

- Gateways used with Cisco Unified MeetingPlace Express must be configured with the standard recommendations set forth in the chapter on [Gateways, page 4-1](#).
- The main gateway issue that may impact Cisco Unified MeetingPlace Express is echo cancellation. Cisco recommends increasing the tail allocation on the gateway to 128 ms if echo issues are encountered.