



CHAPTER 15

Cisco Unified MeetingPlace Express

Last revised on: December 15, 2008

Cisco Unified MeetingPlace Express 2.0 is a rich-media appliance for voice, video and web collaboration. This chapter addresses system-level design considerations around integrating Cisco Unified MeetingPlace Express (Unified MPE) into a Cisco Unified Communications environment. For detailed product information, refer to the Cisco Unified MeetingPlace Express product documentation available on

<http://www.cisco.com>

What's New in This Chapter

Table 15-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 15-1 *New or Changed Information Since the Previous Release of This Document*

| New or Revised Topic | Described in: |
|--|--|
| Capacity and sizing information | Capacity and Sizing, page 15-15 |
| Deploying Unified MPE with the Segmented Meeting Access (SMA) option | Segmented Meeting Access Option, page 15-9 |
| Protocol support | Protocol Support, page 15-3 |

Overview

Cisco Unified MeetingPlace Express (Unified MPE) is a voice, video, and web conferencing solution for mid-market to small enterprise customers. The solution implements common industry protocols such as H.323 and Session Initiation Protocol (SIP) to ensure interoperability with various devices in the network. Unified MPE supports both scheduled and reservationless voice, video, and web conferencing. The mixing of voice, video, and web conferencing is provided by software-controlled mixing inherent in the Unified MPE system. This video mixing does not utilize the Cisco Unified Videoconferencing MCU 3500 system and does not integrate to that advanced video solution. The Unified MPE scheduled system supports only basic videoconferencing features and functions such as voice-activated conferencing. If you need advanced videoconferencing features, use a standalone Cisco Unified Videoconferencing MCU 3500 or Cisco Unified MeetingPlace system.

Unified MPE Video Telephony (Unified MPE VT) is based on the same technology as Unified MPE but is a separate product and is sold as an ad-hoc system only. Unified MPE VT is deployed as a videoconferencing media resource that registers with Cisco Unified Communications Manager to provide ad-hoc videoconferencing capability. It does not support scheduled or reservationless meetings and is not deployed in conjunction with Unified MPE. On a single Cisco Media Convergence Server, either Unified MPE or Unified MPE VT can be installed, but not both.

**Note**

Although they are based on similar technologies, Unified MPE and Unified MPE VT have some differences in design criteria. For example, the G.729 audio codec is supported on Unified MPE but not on Unified MPE VT (in which case, Unified CM would have to provide a transcoder). For more information on Unified MPE VT, refer to the Unified MPE VT data sheets available at http://www.cisco.com/en/US/products/ps6533/products_data_sheets_list.html.

Conferencing Support

Unified MPE has different levels of conferencing support when it integrates with the following call processing agents.

- Unified MPE supports scheduled and reservationless voice, video, and web conferencing with Unified CM 4.1 and later.
- Unified MPE supports scheduled and reservationless voice and web conferencing with Cisco Unified Communications Manager Express (Unified CME).
- Unified MPE supports scheduled and reservationless voice and web conferencing with Survivable Remote Site Telephony (SRST).

Video Support

Any H.323, SIP, or Unified CM SCCP endpoint that joins a video conference provided by Unified MPE must be capable of mid-call video escalation. Any industry-standard video endpoints following either the ITU-T H.323 specification or SIP RFC-3261 are able to participate in a video session on Unified MPE, as are all of the supported SCCP third-party endpoints from Sony, Tandberg, or Polycom available on various releases of Unified CM. The H.323 industry endpoints may be registered to either a Cisco IOS Gatekeeper or Unified CM, which must provide call routing to the Unified MPE system for the Unified MPE dial-in numbers.

The following video attributes must be supported by the video endpoint participating in Unified MPE video sessions:

- H.263 or H.264 video codecs with Common Intermediate Format (CIF)
- G.711 or G.729a audio codecs
- Mid-call video escalation (Endpoints first dial into Unified MPE, then enter the meeting ID. If video ports are scheduled, video will be activated.)
- RFC-2833, SIP KPML, or H.323 out-of-band DTMF support

- Unified MPE supports H.263 and H.264 video codecs, but it cannot transcode the video stream from one codec type to another. The system administrator must specify the exact video codec setting for each video meeting type, and the person scheduling the meeting must choose the meeting type from a permitted list. Unified MPE Profiles users are given one of three levels that control the user experience:
 1. Users can attend video meetings, host video meetings, and reserve video ports.
 2. Users can attend video meeting and host video meetings if video ports are available (not scheduled for another meeting).
 3. Users can attend video meetings.

Video participants can join a meeting with a bit rate from 64 kbps to 768 kbps. No participant is allowed to join the conference at a bit rate higher than the maximum configured bit rate. If a participant joins the conference at a bit rate lower than the maximum bit rate, the additional capacity will remain in the overall system capacity pool and will be utilized for other participants. Unified MPE cannot transrate among various call speeds; therefore the established video session will use the lowest call speed for all participants per meeting.

Unified MPE uses voice activation mode for the video conference, automatically selecting the dominant speaker by determining which conference participant is speaking the loudest and the longest. The video stream of the active speaker is sent to all endpoints in the conference, and the video stream of the previous speaker is sent to the current active speaker. As conditions change throughout the conference, Unified MPE automatically selects a new dominant speaker and switches the video to display that participant. The active speaker (one image, or 1x1 layout) uses Common Intermediate Format (CIF) dimensions only.

Protocol Support

Table 15-2 lists the standard protocols and transport layer ports used by Unified MPE in a Cisco Unified Communications environment.

Table 15-2 Protocols Supported by Unified MPE

| Protocol | Transport | Port(s) | Usage |
|----------------|-----------|----------------|--|
| SSH | TCP | 22 | Secure Access; Voice conferencing events |
| RTMP | TCP | 1935 | Web Conferencing (optional) |
| HTTP, HTTPS | TCP | 80, 443 | Web Admin; Web Conferencing; Cisco Unified Personal Communicator; Microsoft Outlook ¹ ; AXL/SOAP over HTTPS to Unified CM (directory integration) |
| SIP | UDP | 5060 | SIP |
| H.225 | TCP | 1720 | H.323 to Unified CM or gatekeeper |
| H.245 | TCP | 62000 to 62999 | H.323 to Unified CM or gatekeeper |
| RTP | UDP | 16384 to 32767 | Voice packets |
| RTP | UDP | 20480 to 24576 | Video packets |
| NTP | UDP | 123 | Network Time Protocol ² |
| SMTP | TCP | 25 | Email notifications (outbound to server) |
| SNMP | UDP | 161 | SNMP |

1. Microsoft Outlook is integrated using a plug-in that communicates with the Unified MPE server using HTTP or HTTPS.

2. Unified MPE must be associated with the appropriate NTP server so that Unified MPE can schedule meetings and send out meeting notifications with the correct time.

DTMF Support

Unified MPE supports the following standard dual-tone multifrequency (DTMF) transmission methods:

- H.245 Alphanumeric and H.245 Signal DTMF transmissions when using H.323
- RFC2833 and KPML DTMF transmissions when using SIP

For detailed information of DTMF transmission, see the chapter on [Media Resources, page 6-1](#).

Deployment Models

This section describes design recommendations for integrating Unified MPE with the following Cisco Unified Communications deployment models:

- [Single Site, page 15-4](#)
- [Multisite WAN with Centralized Call Processing, page 15-6](#)
- [Multisite WAN with Distributed Call Processing, page 15-7](#)
- [Clustering Over the WAN, page 15-8](#)

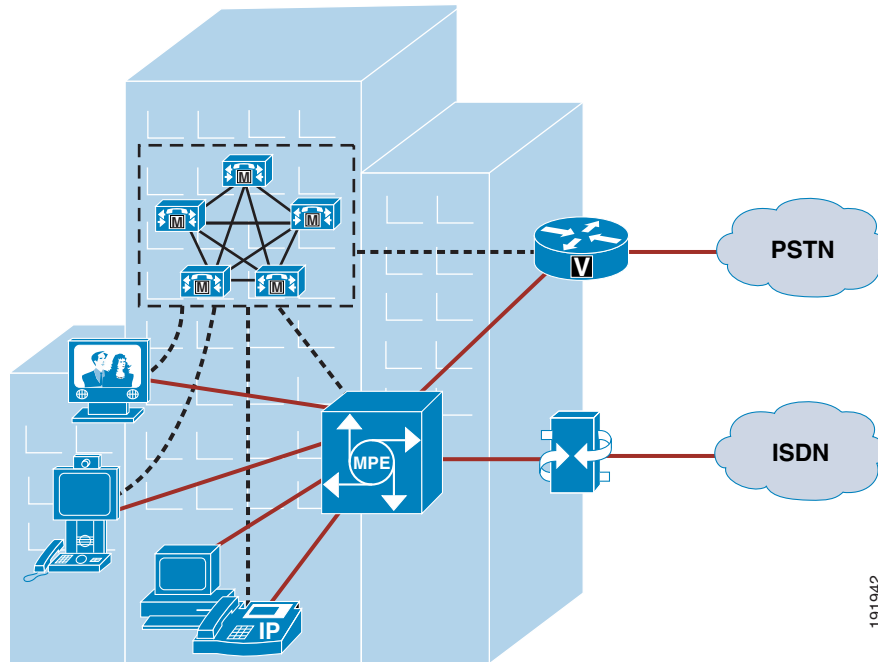
In addition to these deployment models, this section covers deployments involving a demilitarized zone (DMZ). Deployments involving a DMZ are implemented using Segmented Meeting Access (SMA). Each of the deployment models listed above supports the SMA option (see [Segmented Meeting Access Option, page 15-9](#)). For detailed information on design rules for the various deployment models, see the chapter on [Unified Communications Deployment Models, page 2-1](#).

Single Site

In a single-site deployment, all call processing is local and all participants are local as well. In this model, Unified MPE connects to Unified CM through an H.323 or SIP connection (see [Figure 15-1](#)). In the single-site deployment, use of the G.711 codec is recommended because bandwidth is usually not as much of a concern as it would be in multisite deployments. H.323 video endpoints may be registered to either a Cisco IOS Gatekeeper or Unified CM, either of which will provide call routing to the

Unified MPE system for the Unified MPE dial-in numbers. Cisco Unified Videoconferencing 3500 Series Gateways can be deployed to allow external H.320 video clients (which support H.245 Alphanumeric or H.245 Signal for DTMF transmission) to participate in video conferences.

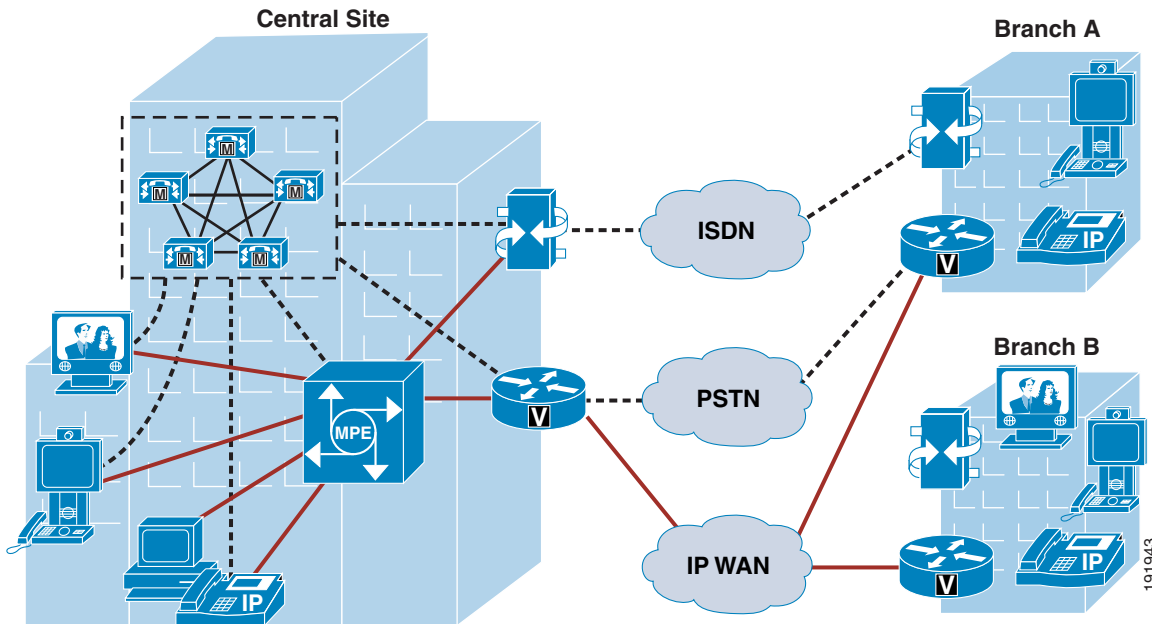
Figure 15-1 *Single-Site Deployment*



Multisite WAN with Centralized Call Processing

In a multisite WAN deployment with centralized call processing, the Unified MPE server is usually located in the central site, where all call processing occurs. (See [Figure 15-2](#).)

Figure 15-2 Multisite WAN Deployment with Centralized Call Processing



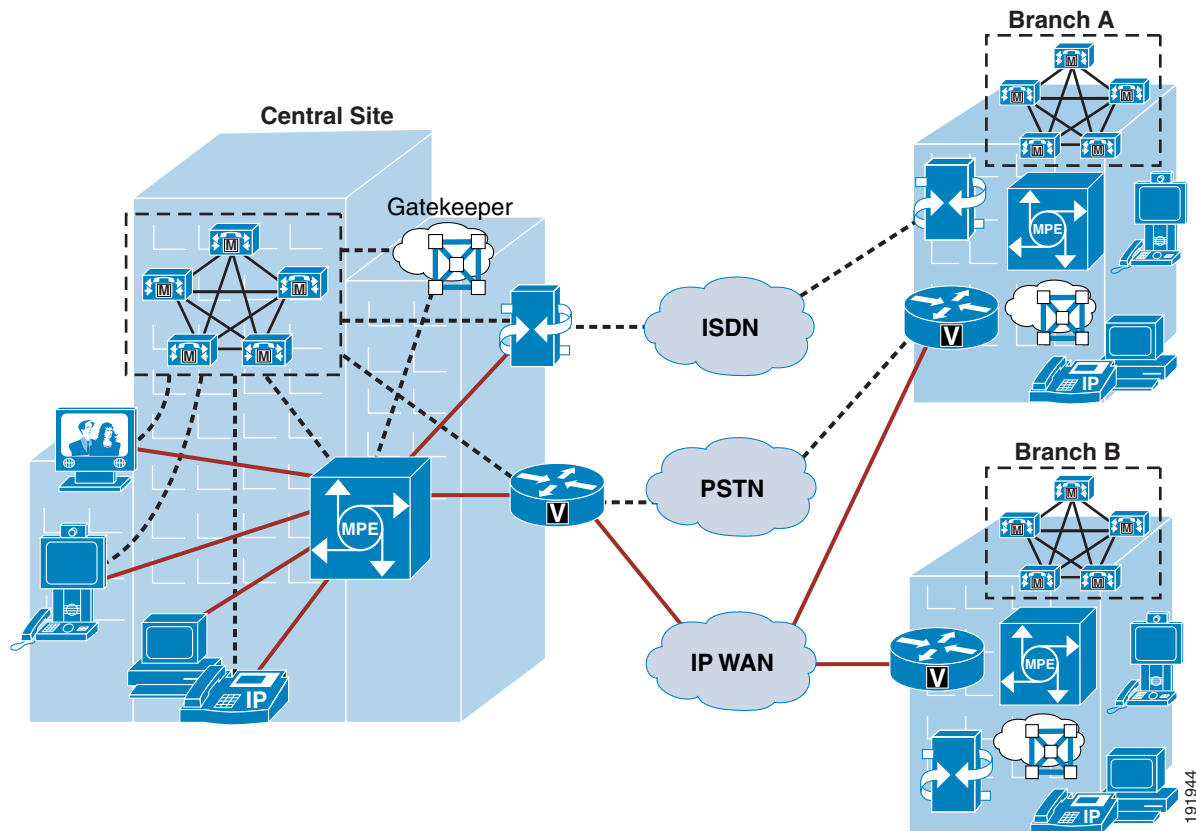
Compared to local participants, remote participants usually require the following additional considerations:

- In addition to G.711 mu-law and a-law codec support, Unified MPE also supports G.729a natively for optimal bandwidth usage across the IP WAN.
- Native G.729a codec support requires numerous Unified MPE system resources. A single G.729a audio call costs 5 SRUs from the overall system capacity pool. Deploying an external transcoding resource to transcode the voice stream from G.729a or other non-G.711 codec to G.711 codec would allow greater scalability with Unified MPE. Video conferencing is not compatible with an external transcoding resource; therefore, an external transcoding resource should be used with voice conferencing only.
- Web collaboration requires significant bandwidth that must be provisioned. (See [Bandwidth Considerations for Web Applications and Screen Sharing](#), page 15-10.)
- During normal operation, all voice, video, and web traffic from remote offices is sent across the IP WAN and terminates at Unified MPE in the central site. During Unified CM fallback mode, in order to join the conference, the remote endpoint sends its voice traffic to the central-site Unified MPE across the PSTN. Video conferencing is not supported to endpoints operating in Unified CM fallback mode.
- The same QoS and call admission control mechanisms used for the existing Cisco Unified Communications deployment are required. For purposes of call admission control, Unified MPE should be treated as a telephony gateway in the central site.

Multisite WAN with Distributed Call Processing

In a multisite WAN deployment with distributed call processing, Unified MPE is usually located in a site local to Unified CM. [Figure 15-3](#) depicts an example of a multisite WAN deployment with distributed call processing.

Figure 15-3 Multisite WAN Deployment with Distributed Call Processing



Each site in the distributed call processing model can be one of the following:

- A single site with its own call processing agent
- A centralized call processing site and all of its associated remote sites
- A legacy PBX with Voice over IP (VoIP) gateway

All the design considerations that have been discussed in the previous two call processing models are also applicable to the multisite WAN deployment with distributed call processing.

Unified MPE is a single server with no cascading, mirroring, or redundancy capabilities, so a single active server at a single site would be typical. There is no communication between different Unified MPE servers, such as the Unified MPE server in central site and the one at branch A in [Figure 15-3](#).

The call processing agent at a branch site (for example, branch B in [Figure 15-3](#)) can directly route calls to the central-site Unified MPE. This can be done by defining an H.323 gateway or SIP trunk on the branch call processing agent, which points to the central-site Unified MPE. Having multiple call processing agents pointing to the same Unified MPE is not a recommended practice. In order for

branch B Unified CM to route calls to the central-site Unified MPE, Cisco recommends routing calls to the central-site Unified CM first, which then directs the calls to its local Unified MPE. Call admission control is performed by the central-site call processing agent or the gatekeeper that is responsible for the intercluster call processing.

Clustering Over the WAN

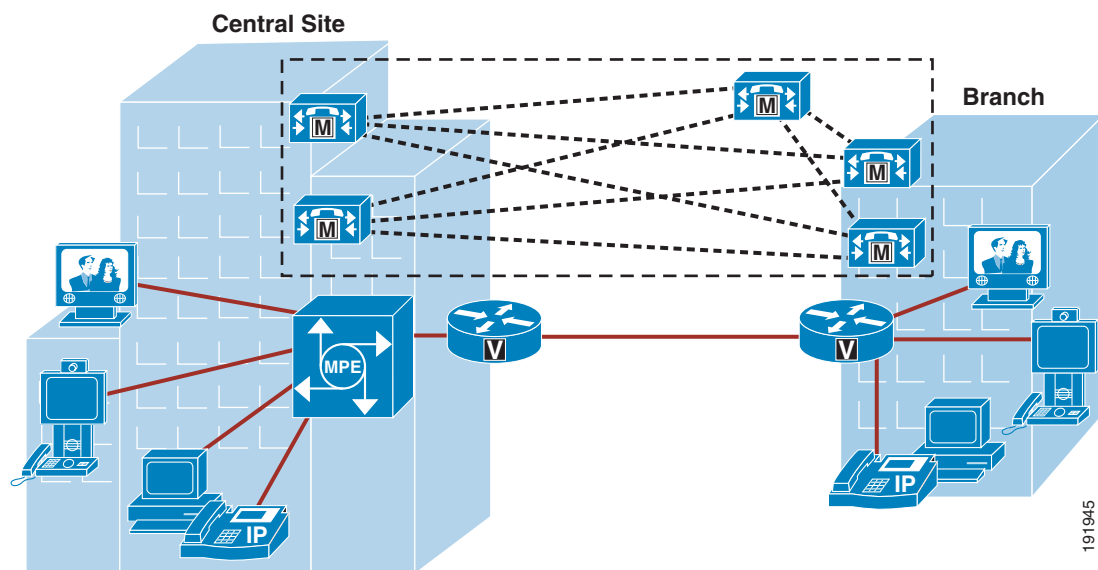
In a deployment with clustering over the WAN, the Unified CM cluster is split across one or more locations separated by high-capacity and high-speed WAN or MAN links. (See [Figure 15-4.](#)) In this call processing model, the maximum one-way delay for all priority Intra-Cluster Communication Signaling (ICCS) traffic between any two Unified CM servers must not exceed 40 ms total round-trip time (RTT) with Unified CM 6.0 or 80 ms RTT with Unified CM 6.1 and later releases.



Note

In addition to RTT requirements, clustering over the WAN also has strict bandwidth requirements. See [Clustering Over the IP WAN, page 2-21](#), for more details.

Figure 15-4 Clustering Over the WAN



Unified MPE does not have any server-to-server redundancy and cannot fully utilize the high-availability nature of this call processing model.

Placement and design considerations for Unified MPE in this model are identical to the previous deployment model, [Multisite WAN with Distributed Call Processing, page 15-7](#).

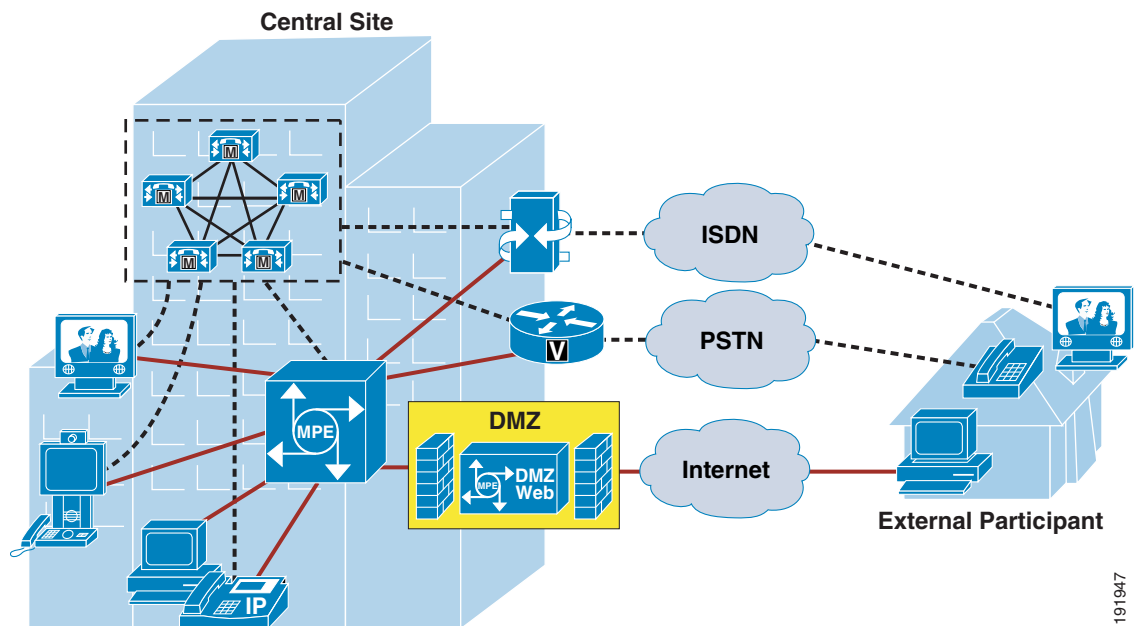
To have a multisite redundant and distributed collaboration system, consider Cisco Unified MeetingPlace as an option. See the chapter on [Cisco Unified MeetingPlace, page 14-1](#), for more information.

Segmented Meeting Access Option

Deploying Unified MPE in a demilitarized zone (DMZ) enables external users (users external to the private network) to participate in Unified MPE meetings. It allows external users to join meetings across the Internet while still keeping voice, video, and privately listed meetings internal to the private network. This is referred to as Segmented Meeting Access (SMA). This deployment option allows for separation between private and public web meetings and allows for the most secure voice, video, and web conferencing deployment. This approach is highly recommended for most customer scenarios and may be applied to any of the deployment models discussed previously in this chapter.

An SMA design involves dual servers, with one Unified MPE server located on the internal network and placement of a Unified MPE Web server within the DMZ for publicly listed meetings. Figure 15-5 shows typical SMA deployment.

Figure 15-5 Dual-Server DMZ Deployment



All private meetings (voice, video, and web) are hosted on the internal Unified MPE server, which is on the internal network but not located within the DMZ. Internal participants can schedule both private and public meetings, and external participants can only attend the public meetings. For a public meeting, internal participants send their web and voice streams to the internal Unified MPE server, while external participants send their web traffic across the Internet to the Unified MPE Web server inside the DMZ. External users' voice streams connect to the internal Unified MPE server through the voice gateway on the internal network. For public web collaboration, the meetings are actually hosted on two Unified MPE web instances, one running on the internal Unified MPE server that is on the internal network and the other running on the Unified MPE Web server in the DMZ.

The web component on the Unified MPE DMZ Web server shares web conferencing information with the integrated web component of the internal Unified MPE server via the Real Time Messaging Protocol (RTMP) over TCP port 1935. If a connection cannot be established on TCP port 1935, a connection will be attempted on TCP port 443 (HTTPS). If a connection cannot be established via HTTPS, a connection will be attempted on TCP port 80, thereby tunneling RTMP inside of HTTP. The internal Unified MPE server also sends voice conferencing events to the external Unified MPE web server via SSH protocol.

(TCP port 22). Both the web (TCP 1935, 443, or 80) and voice (TCP 22) ports must be open on the internal corporate firewall to allow communications between the two servers. Note that Web user licenses (ULs) are shared between the internal Unified MPE server and the Unified MPE DMZ Web server.

The following ports must be open on the internal corporate firewall so that the firewall will not block communications between the internal Unified MPE server and the Unified MPE DMZ Web server:

- One of the following for web conferencing: TCP port 1935, 80, or 443.
- Secure Shell (SSH) access over TCP port 22 to the server from the internal network is needed for voice conferencing events to be relayed. In addition, Cisco Technical Assistance Center (TAC) might require SSH access to support Unified MPE properly.

There is another variation of this SMA deployment option with the dual-server approach, which can increase system scalability. You can designate the second Unified MPE DMZ Web server to HOST ALL WEB MEETINGS. It is possible to deploy Unified MPE in this manner without the DMZ requirement. This second web-only server can be deployed either internally (on the internal network but not within the DMZ) for private web meetings or inside the DMZ to allow external participants to join public web meetings. The internal Unified MPE server can then allocate all of its system resources to voice and video meetings. With this type of deployment, the internal Unified MPE server serves only voice and video meeting requests, allowing it to provide more capacity for G.729a codec conferences and high-bandwidth video conferencing capacity. With such a setup, internal participants always send their web traffic to the secondary web server for all web meetings, whether public or private. This deployment option should be used only in certain high-capacity scenarios based on customer usage, and it is not recommended for typical customer deployments. For a comprehensive list of MCS models and related capacities, refer to the Unified MPE 2.0 data sheet, available at:

http://www.cisco.com/en/US/products/ps6533/products_data_sheets_list.html

Call Admission Control, Bandwidth, and QoS

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

Call Admission Control

Unified MPE should be treated as a telephony gateway for purposes of call admission control. Unified CM can perform both static-location and RSVP-enabled location call admission control for the voice and video conferences that are hosted on Unified MPE. 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, depending on what a user is sharing. Many colors, content with pictures, and so forth, can cause very large bandwidth requirements. If media imaging, pictures, or high-resolution graphics are shared, that will require higher capacity network bandwidth. 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 to the two switch ports.

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 1.5 Mbps occur in the data from the remote server to each user, 15 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 28 kbps
- **DSL** — Bandwidth limited to 250 kbps
- **LAN** — Bandwidth up to 1,500 kbps

Bandwidth bursts above 1,500 kbps are possible if high-resolution images or photos are shared. Sharing normal to complex presentations or documents should not generate bursts above 1,500 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 at which data is delivered to an individual user from Unified MPE.
 - Limits the speed at which data is sent from the presenter to Unified MPE.
 - Presenter speed does not limit the rate at which participants receive data.
- Optimize Room Bandwidth
 - Limits the rate at which 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 Unified MPE at Modem speed (28 kbps) and a participant is set to receive data at LAN speed (1,500 kbps), then the participant will still receive data up to 1,500 kbps.

**Note**

While the Optimize Room Bandwidth setting does reduce the rate at which 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 Unified MPE 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) must be implemented in the network to minimize quality impairments such as packet loss, delay, and delay variation, so that participants have a good user experience during the meeting. Unified MPE uses the Differentiated Services Code Point (DSCP) mechanism for its traffic marking and classification.

Traffic from Unified MPE is classified or marked as follows:

- SIP, H.323, and call control — Not marked
- Voice media (RTP) — Marked EF (can be modified in Unified MPE)
- Video media (RTP) — Marked AF41 (can be modified in Unified MPE)
- 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 Unified MPE and the call processing agent 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 Unified MPE 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 not recommended. If you attempt to prioritize the web collaboration traffic, classify it separately and lower than other prioritized data.

External Directory Integration via Unified CM

Integrating an external directory with Unified MPE through Unified CM provides two main functions:

- Automatic profile creation in Unified MPE
- External authentication using a third-party directory

When Unified MPE is integrated with Unified CM (which is integrated with an external LDAP directory), user profiles are created automatically the first time users log into Unified MPE. The profiles enable users to schedule meetings immediately and use the system.

To log into Unified MPE, the user must have a profile with the correct UserID and password configured natively in Unified MPE or the user must be authenticated against the external corporate directory with which Unified CM is integrated.

Cisco Unified CM releases 3.3 and higher as well as 4.x require the application of the Unified CM LDAP plugin for proper integration with an external LDAP directory, but Unified CM 5.x, 6.x, and 7.x do not require any schema changes to the external LDAP system. Unified MPE supports only the same external LDAP systems and versions as Unified CM supports. Unified MPE integrates with Unified CM 5.x, 6.x, and 7.x via Cisco AVVID XML Layer (AXL) Simple Object Access Protocol (SOAP). Unified MPE does not support direct LDAP integration to an external corporate directory.

**Note**

LDAP integration is not supported with Cisco Unified Communications Manager Express (Unified CME), voice gateways, or SIP systems.

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 Integration with Unified CM

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

The Unified MPE system contains embedded IP gateway software that integrates to standards-based H.323 and/or SIP systems, however Unified CM is more frequently deployed as the integration point for these systems. Integration with Unified CM allows Unified CM to perform dial plan resolution, toll-fraud control, and call admission control for conferences hosted by Unified MPE. Any call control system can send inbound calls into Unified MPE without any configuration necessary on the Unified MPE system. (No blocking is done inbound by Unified MPE until all the Voice User Licenses are in use, then busy tone would be returned to the caller.) Only "outdial" configuration on Unified MPE is required for sending any outdial requests to either the H.323 or SIP gateway (but not both). The outdial calls must be resolved by the call processing system for providing toll fraud control, routing, and so forth, because Unified MPE has no facilities to perform any of those functions.

Customers can publish up to four different numbers to dial into a Unified MPE voice and video system. These numbers are automatically available on the notification templates and consist of the following types:

- Toll Free (for example, 800-XXX-XXXX)
- DID or Direct CO (for example, 408-XXX-XXXX) for international)
- Local 3-, 4-, or 5-digit internal number (for example, 4000)
- Private Network Dial Plan (for example, 774-4000)

H.323 Gateway

The simplest integration option is to define Unified MPE as an H.323 gateway in Unified CM. This also requires the administrator to configure one or more route patterns in Unified CM that use the defined H.323 gateway for routing calls to the Unified MPE system.

SIP Trunk

To integrate Unified MPE with Unified CM via a SIP connection, you can configure a SIP trunk directly from Unified CM to Unified MPE. The following design rules apply to this type of integration:

- A separate SIP Security Profile must be created and associated with the SIP trunk to Unified MPE. This security profile must have the transport set to UDP. The default setting is TCP, which will not work with Unified MPE.
- The SIP trunk does not require MTPs because Unified MPE supports both SIP early-offer and delay-offer mechanisms. 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 can cause an MTP to be invoked dynamically when completing a call to Unified MPE.



Note

Cisco recommends using SIP trunk integration with Unified CM when Cisco Unified Personal Communicator is used for any video sessions.

Gatekeeper Integration

Unified MPE can be integrated into a gatekeeper environment in accordance with the design considerations presented in this section. The gatekeeper registration method is as a gateway, using a single E.164 address with the registration. Unified MPE will always initiate a video conference as an audio-only session and then escalate to the video conference after the system locates a video-capable endpoint. Unified MPE will send a Bandwidth Request (BRQ) message to the gatekeeper to confirm the requested bandwidth before it starts media capability exchange with the video endpoint. If there is not enough bandwidth for the video escalation, the connection will stay as an audio-only session.

The design considerations in this section must be taken into account when designing a Unified MPE system for use in a gatekeeper environment.

Design Considerations



Note

Unified MPE will not register into a specific zone. The default (or first) local zone is always used when multiple local zones exist.

To force Unified MPE to use a specific local zone, use the **no zone** command on all zones where you do not want Unified MPE to register. For example, the following commands force Unified MPE (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 Unified MPE direct meeting dial-in feature requires additional gatekeeper configuration.

Unified MPE registers as an H.323 gateway with 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 Unified MPE.

```
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) | | | | | | |

Capacity and Sizing

On a single Cisco Media Convergence Server (MCS) 7845 H2, Unified MPE can support up to 200 concurrent users of voice conferencing using the G.711 codec, 150 concurrent users of videoconferencing (up to 384 kbps, and each video endpoint uses one voice port and one video port per meeting), and 200 concurrent users of web conferencing. If the Segmented Meeting Access option is deployed in a manner so that all web conferencing is hosted on a second MCS 7845 H2, the maximum capacity increases to 200 concurrent audio, 200 concurrent video, and 200 concurrent web conferencing users. See the section on [Segmented Meeting Access Option, page 15-9](#), for more information on the Segmented Meeting Access deployment option.

**Note**

Deploying earlier server models will result in diminished capacity. Refer to the Unified MPE 2.0 data sheet (available at http://www.cisco.com/en/US/products/ps6533/products_data_sheets_list.html) for a comprehensive list of MCS models and related capacities.

System Resource Unit (SRU)

Use of the G.729a codec and high-bandwidth videoconferencing (above 384 kbps) will affect overall system capacity. Estimating the overall system capacity for Unified MPE involves the concept of a system resource unit (SRU). The number of SRUs available to a system is based on the type of media convergence server (MCS) deployed and is reported on the Meeting Configuration page in the Web Administration Center, given a particular codec and video configuration. Each voice, video, or web SRU required for a user session consumes a corresponding voice, video, or web user license (UL) in the system.

A video session with a bit rate of 384 kbps or less requires one SRU. Two SRUs are required for any video session greater than 384 kbps and up to 768 kbps. A voice session with a G.711 codec requires one SRU, and a voice session with a G.729a codec requires five audio SRUs. Web conferencing requires two SRUs per user session.

When a participant joins a video conference with a video bit rate of 384 kbps (or less) using the G.711 codec, Unified MPE allocates two SRUs, one video user license (UL), and one audio UL for this participant. If this same video endpoint joins with a G.729a codec, then six SRUs are allocated for the voice and video portion of the call.

Unified MPE does not take the flow-controlled bit rate into account for its system capacity calculation. For example, if a 384 kbps participant joins a conference with a video-session bit rate of 768 kbps, that participant lowers the session bit rate to 384 kbps, but Unified MPE still holds two video ULs for the existing session.



Note

The Solution Expert Tool can assist in determining the correct MCS model size based on your design criteria. This tool is available (with appropriate login authentication) at <http://www.cisco.com/go/sx>.

Redundancy

This section describes the following types of redundancy:

- [Unified MPE Server Redundancy, page 15-16](#)
- [Redundancy Using a Gatekeeper, page 15-17](#)
- [Redundancy Using H.323 Gateway Integration, page 15-17](#)
- [Redundancy Using SIP Trunk Integration, page 15-18](#)

Unified MPE Server Redundancy

Unified MPE 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. Unified MPE has two Ethernet ports, but they are used for different purposes: one for call control, web scheduling, administration interfaces, and media; and the other for web collaboration.

Cascaded conferencing between separate Unified MPE servers is not available. With the Segmented Meeting Access (SMA) option, both the Unified MPE server and the Unified MPE DMZ Web server share one internal database. Although Unified MPE is a standalone server, multiple Unified MPE servers

can be deployed using the same Unified CM 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 Unified MPE servers are needed for this option.

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. Unified MPE registers with its defined gatekeeper. Upon registration, the gatekeeper informs Unified MPE 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, Unified MPE 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 Unified MPE, booting or rebooting of the server when the primary gatekeeper is inaccessible will prevent Unified MPE from registering with the alternate gatekeeper.

Detailed information about gatekeeper redundancy can be found in the section on [Gatekeeper Redundancy, page 8-27](#).

Outbound Calls

Multiple Unified CM servers in a single cluster can register to a gatekeeper for redundancy. The gatekeeper will choose an active Unified CM to complete an outdial from Unified MPE.

Gatekeeper redundancy as described in the previous section ([Inbound Calls, page 15-17](#)) applies to outbound calls as well.

Redundancy Using H.323 Gateway Integration

Inbound Calls

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

Outbound Calls

Unified MPE allows for definition of multiple H.323 outdial connections that point to Unified CM, Unified CME, and other H.323-compliant call processing agents. Unified MPE keeps sending outbound calls to the first H.323-compliant call processing agent in the list until an outdial call failure occurs. Then Unified MPE automatically sends an H.225 setup message to the next available call processing agent in the list. Failure of the call processing agent does not affect existing calls. The existing media connection is torn down after the user disconnects.

Redundancy Using SIP Trunk Integration

Inbound Calls

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

Outbound Calls

Unified MPE allows for definition of multiple SIP outdial connections that point to Unified CM, Unified CME, and other SIP-compliant call processing agents. Unified MPE keeps sending outbound calls to the first SIP-compliant call processing agent in the list until an outdial call failure occurs. Then Unified MPE automatically sends a SIP Invite message to the next available call processing agent in the list. Failure of the call processing agent does not affect existing calls. The existing media connection is torn down after the user disconnects.



Note

Unified MPE cannot have outdialing capability via both H.323 and SIP connections at the same time. H.323 and SIP outdialing capabilities are mutually exclusive in Unified MPE.

Other Important Design Considerations

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

Network Connectivity

- Unified MPE 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 Unified MPE 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 Unified MPE and will cause configuration issues. Changing the host names and domain name of a system requires application of a patch that is available through Cisco Technical Assistance Center (TAC).

IP Telephony Gateways

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