



## Cisco Unified MeetingPlace Integration

---

This chapter covers system-level design and implementation of Cisco Unified MeetingPlace 5.4 in a Cisco Unified Communications Manager 5.x environment. The following aspects of design and configuration of Cisco Unified MeetingPlace not related to system design with Cisco Unified Communications Manager (Unified CM) are *not* covered in this chapter:

- Hardware requirements
- Software component configuration
- Sizing of voice, web, and video resources
- Audio, web, and video conferencing detailed explanations and configuration outside of system-level design
- Much of the TDM capabilities of Cisco Unified MeetingPlace 5.4

For information on these topics, refer to the Cisco Unified MeetingPlace product documentation available at

[http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd_products_support_series_home.html)

Cisco Unified MeetingPlace 5.4 introduces new and enhanced video capabilities, including:

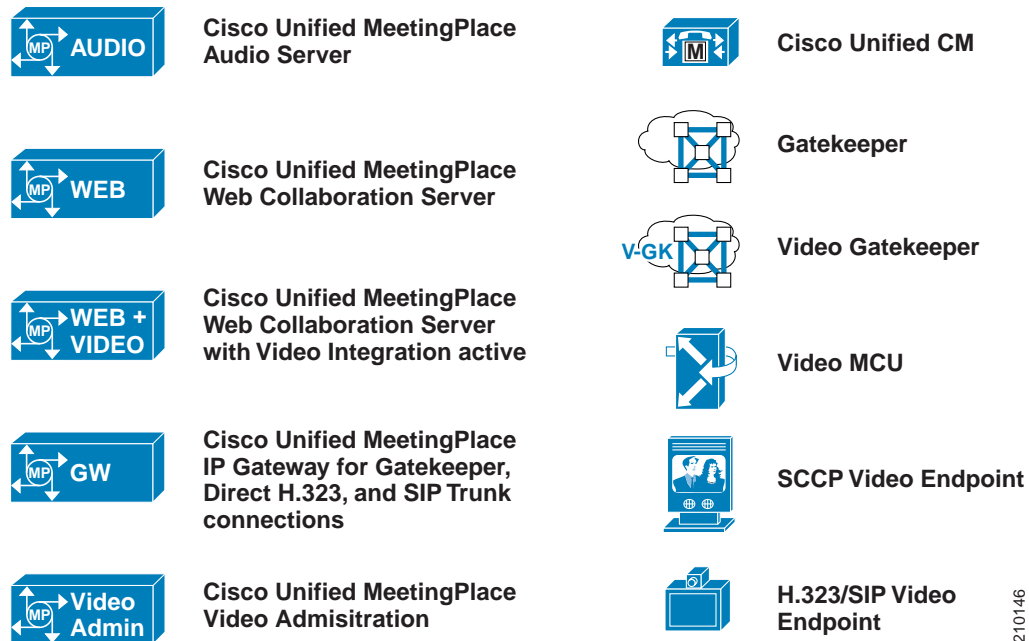
- Video scheduling integrated into meeting scheduling, allowing reservation of video ports and terminals
- Ability to cascade MCU resources, allowing larger video meetings
- Ability to see and control individual video speaker status on participant list

Cisco Unified MeetingPlace Video in many ways acts as a separate entity with full integration into Cisco Unified MeetingPlace 5.4. The first sections of this chapter cover Cisco Unified MeetingPlace implemented as a base deployment with Audio and Web Collaboration. The final section covers the details of adding video to Cisco Unified MeetingPlace 5.4 base deployments. All guidance given in the first sections also applies to deployments with video.

# Cisco Unified MeetingPlace Components

Figure 14-1 lists the components of a Cisco Unified MeetingPlace deployment. The icons and symbols in Figure 14-1 are used in diagrams throughout this chapter.

Figure 14-1 Cisco Unified MeetingPlace Components



210146

All components on the left (containing the MP symbol) are specific to Cisco Unified MeetingPlace, but this is not an all-inclusive list. There are other Cisco Unified MeetingPlace components not shown in the diagrams in this chapter. All Cisco Unified MeetingPlace components, with the exception of the Audio Server, are software components that run on Microsoft Windows 2000 or 2003 servers. The Audio Server is a hardware component using a specialized OS. Specifics on server and OS requirements are listed in the product documentation available at

[http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd_products_support_series_home.html)

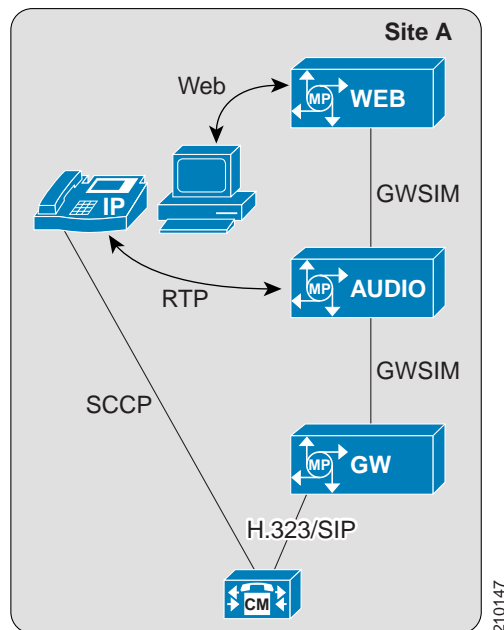
# Deployment Models

This section discusses design considerations and recommendations for adding Cisco Unified MeetingPlace to each of the basic Cisco Unified Communications Manager (Unified CM) deployment models. Many variations are possible in the deployments, but the models presented here cover the base deployments without examining every variation.

## Single Site

The single-site deployment is the base deployment, with all server components and users located at a single site interconnected by a single LAN (see [Figure 14-2](#)). In this model, Cisco Unified MeetingPlace is co-located with the Unified CM cluster and integrated via H.323 or SIP, as described in sections on [H.323 and SIP Direct Integration, page 14-10](#), and [Gatekeeper Integration, page 14-11](#).

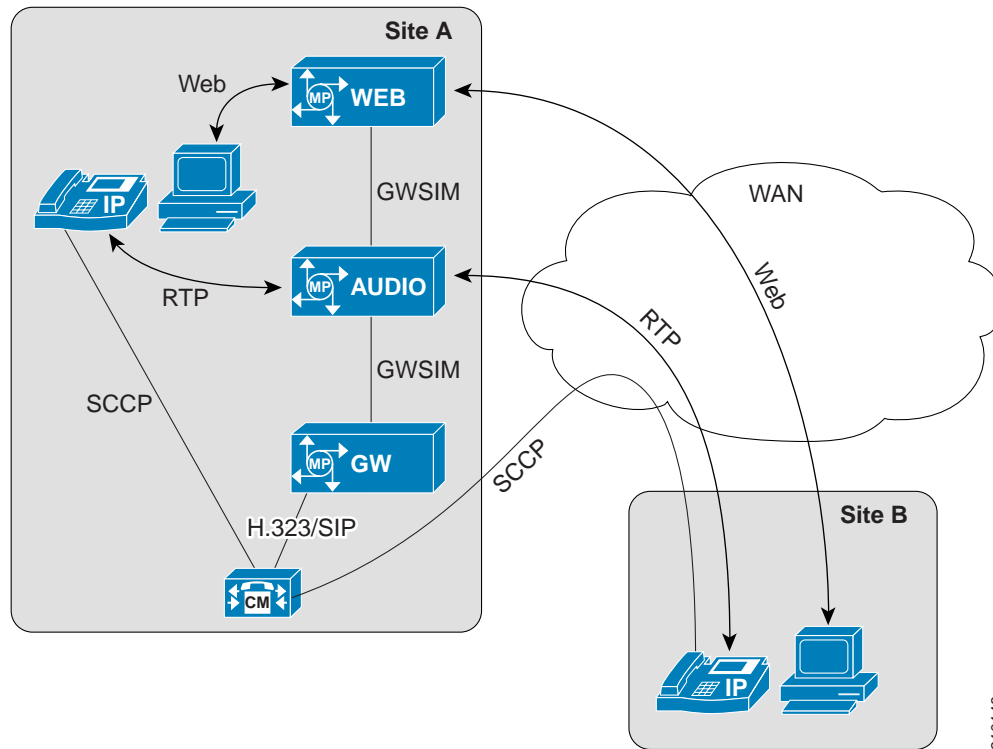
*Figure 14-2 Single Site*



## Multisite WAN with Centralized Call Processing

The multisite WAN deployment with centralized call processing builds upon the single-site model by incorporating remote sites (see [Figure 14-3](#)). All Cisco Unified MeetingPlace components are assumed to be centrally located for this model, although distribution of some components is an option. Distributed components are covered in the next model in conjunction with distributed call processing.

**Figure 14-3** Multisite Deployment with Centralized Call Processing



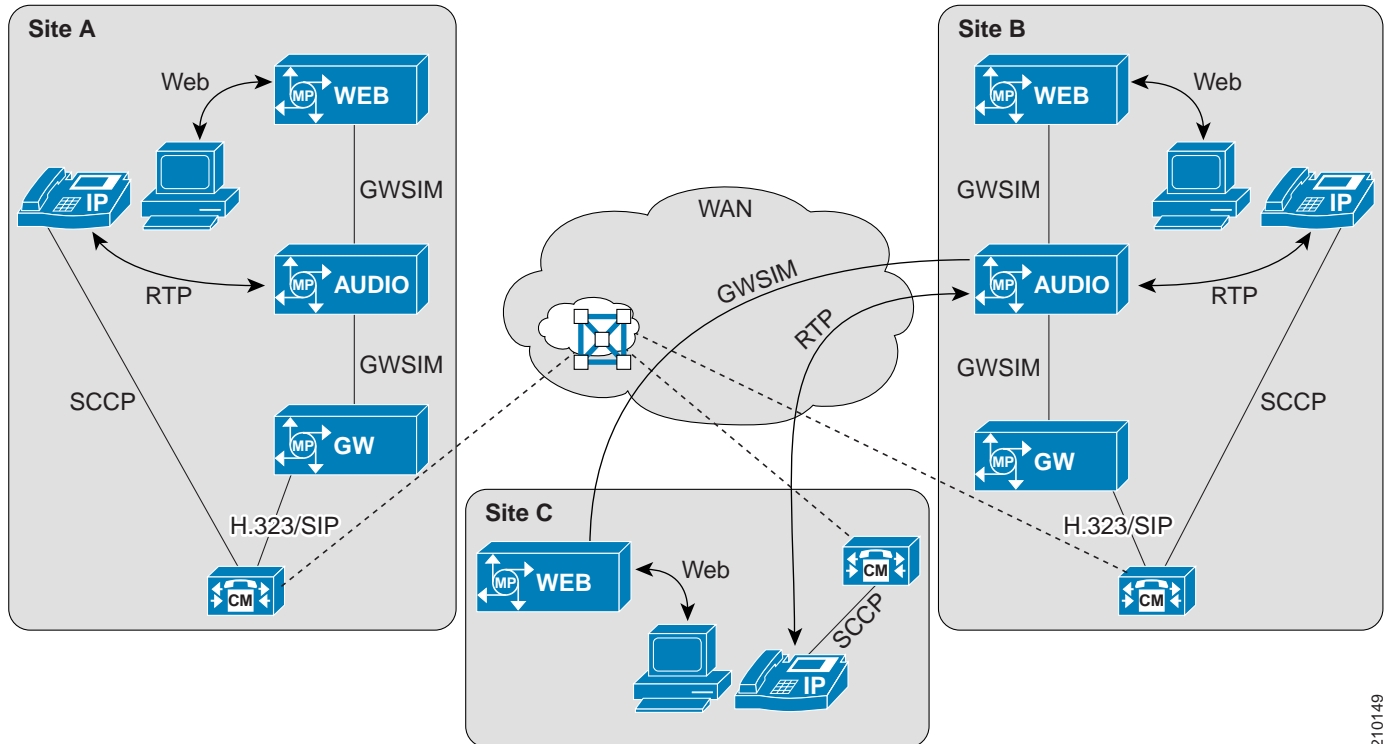
The addition of remote sites, with users separated from Cisco Unified MeetingPlace via WAN links, adds the following design recommendations:

- Remote user web collaboration bandwidth must be taken into account to understand the impact on existing links and to size new links. Bandwidth utilization is covered in the section on [Call Admission Control, QoS, and Bandwidth](#), page 14-8.
- Cisco Unified MeetingPlace supports G.711 and G.729, allowing remote participants to connect via G.729 without the use of transcoders.
- WAN outage to remote sites would require remote participants to connect via the PSTN. Web collaboration connectivity would be unavailable unless a backup data path exists.

## Multisite WAN with Distributed Call Processing

The multisite WAN deployment with distributed call processing builds again upon the previous model, moving call processing to multiple locations via multiple Unified CM clusters (see Figure 14-4). In this example environment, Cisco Unified MeetingPlace components are distributed as well.

Figure 14-4 Multisite Deployment with Distributed Call Processing



210149

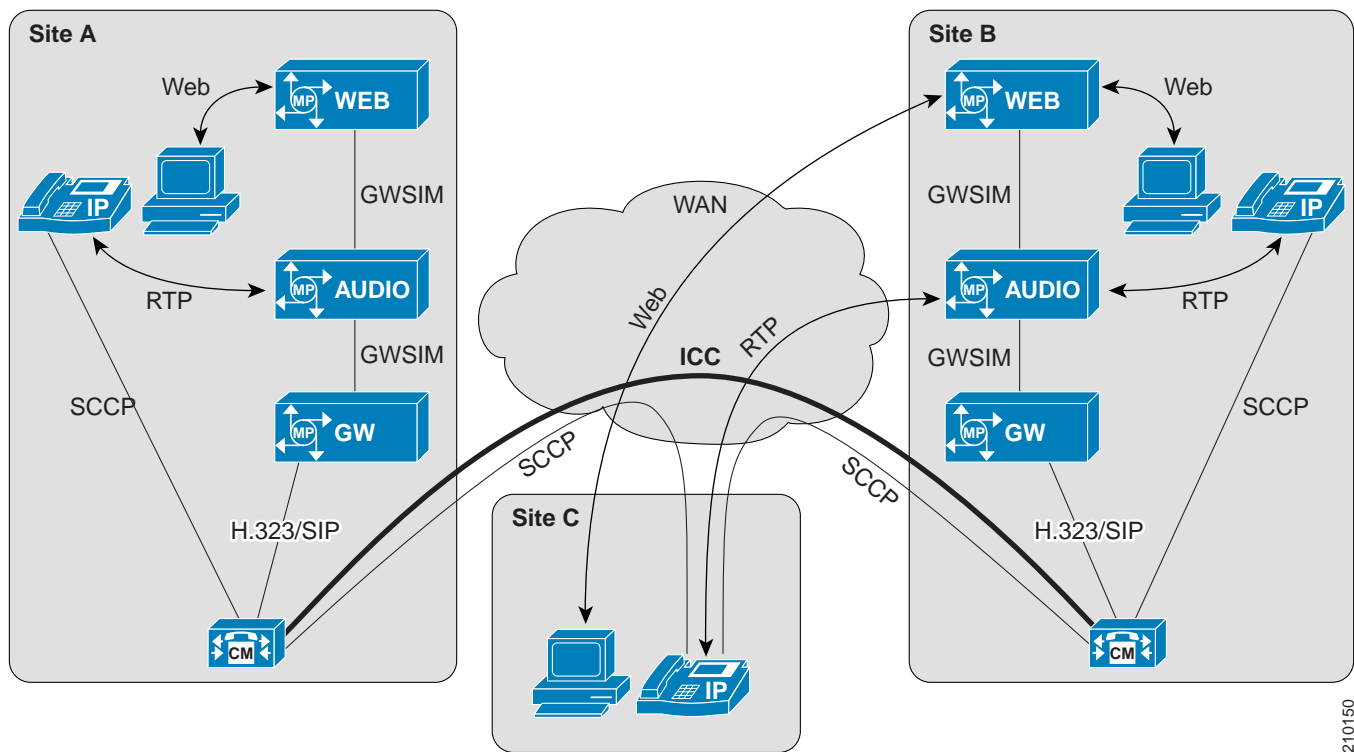
The multisite model with distributed call processing adds the following design considerations:

- Options for distributing Cisco Unified MeetingPlace can be applied to the centralized call processing model.
- Audio servers can be distributed to multiple locations, all with direct connectivity to a single central cluster or to multiple co-located clusters.
- Cisco Unified MeetingPlace Multiserver Meetings allow cascading of audio servers, which can conserve bandwidth by allowing local users to utilize their local audio server.
- Cisco Unified MeetingPlace Web collaboration servers can be distributed across multiple sites, but not geographically cascaded for active conferences. Multiserver or Clustered web conferencing is not geographically aware but does provide load balancing and scalability.

## Clustering Over the WAN

The model for clustering over the WAN spreads a single Unified CM clusters across multiple sites, making that single cluster geographically redundant and taking high availability to the next level (see [Figure 14-5](#)). Incorporating Cisco Unified MeetingPlace into this environment implies a focus on redundancy and high availability.

Figure 14-5 Clustering Over the WAN



Multiple Cisco Unified MeetingPlace audio servers and web collaboration servers can be distributed across Unified CM clustered sites. User profile information can be synchronized between servers, keeping user profiles accurate in multiple sites. During a WAN outage, each server will still be able to serve local participants as well as any remote participants having connectivity.

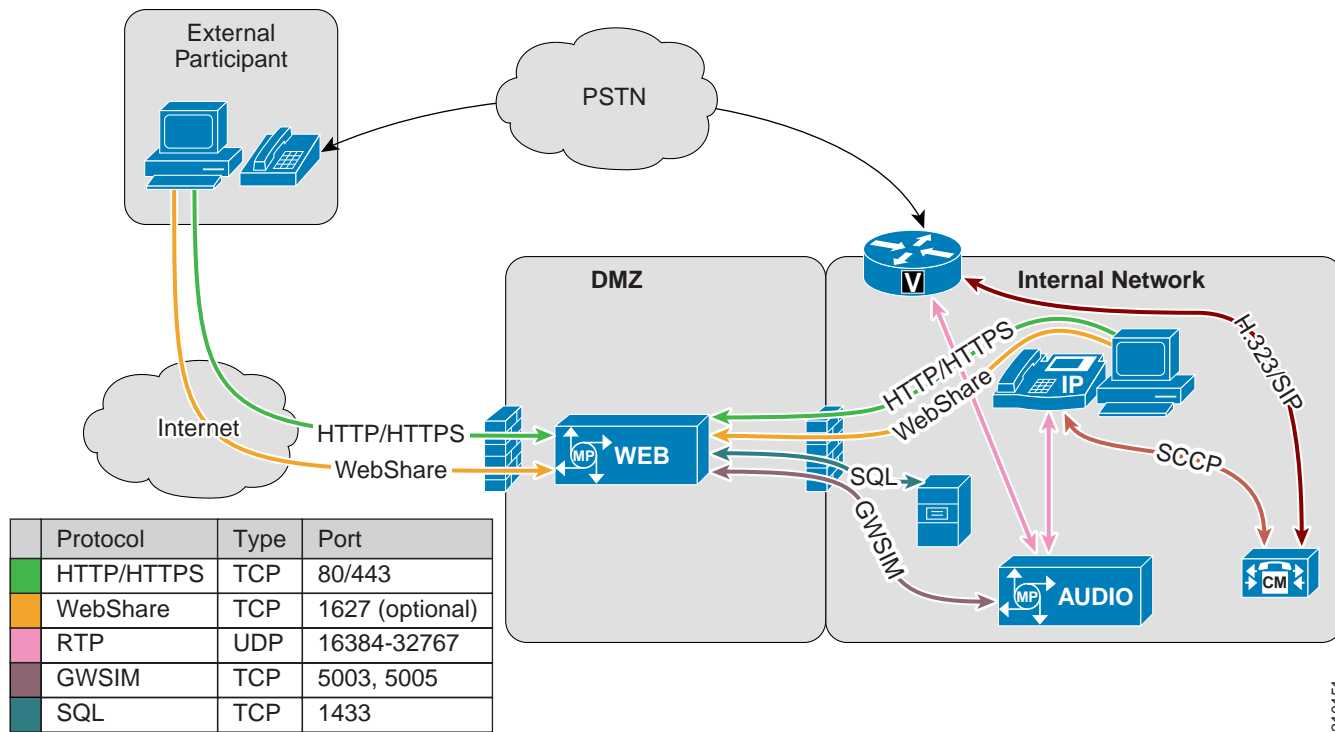
For more information regarding Cisco Unified MeetingPlace redundancy features, refer to the section on [Redundancy and Load Balancing, page 14-12](#), as well as the Cisco Unified MeetingPlace product documentation available at

[http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd_products_support_series_home.html)

## DMZ Deployment

Cisco Unified MeetingPlace (Release 5.4 and later) supports the placement of a web collaboration server within the demilitarized zone (DMZ). (See Figure 14-6.) Meetings with external participants automatically use this server for web collaboration. Audio from external participants comes into Cisco Unified MeetingPlace either through a direct TDM trunk to the Audio Server or through a VoIP gateway (controlled by Unified CM) to a VoIP port on the Audio Server.

Figure 14-6 DMZ Deployment



This deployment option, referred to as Segmented Meeting Access (SMA), may be applied to any variation of the deployment models discussed previously in this chapter. SMA implementations require deployment of an internal web server. For more information on SMA, refer to the Cisco Unified MeetingPlace product documentation available at

[http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd_products_support_series_home.html)

210151

# Call Admission Control, QoS, and Bandwidth

Call admission control, Quality of Service (QoS), and proper bandwidth allocation are the main mechanisms to ensure voice and video quality. This section describes how these mechanisms apply to Cisco Unified MeetingPlace.

## Call Admission Control

Call admission control with Cisco Unified MeetingPlace should be treated the same as call admission control with a Cisco IP Telephony gateway. Cisco Unified MeetingPlace acts like a gateway connected via a gatekeeper, directly via H.323, or via a SIP trunk. For the most effective call admission control implementations, the Cisco Unified MeetingPlace Audio Server and IP Gateway component should be co-located.

For further information regarding call admission control strategies, refer to the chapter on [Call Admission Control](#), page 9-1.

## QoS Markings

### Cisco Unified MeetingPlace Web Collaboration

Web collaboration traffic is not marked.

### Cisco Unified MeetingPlace Audio Server

RTP media from the Audio Server is marked EF (DSCP 0x2E) by default. GWSIM traffic to and from other Cisco Unified MeetingPlace components is not marked.

### Cisco Unified MeetingPlace IP Gateway Signaling

H.323 and SIP signaling traffic from the IP Gateway is not marked. Signaling traffic from Unified CM to the IP Gateway is marked CS3 (DSCP 0x18) by Cisco Unified MeetingPlace. If the IP Gateway is co-located with Unified CM, the lack of signal marking will not be an issue unless congestion is present in the locally switched network. For implementations with these components remote from each other, additional configuration may be needed to re-mark signaling traffic on the edge devices.

## Bandwidth

### Web Collaboration Bandwidth

Web Collaboration is the largest bandwidth consumer, ranging up to several Mbps per web collaboration client. This traffic becomes especially significant for remote users across WAN links. Cisco Unified MeetingPlace Web Collaboration does have the ability to reduce the amount of bandwidth consumed based on congestion encountered, but most available bandwidth will be utilized up to the maximum that Cisco Unified MeetingPlace Web can use.

### Audio Bandwidth

Audio traffic consists of Real-Time Transport Protocol (RTP) traffic flowing to and from the Cisco Unified MeetingPlace Audio server. Both G.711 and G.729 codecs are supported with Cisco Unified MeetingPlace, allowing remote users to utilize the lower bandwidth codec without the need for transcoding resources.

### Call Control Bandwidth

Call control bandwidth is extremely small but critical. Co-locating the Cisco Unified MeetingPlace IP Gateway component with Unified CM or the gatekeeper helps protect against issues with call control. Remote locations need proper QoS provisioning to ensure reliable operation.

### GWSIM

GWSIM traffic flows between the Cisco Unified MeetingPlace Audio server and other Cisco Unified MeetingPlace components including the Cisco Unified MeetingPlace IP Gateway and Cisco Unified MeetingPlace Web.

Traffic between the Cisco Unified MeetingPlace Audio Server and the Cisco Unified MeetingPlace IP Gateway component is minimal but important traffic. Placing the Audio Server and IP Gateway component in the same location helps ensure proper operation. Separation of components by a WAN would require proper QoS provisioning to ensure reliable operation.

Traffic between the Cisco Unified MeetingPlace Audio Server and Cisco Unified MeetingPlace Web includes some database synchronization and might therefore at times be bursty in nature, but this traffic is not real-time.

## Directory Integration

The Cisco Unified MeetingPlace Directory Services component provides direct synchronization of directory server information. The Directory Services component supports the following directory servers:

- Microsoft Active Directory 2000 and 2003

Microsoft Active Directory enables you to store, access, and manipulate organizational information about users and resources, and manage all elements of a networked environment, such as computers, groups, users, policies, and other user-defined objects.

- Netscape/SunOne/iPlanet LDAP Directory Server Version 4 and Version 5

Netscape/SunOne/iPlanet is a general-purpose LDAP directory that stores, publishes, and centrally manages users and network resources.

- Unified CM directory

Synchronizations of user data from the Unified CM directory enable the Cisco Unified MeetingPlace system to support IP telephony users who are configured in Unified CM.

For details about the Directory Services component, refer to the *Administration Guide for Cisco Unified MeetingPlace Directory Services*, available at

[http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html)

## H.323 and SIP Direct Integration

Cisco Unified MeetingPlace integrates with Unified CM through the Cisco Unified MeetingPlace IP Gateway. This gateway provides multiple methods for integration. The first two methods, discussed in this section, involve direct integration via H.323 or SIP between Unified CM and the Cisco Unified MeetingPlace IP Gateway. The third method involves the use of a gatekeeper for integration and is discussed in the section on [Gatekeeper Integration, page 14-11](#).

*Figure 14-7 Direct Integration Through H.323 or SIP*



### H.323

H.323 integration, by defining Cisco Unified MeetingPlace as an H.323 gateway on Unified CM, is the preferred implementation at this time. This method has the following characteristics:

- All outbound and inbound calls route through a single Unified CM cluster.
- Call admission control and dial plan rules are enforced using the defined H.323 gateway.

### SIP

SIP integration, by defining a SIP trunk on Unified CM and Cisco Unified MeetingPlace, is the less preferred implementation at this time. A static media termination point (MTP) must be associated with all calls across a SIP trunk between Unified CM and Cisco Unified MeetingPlace. This requirement is due to the lack of delayed-media support in Cisco Unified MeetingPlace. The SIP trunk has the same capabilities listed above for H.323, but the following limitations apply:

- Static MTP is required
- The audio codec must be G.711 with the static MTP; transcoders must be used for G.729.

Due to these limitations, implementation via H.323 is the preferred method at this time.

Implementation of a SIP trunk also has the following requirements when configuring on Unified CM:

- MTP Required must be checked in the SIP Trunk configuration, and MTP resources must be available.
- A separate SIP Trunk Security profile must be created, with the outbound transport type set to UDP and associated with the SIP Trunk to Cisco Unified MeetingPlace.

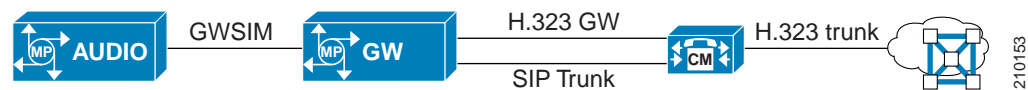
# Gatekeeper Integration

Cisco Unified MeetingPlace can be integrated into a gatekeeper environment by either of the two methods detailed in this section. The addition of video support to Cisco Unified MeetingPlace adds more complex gatekeeper requirements, which are outlined in the section on [Video Gatekeeper Integration](#), page 14-20.

## Integration Via Unified CM to a Gatekeeper

Integrating via H.323 or SIP directly to Unified CM, as described in the previous section, allows all incoming and outgoing calls to be controlled by Unified CM. Off-cluster incoming and outgoing calls are routed through the Unified CM gatekeeper trunk (see [Figure 14-8](#)). Implementation in this manner takes advantage of Unified CM dial plan restrictions, abbreviated dial, and digit manipulation.

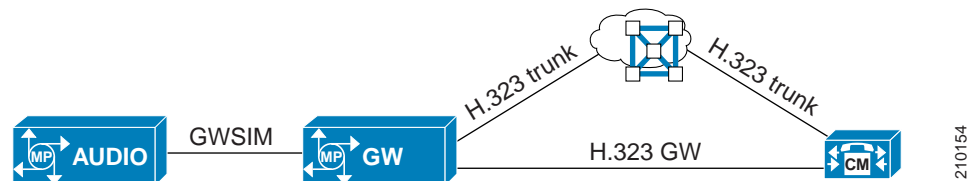
**Figure 14-8** Integration Via Unified CM to a Gatekeeper



## Integration Directly to a Gatekeeper

Cisco Unified MeetingPlace can register directly with a gatekeeper as a terminal (see [Figure 14-9](#)). The primary E.164 address defined in the Cisco Unified MeetingPlace system is used when registering. Additional E.164 addresses for direct-dial meetings must be assigned statically in the gatekeeper. This model has some additional redundancy because the gatekeeper is able to route outbound calls to multiple nodes.

**Figure 14-9** Integration Directly to a Gatekeeper



The destination Unified CM cluster or clusters may be configured with an H.323 gateway pointing to one or more MeetingPlace IP Gateways to match incoming calls from these gateways and enforce dial plan restrictions and call admission control restrictions.

In a Unified CM environment, the following considerations apply to direct registration with a gatekeeper:

- Outdialed calls from Cisco Unified MeetingPlace are resolved in the gatekeeper and are not subject to dial restrictions or call admission control restrictions imposed in Unified CM.
- Outdialed calls from Cisco Unified MeetingPlace do not benefit from abbreviated dialing or digit manipulation defined in Unified CM.

# Dial Plan

The dial plan is one of the key elements of an IP Telephony system and an integral part of all call processing agents. The dial plan is responsible for instructing the call processing agent on how to route calls.

## Unified CM Dial Plan

As mentioned previously, Cisco Unified MeetingPlace can be integrated with Unified CM by any of the following means:

- H.323 gateway defined on Unified CM
- SIP trunk between Cisco Unified MeetingPlace and Unified CM
- Direct gatekeeper integration

With the first two methods, the dial plan with respect to Cisco Unified MeetingPlace is relatively simple. Cisco Unified MeetingPlace is referenced via a route pattern defined on Unified CM, which points to the H.323 gateway or SIP trunk. All other dial plan configuration is handled through Unified CM and possibly a gatekeeper if Unified CM is connected to a gatekeeper. Use of a route list to point to multiple Cisco Unified MeetingPlace IP gateways adds redundancy and is covered in the section on [Redundancy and Load Balancing, page 14-12](#).

With the third method, direct gatekeeper integration, the dial plan centers more on the gatekeeper. Cisco Unified MeetingPlace registers with the gatekeeper as a terminal with a single E.164 address. You must consider this factor when planning gatekeeper integration so that any abbreviated dialing expansion or digit manipulation can allow for proper call resolution to the single E.164 address.

## Reservationless Single Number Access (RSNA)

The Reservationless Single Number Access (RSNA) feature enables multiple Cisco Unified MeetingPlace Audio Servers to appear as one server to the user community. This feature is designed primarily for reservationless meetings. With this feature, users can dial a single directory number to access multiple Audio Servers deployed in the same or different locations. Users enter their reservationless ID, and the system directs the calls to the appropriate server for that meeting. This feature also enables users in a remote location to dial the local server.

RSNA relies on the SIP REFER method. SIP trunks on Unified CM support REFER, enabling the implementation of this feature. Before planning implementation of RSNA, refer to the limitations of integration via a SIP trunk listed in the section on [H.323 and SIP Direct Integration, page 14-10](#).

## Redundancy and Load Balancing

This section describes redundancy and load balancing considerations for the following MeetingPlace components:

- [Cisco Unified MeetingPlace Audio Server, page 14-13](#)
- [Cisco Unified MeetingPlace H.323/SIP IP Gateway, page 14-14](#)
- [Cisco Unified MeetingPlace Web, page 14-15](#)
- [Unified CM, page 14-15](#)

## Cisco Unified MeetingPlace Audio Server

If the MeetingPlace Audio Server fails, calls in progress will be dropped. If the Audio Server is unreachable by the MeetingPlace H.323/SIP IP Gateway, the MeetingPlace H.323/SIP IP Gateway will immediately reject any incoming calls. If the MeetingPlace H.323/SIP IP Gateway is down, Unified CM will be unable to establish an H.323 connection with the MeetingPlace H.323/SIP IP Gateway. There is no automatic failover mechanism available for the MeetingPlace Audio Server.

### Disaster Recovery

A disaster recovery plan provides for orderly restoration of the database, computing, and services. The plan usually includes the following provisions:

- Redundancy (spare parts of hardware)
- Data and software backups
- Alternate emergency locations
- Operations split across multiple sites

A component called the MeetingPlace Network Backup Gateway enables system managers to transfer multiple copies of the MeetingPlace database (audio configuration files and scheduled meeting information) from the Audio Server to a designated storage server on the network. Files are encrypted for security. A maximum of three Network Backup Gateways per system can be implemented, but only one of them can make the database transfer at a time.

### Redundancy

If two or more MeetingPlace Audio Servers are deployed, any of the following plans for redundancy can be implemented:

- Shadow Server

A shadow server is a redundant MeetingPlace Audio Server that is not active until the primary Audio Server fails. During the disaster, the shadow server must be switched from shadow mode to active mode using the command line interface (CLI). Once active, the shadow server can store only limited information, such as profile information, meeting information (past, present, and future), and participant information. Recording, attachments, hardware and network configuration, and automatic software upgrades are not available on the shadow server. The shadow server has the following network connectivity requirements:

- Less than 250 ms round trip delay
- Less than 1% packet loss
- Minimum bandwidth of 384 kbps

- Dual Conference Servers

In this plan, two MeetingPlace Audio Servers are active production servers, and each one can overflow to the other. Profiles are synchronized automatically between the servers through the Directory Services. Automatic failover between the two Audio Servers does *not* occur. Meetings have to be uploaded to the remaining server during an emergency, and users must rejoin the meetings manually. On Unified CM, you can configure route groups and route lists so that if one MeetingPlace Audio Servers fails, the calls will be routed to the other active MeetingPlace Audio Server.

- Continuous Meeting Server

In this plan, a MeetingPlace Audio Server is implemented with a set of critical meetings pre-created and always available. This deployment is suitable for any crisis management application, with features such as blast outdial to crisis management teams.

## Cisco Unified MeetingPlace H.323/SIP IP Gateway

The following redundancy and load balancing considerations apply to the MeetingPlace H.323/SIP IP Gateway.

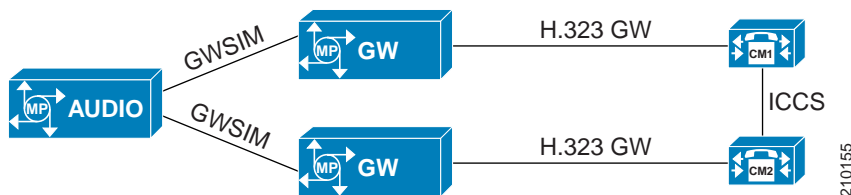
### Redundancy

If the MeetingPlace H.323 IP Gateway fails, calls in progress will be dropped.

Two or more MeetingPlace H.323 IP Gateways can connect to the same MeetingPlace Audio Server. There are two methods for implementing redundancy, one with and one without a gatekeeper.

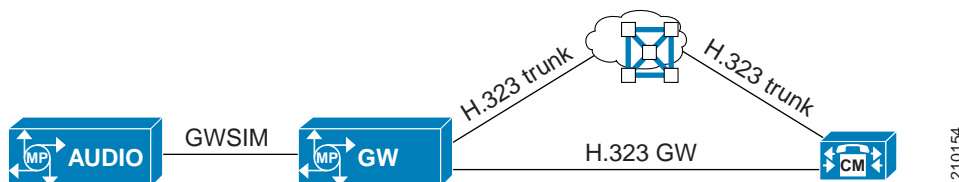
- Redundancy without a gatekeeper (see [Figure 14-10](#))
  - Configure all of the MeetingPlace H.323 IP Gateways on Unified CM and put them in the same route group. If the link between Unified CM and the MeetingPlace H.323/SIP IP Gateway fails, Unified CM chooses the next MeetingPlace H.323/SIP IP Gateway in the current route group. This same method also works for load balancing.
  - Configure the MeetingPlace H.323 IP Gateways to point to different Unified CM nodes. If one Unified CM node fails, outbound calls are placed through one of the other MeetingPlace IP Gateways to its configured Unified CM node.

**Figure 14-10** Redundancy Without a Gatekeeper



- Redundancy with a gatekeeper (see [Figure 14-11](#))
  - Calls outbound from MeetingPlace that are sent to the gatekeeper may be directed to alternate Unified CM nodes in the event of a Unified CM failure. This is an advantage over direct outbound configuration on a single MeetingPlace IP Gateway, which allows only one destination node to be configured.
  - The use of a defined H.323 gateway on Unified CM is still recommended for this model to provide call admission control and dial plan restrictions as well as redundancy for inbound calls if there are multiple MeetingPlace IP Gateways.

**Figure 14-11** Redundancy With a Gatekeeper



### Load Balancing

For dial-in load balancing, you can use either of the following same approaches for redundancy:

- Use a route group in Unified CM, but choose **Circular** instead of **Top down** for the Distribution Algorithm. Unified CM will distribute the outbound calls between the gateways in round-robin fashion.
- Use a gatekeeper. For purposes of load balancing, do not configure **gw-priority** to specify a preferred gateway. Instead, let the gatekeeper distribute the calls in round-robin fashion to all the registered gateways.

As explained in the previous section, load balancing for outdialing is done only among those MeetingPlace H.323/SIP IP Gateways that never have outdial failures.

## Cisco Unified MeetingPlace Web

The following redundancy and load balancing considerations apply to the MeetingPlace Web.

### Redundancy

If a web-conferencing server fails during a web conference, all users are disconnected from the web portion of the meeting, and the current web conference cannot continue. Users can rejoin their web conference on another active web server. If the SQL server database is on the failed server, all web conferencing servers in the cluster become nonfunctional and users will be unable to conduct web conferences until the database is restored.

### Load Balancing

MeetingPlace Web servers can be grouped into clusters to increase performance for load balancing (to distribute the meeting requests to different web servers) and to increase the capability of handling more meetings. The MeetingPlace Web cluster can contain a maximum of six web servers in either internal or external configurations.

The MeetingPlace WebConnect feature provides integration between multiple internal and external MeetingPlace systems through a single URL. External systems reside in the DMZ for external users. It can schedule across multiple Audio Servers. If there is not enough capacity on the first Audio Server, it will try the second, and so on.

## Unified CM

The following redundancy and load balancing considerations apply to Unified CM.

### Redundancy

If Unified CM fails, MeetingPlace calls in progress using that Unified CM will be dropped and users must rejoin the meeting.

For calls going to and from the MeetingPlace H.323/SIP IP Gateway, see the section on [Cisco Unified MeetingPlace H.323/SIP IP Gateway, page 14-14](#), for redundancy information.

### Load Balancing

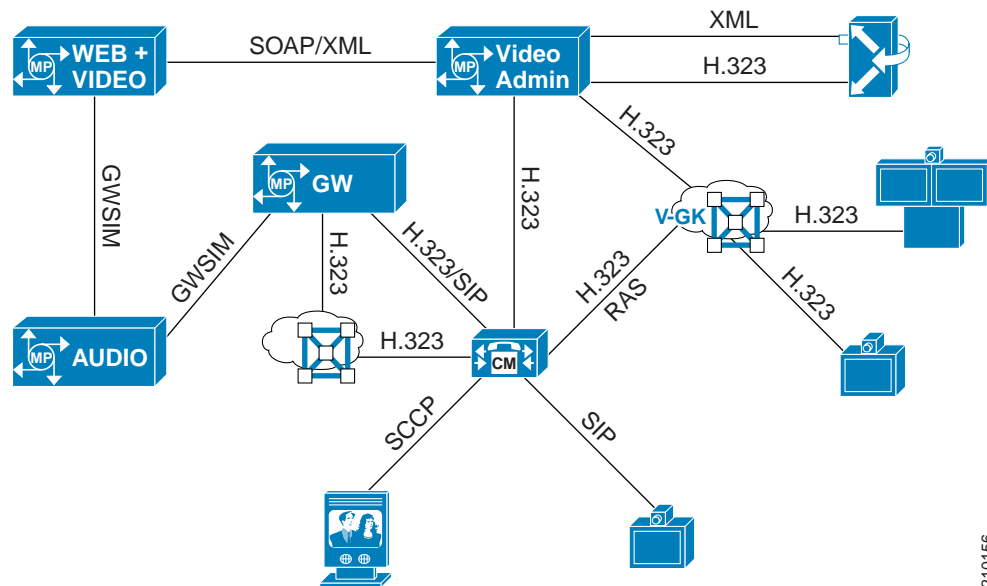
For dial-in from endpoints to MeetingPlace, load balancing for calls is achieved through Unified CM redundancy groups and route group configurations.

For outdialing from MeetingPlace through a MeetingPlace H.323/SIP IP Gateway, the same guidelines apply for load balancing as for redundancy.

# Cisco Unified MeetingPlace Video

Integrating video with Cisco Unified MeetingPlace 5.4 differs greatly from video integration with previous versions of Cisco Unified MeetingPlace. Cisco Unified MeetingPlace 5.4 introduces a new component called Video Administration, which is the control point for all video calls to and from the MCU. Video Administration interfaces with the Video Integration component on the MeetingPlace Web server as well as with the gatekeeper and Unified CM directly. (See [Figure 14-12](#).) The remainder of this chapter discusses the impact on system design due to Cisco Unified MeetingPlace Video, and primarily due to the Video Administration component.

**Figure 14-12** Cisco Unified MeetingPlace 5.4 Video Integration



## Note

In this chapter, the name Cisco Unified MeetingPlace Video refers to the entire video system, including Video Administration, the Video Integration component, MCUs, gatekeepers, endpoints, and Unified CM. One component of the system is the Video Integration component, which resides on one or more Cisco Unified MeetingPlace Web servers. Some other Cisco Unified MeetingPlace documents refer to Video Integration as the entire video system, and this difference will be noted where possible when referencing those documents.

## Video Administration

Video Administration is a new component introduced with Cisco Unified MeetingPlace 5.4 Video. It controls all aspects of video conferencing, interfacing with MCUs, gatekeeper, Unified CM, and other Cisco Unified MeetingPlace 5.4 components.

Video Administration is the main control point for all incoming and outgoing video calls, and it makes all decisions regarding resource utilization and cascading of resources. In addition to basic MCU cascading to increase conference size, Video Administration can intelligently select which MCU to use based on internally defined locations for each participant. Multisite video meetings can result in cascading MCUs local to user groups, thus creating one link across a WAN between cascaded MCUs.

Video Administration has the following characteristics:

- Video Administration resides on a separate Windows-based server and cannot reside on the same server with other Cisco Unified MeetingPlace components.
- Video Administration sits between the MCUs and all other components. The Cisco Unified MeetingPlace Video Integration component, Unified CM, and the gatekeeper communicate with Video Administration, which in turn communicates with the MCUs.
- Video Administration contains a special integrated gatekeeper to which only the MCUs register. The MCUs must register to Video Administration.
- All routing decisions for MCU selection and cascading are made by Video Administration.
- Video Administration terminates and authenticates all inbound calls, and only media is sent to the MCUs.
- Video Administration originates and maintains all outbound calls, and only media is sent to the MCUs.
- Video Administration requires the use of an external gatekeeper for outbound calls.
- Video Administration does not register to the gatekeeper it uses for outbound calls.
- Video Administration does not support a direct SIP trunk connection from Unified CM.
- Video Administration does not support a direct H.323 gatekeeper-controlled trunk connection from Unified CM but rather is defined as an H.323 gateway in Unified CM.
- All video meetings scheduled in Cisco Unified MeetingPlace 5.4 are replicated in Video Administration, with appropriate resources reserved
- Participant information and real-time status are relayed from the MCUs to Cisco Unified MeetingPlace components by Video Administration.
- Other than media stream termination, only Video Administration communicates with the MCUs.
- Video Terminals can be defined in Video Administration and reserved within Cisco Unified MeetingPlace Web when users create a meeting.
- Any endpoint (H.323, SCCP, or SIP) can be defined in Video Administration as a Video Terminal.
- MCU selection can be impacted by assigning locations to MCUs and Video Terminals defined in Video Administration.

## Video Deployment Models

This section discusses design considerations and recommendations for adding Cisco Unified MeetingPlace Video to each of the basic Unified CM deployment models. Many variations are possible in the deployments, but the models presented here cover the base deployments without examining every variation.

### Single-Site Deployment

With a single-site deployment, all components are located in one site with no remote participation. [Figure 14-12](#) illustrates a single site.

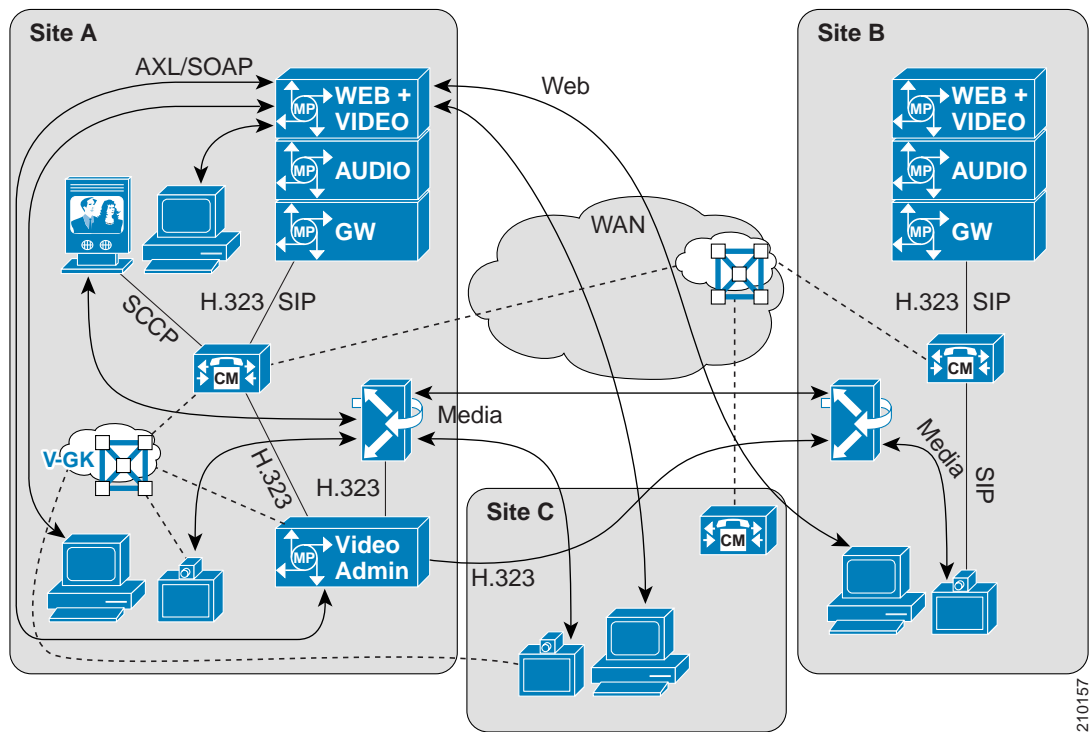
### Multisite Centralized Deployment

The multisite model with centralized call processing adds remote users to a centralized deployment. All Cisco Unified MeetingPlace Video components reside in the central data center. Remote participants proper bandwidth allocation and QoS provisioning to ensure proper operation. See [Call Admission Control, QoS, and Bandwidth](#), page 14-8, for more information.

### Multisite Distributed Deployment

Multisite distributed deployment adds decentralized call processing and decentralized Cisco Unified MeetingPlace Video components.

Figure 14-13 Multisite Distributed Deployment with Video



The following design notes apply to this model:

- For MCUs that are remote from Video Administration, you must take into account the important call admission control and call routing restrictions that are documented in the section on [Call Admission Control, QoS, and Bandwidth](#), page 14-8.
- Video Administration does have the ability to route calls intelligently to local MCU resources if they are configured properly.
- Remote H.323 video endpoints must be registered to the central video gatekeeper unless multiple video gatekeepers are implemented
- All Cisco Unified MeetingPlace Web participants must use the single active Cisco Unified MeetingPlace Web server with Video Integration enabled.
- The dial plan on the infrastructure gatekeeper should route all calls destined for Cisco Unified MeetingPlace Video to the associated Unified CM cluster.

### Clustering Over the WAN

Due to the limitations of having only one Video Administration server, clustering over the WAN does not change from the multisite distributed model with respect to Unified CM Video components.

When implementing clustering over the WAN, it is best to include only local Unified CM nodes when defining the redundancy group for Video Administration connections.

## Video Call Admission Control, QoS, and Bandwidth

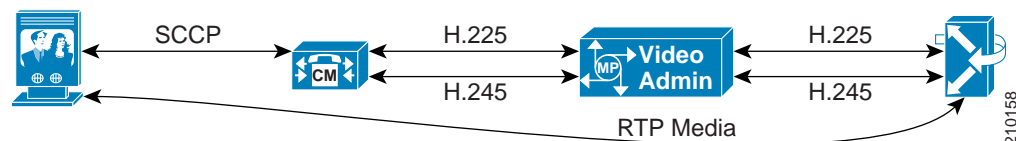
Call admission control, Quality of Service (QoS), and proper bandwidth allocation are the main mechanisms to ensure voice and video quality. This section describes how these mechanisms apply to Cisco Unified MeetingPlace Video.

### Video Call Admission Control

Video Administration is the routing point for all MCUs, and it determines on which MCU each call terminates. As shown in [Figure 14-14](#), all H.225 and H.245 signaling terminates on Video Administration:

- All inbound video calls terminate on Video Administration.
- All outbound video calls originate from Video Administration.
- All signaling to and from the MCU is handled by Video Administration.

**Figure 14-14** Video Administration Signaling Termination



Because of this functionality, visibility beyond Video Administration for any current call admission control mechanism is not possible. Video Administration is seen as the terminating endpoint to all call admission control mechanisms.

Implementation of call admission control with MCUs distributed across multiple sites becomes a challenge. Currently the only call admission control capabilities for distributed MCUs are implemented separately within Video Administration and do not tie into any other mechanism in any way. This is an independent, standalone call admission control mechanism for use only with Video Administration MCUs. It is not an optimal way to implement call admission control but is the only available option for this release of Cisco Unified MeetingPlace.

Implementation of call admission control via the Video Administration component is detailed in the *Administration Guide for Cisco Unified MeetingPlace Video Integration Release 5.4*, available at

[http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html)



#### Note

The term Video Integration in the above Administration Guide is equivalent to the term Cisco Unified MeetingPlace Video in this chapter.

## Video QoS

The following traffic markings apply call control, media, and other flows:

- Video Administration does not mark outgoing H.323 call control traffic.
- Incoming H.323 call control traffic from Unified CM to Video Administration is marked CS3 (DSCP 0x18) by default.
- Traffic between Video Administration and the MCU is not marked.
- The MCU marks outgoing media with AF41 (DSCP 0x22) by default.
- Traffic between Video Administration and the Video Integration component is not marked.

For components separated by WAN links, re-marking may be needed to ensure reliable operation. For further information regarding video QoS, refer to the chapter on [IP Video Telephony, page 16-1](#).

## Video Bandwidth

See the chapter on [IP Video Telephony, page 16-1](#), for current information regarding video bandwidth.

## Video Gatekeeper Integration

With the introduction of Cisco Unified MeetingPlace 5.4, Gatekeeper is required to outdial video calls from Video Administration to video endpoints, regardless of the type of endpoint. This requirement, among other changes with Cisco Unified MeetingPlace Video, significantly impacts the way Unified CM, Cisco Unified MeetingPlace, and Video Gatekeeper interact in this environment. The following sections detail relevant subjects involving Video Gatekeeper and its critical role in the deployment of video with Cisco Unified MeetingPlace 5.4.

This section assumes Video Administration uses Video Gatekeeper to route all outbound calls through Unified CM. Integration of Video Administration into an infrastructure gatekeeper environment, bypassing Unified CM, is another deployment option not covered here due to the focus on endpoints controlled by Unified CM.

This section covers the following topics:

- [H.323 Video Endpoints and Video Gatekeeper, page 14-21](#)  
Basic concepts of how H.323 video endpoints interact with Video Gatekeeper.
- [Via-Zone Video Gatekeeper, page 14-21](#)  
Description of how a via-zone gatekeeper operates.
- [Video Administration and Video Gatekeeper Overview, page 14-22](#)  
Overview of how Video Administration and Video Gatekeeper interact and process inbound and outbound calls.
- [Video Administration and Video Gatekeeper Integration with Unified CM, page 14-23](#)  
Specifics around Unified CM configuration and interaction with Video Administration and Video Gatekeeper.
- [Additional Video Gatekeeper Configuration Requirements, page 14-23](#)  
Additional steps to ensure proper call resolution within Video Gatekeeper for outbound calls from Video Administration.

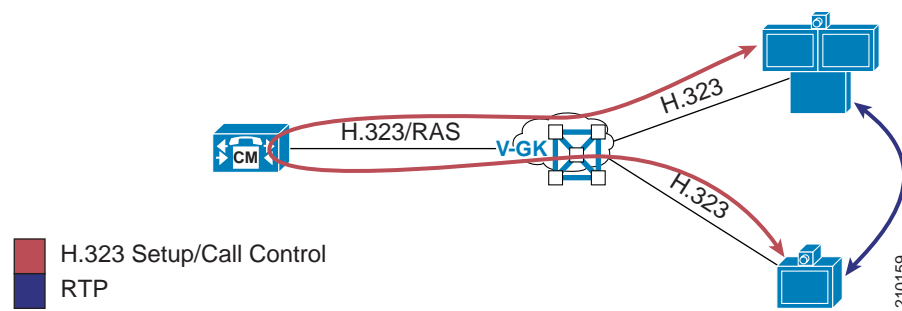
- [Zones and RASAggregator Redundancy Groups with H.323 Video Endpoints on Unified CM, page 14-24](#)

Critical information regarding redundancy groups and gatekeeper zone configuration of H.323 video endpoints defined on Unified CM.

## H.323 Video Endpoints and Video Gatekeeper

For deployments incorporating H.323 video endpoints, a separate video endpoint gatekeeper is recommended. (See [Figure 14-15](#).) This gatekeeper should be set up as a via-zone gatekeeper, as explained below. Setup of this nature ensures that every call between H.323 video endpoints and any other video endpoint or termination point (SIP, SCCP, Cisco Unified MeetingPlace Video Administration, or other H.323 video endpoints on the same gatekeeper) are handled by Unified CM for digit manipulation, dialing restrictions, and call admission control.

*Figure 14-15 Video Endpoints and Video Gatekeeper*



## Via-Zone Video Gatekeeper

The via-zone gatekeeper can be a complex concept, but the following points present a very simplified way of looking at it and the easiest way to understand the basic operation in this environment:

- Via-zone gatekeepers route calls through an IP-to-IP gateway.
- Video Gatekeeper is a via-zone gatekeeper.
- Unified CM acts as an IP-to-IP gateway.
- Video Gatekeeper routes all calls through Unified CM.



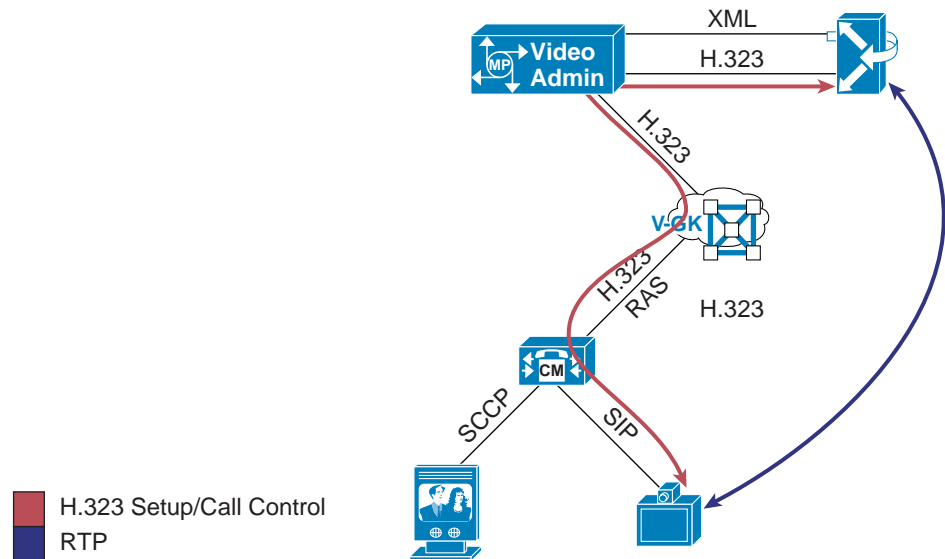
Note

You must configure Unified CM to act as an IP-to-IP gateway by setting the H.323 Service Parameter **Send Product ID and Version ID** to **TRUE**.

## Video Administration and Video Gatekeeper Overview

Video Administration requires the use of a gatekeeper to resolve outbound calls. Video Administration sends Location Request messages (LRQs) to this gatekeeper while not registering in any way to that gatekeeper. (See [Figure 14-16](#).) This behavior differs greatly from previous Cisco Unified MeetingPlace versions.

*Figure 14-16 Video Administration and Video Gatekeeper*



In [Figure 14-16](#), an outbound call is placed to a SIP video endpoint controlled by Unified CM. This example is a simplified illustration of basic call flow but is not a detailed or complete example of call flow for outbound calls. For a detailed explanation of call flows, See the section on [Video Call Flows](#), page 14-27.

In a Unified CM environment that contains a Video Gatekeeper for H.323 video endpoints, the logical choice is to use Video Gatekeeper to route all calls through Unified CM.

Sending outbound calls to the Video Gatekeeper would route calls through Unified CM and would apply dial plan restrictions, abbreviated dial, and digit manipulation.

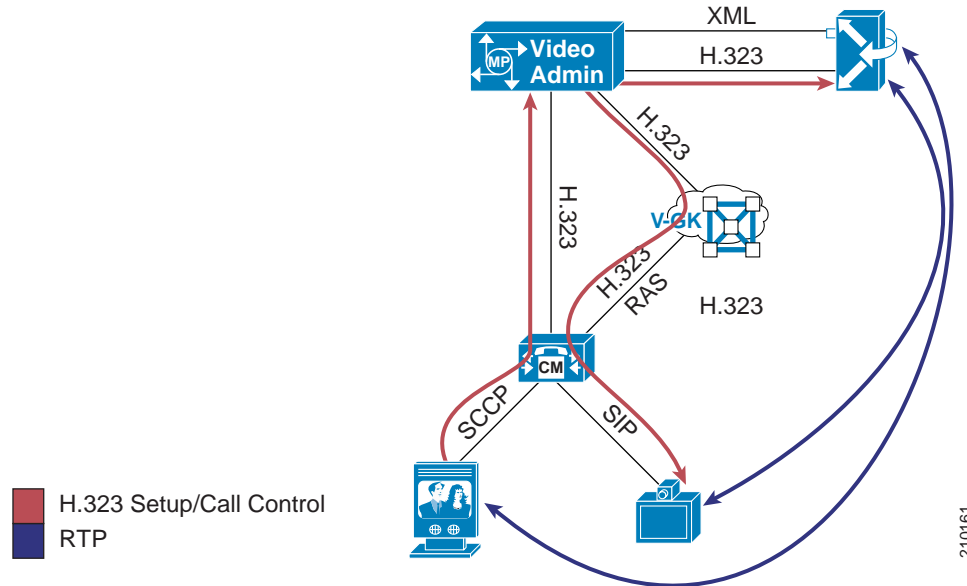
Sending outbound video calls to the primary gatekeeper, if one exists, would have the following effects:

- Outdialed calls from Video Administration are resolved in the gatekeeper and are not subject to dialing restrictions imposed in Unified CM.
- Outdialed calls from Video Administration do not benefit from abbreviated dialing or digit manipulation defined in Unified CM.

## Video Administration and Video Gatekeeper Integration with Unified CM

Building upon the previous section, this section takes a closer look at the role of Unified CM configuration in the environment illustrated in [Figure 14-17](#).

*Figure 14-17 Video Administration, Video Gatekeeper, and Unified CM*



You must configure an H.323 gateway on Unified CM to point to the Video Administration server. The role of this H.323 gateway is critical for calls both inbound to and outbound from Video Administration.

Calls inbound to Unified CM (outbound from Video Administration) resolve via Video Gatekeeper to a particular Unified CM node. H.225 setup is then sent from Video Administration to that Unified CM node. Unified CM matches the incoming call to the defined H.323 gateway and applies any restrictions or manipulation associated with that gateway to the call. The H.323 trunk and Registration Admission Status (RAS) Aggregator to Video Gatekeeper are critical as well to provide call resolution, but the H.323 gateway defined on Unified CM provides control of the ingress call from Video Administration.

Calls outbound to Video Administration (inbound from Unified CM) are resolved via dial pattern matches associated with the defined H.323 gateway on Unified CM. H.225 setup is sent directly to Video Administration, and the call is completed without the use of Video Gatekeeper.

### Additional Video Gatekeeper Configuration Requirements

With the use of a via-zone gatekeeper to resolve outbound calls from Video Administration, some additional configuration may be necessary to ensure proper call resolution.

When Video Administration attempts to resolve an outbound call, it begins by sending an LRQ to Video Gatekeeper. This LRQ is resolved to Unified CM for all outgoing calls, based on Video Gatekeeper being a via-zone gatekeeper as discussed previously. For a detailed explanation of the call flow, see the section on [Video Call Flows](#), page 14-27.

One scenario, however, can cause Video Gatekeeper to resolve to something other than Unified CM. If zone prefixes are not used in the Video Gatekeeper and the outdialed number from Video Administration matches exactly with an E.164 address registered to the Video Gatekeeper, the call will bypass Unified CM and complete directly to that endpoint. This behavior occurs regardless of the zone in which

the endpoint is registered. To resolve this issue, you can add a **hopoff** statement to Video Gatekeeper to resolve all LRQs to Unified CM via an intercluster trunk. This method should be implemented on endpoint via-zone gatekeepers only. The **hopoff** will send all calls to a particular zone regardless of origin or destination. (The example below illustrates use of the **hopoff** statement.) If zone prefixes are used on the Video Gatekeeper, this scenario does not occur.

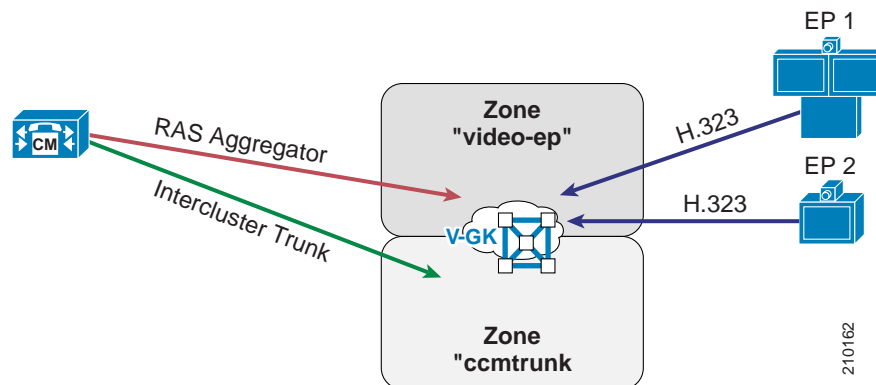
The following notes apply to the example below, which shows a simplified Video Gatekeeper configuration:

- An intercluster trunk (ICT) from Unified CM is registered to the zone `ccmtrunk`.
- H.323 video endpoints are registered to the zone `video-ep`.
- Zone prefixes are not used, forcing the use of the **hopoff** statement.
- The H.323 endpoints are defined on Unified CM in the zone `video-ep`, causing a RASAggregator trunk from Unified CM to register in that same zone.

Gatekeeper

```
zone remote video-admin cisco.com 10.2.2.2 invia ccmtrunk outvia ccmtrunk
zone local video-ep cisco.com 10.1.1.1 invia video-ep outvia video-ep enable-intrazone
zone local ccmtrunk cisco.com invia ccmtrunk outvia ccmtrunk enable-intrazone
send-cisco-circuit-info
gw-type-prefix * hopoff ccmtrunk default-technology
lrq forward-queries
no use-proxy video-ep default inbound-to terminal
no use-proxy video-ep default outbound-from terminal
no use-proxy ccmtrunk default inbound-to terminal
no use-proxy ccmtrunk default outbound-from terminal
```

Figure 14-18 Gatekeeper Configuration Example



## Zones and RASAggregator Redundancy Groups with H.323 Video Endpoints on Unified CM

Unified CM redundancy groups (Unified CM groups and device pools) can be defined for H.323 video endpoints to allow failover to another node if the primary node fails. Improper configuration of H.323 video endpoints on Unified CM with respect to these redundancy groups can easily cause call failure.

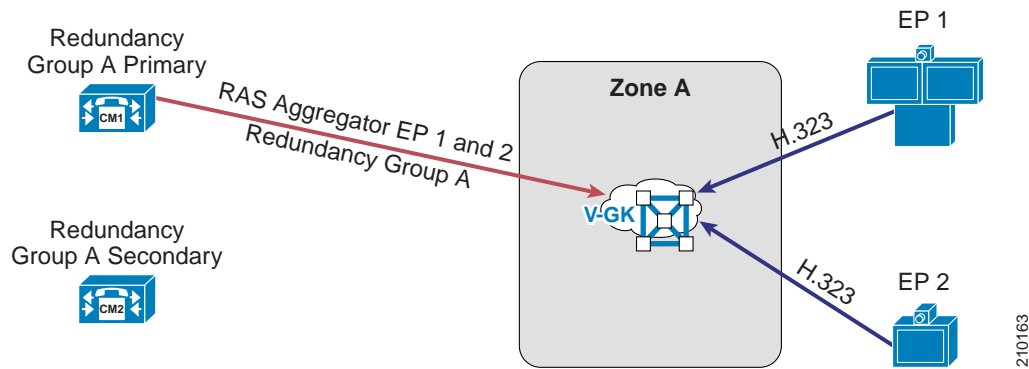
When you configure H.323 video endpoints on Unified CM, a gatekeeper and a zone are defined in addition to a redundancy group. Unified CM registers a single RASAggregator Trunk from the highest priority node listed in the chosen redundancy group. Improper configuration that allows two nodes to register RASAggregator Trunks to the same gatekeeper zone will cause call routing issues and call failure.

The following sections list the possible configuration scenarios.

**One Zone and One Redundancy Group**

In the most straightforward scenario, all the H.323 video endpoints have the same redundancy group and use the same gatekeeper zone (see Figure 14-19). One RASAggregator Trunk is registered in the single endpoint zone. This configuration ensures proper operation, with no call loss due to mis-routing.

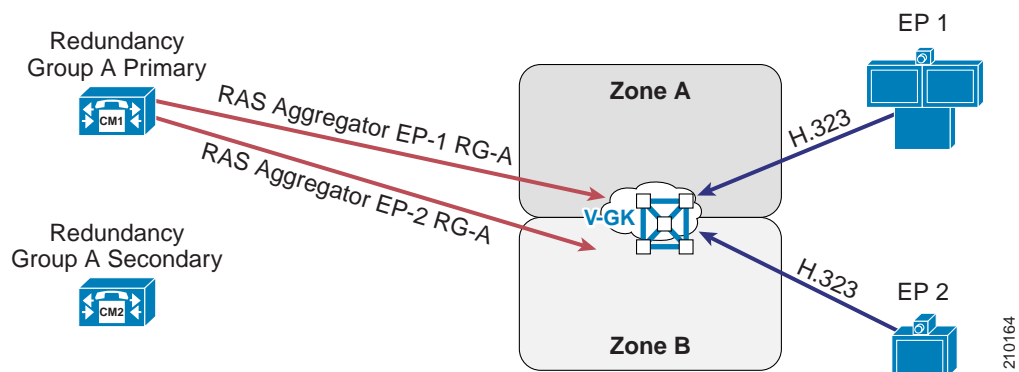
*Figure 14-19 One Zone and One Redundancy Group*



**Multiple Zones and One Redundancy Group**

In this scenario, H.323 video endpoints can be defined in Unified CM to be in different zones on the same video gatekeeper (see Figure 14-20). Two RASAggregator Trunks are registered in the two separate endpoint zones. Again this ensures proper operation, with no call loss due to mis-routing.

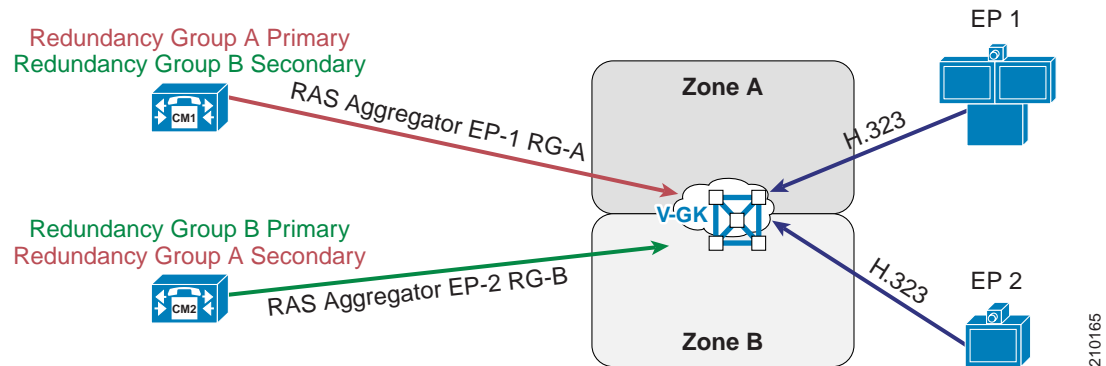
*Figure 14-20 Two Zones and One Redundancy Group*



### Multiple Zones and Multiple Redundancy Groups

This scenario should be avoided if possible due to the complexity that it adds (see [Figure 14-21](#)). Improper configuration can easily lead to failed calls.

**Figure 14-21** Two Zones and Two Redundancy Groups



### Incorrectly Configured Redundancy Groups Cause Failures

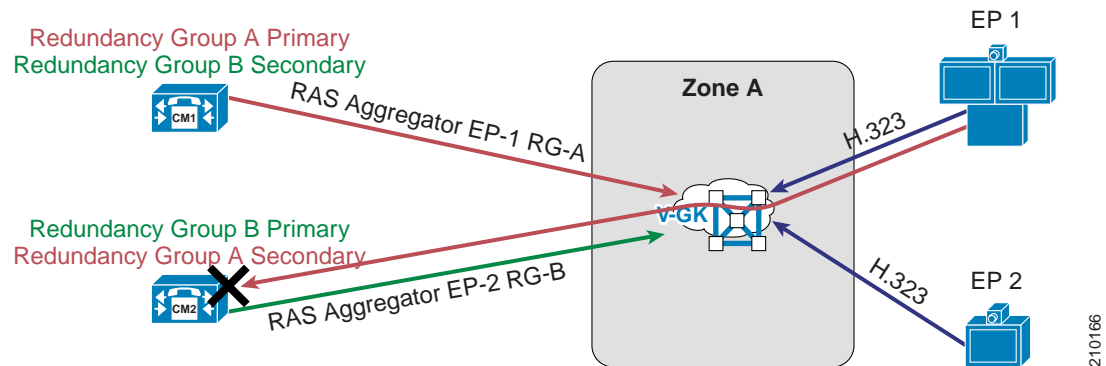


Note

All endpoints in a particular zone *must* use the same redundancy group.

[Figure 14-22](#) shows an *incorrect* configuration of two different redundancy groups registered to the same endpoint zone. This configuration will cause call failures.

**Figure 14-22** Incorrect Configuration of One Zone and Two Redundancy Groups



As shown in [Figure 14-22](#), if two endpoints in the same zone use different redundancy groups with different primary Unified CMs, two RASAggregator Trunks will be registered to one zone from different nodes, thus causing the gatekeeper to load-balance between these two trunks. In this case, some calls will be sent across incorrect RASAggregator Trunks and will fail.

## Video Call Flows

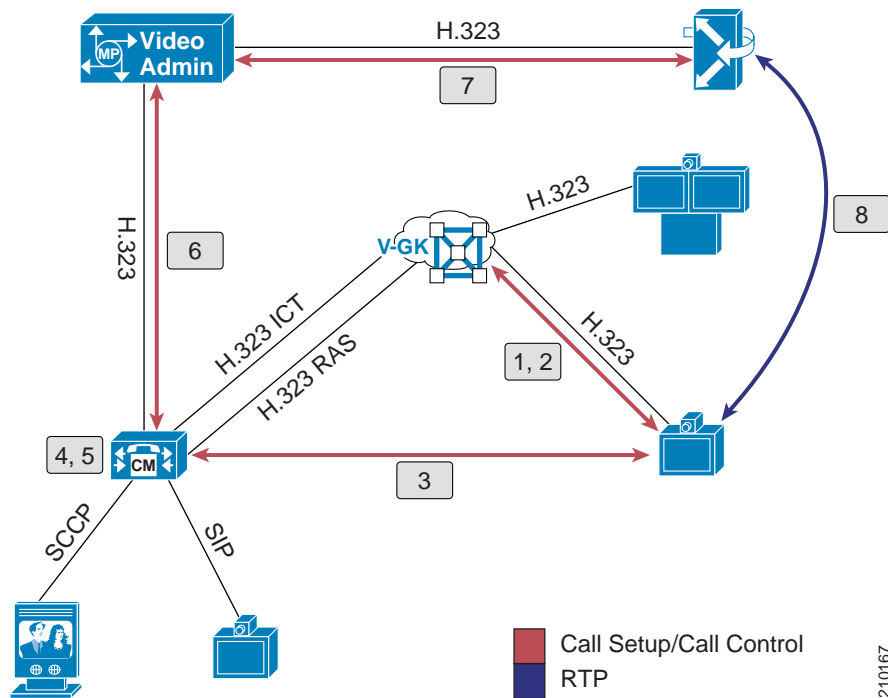
This section shows examples of call flows for inbound and outbound video calls with Cisco Unified MeetingPlace configured.

### Inbound Call from an H.323 Video Endpoint

Figure 14-23 illustrates the flow for this call scenario, which involves the following sequence of events:

1. Admission Request (ARQ) sent from the H.323 video endpoint to the video gatekeeper.
2. Admission Confirm (ACF) sent from the video gatekeeper to the H.323 video endpoint, specifying Unified CM.
3. H.225 setup sent from the H.323 video endpoint to Unified CM.
4. Dial plan restrictions and digit manipulation performed by Unified CM.
5. Dialed number matches route pattern for H.323 gateway defined for Video Administration.
6. H.225 setup sent from Unified CM to Video Administration.
7. H.225 setup sent from Video Administration to the MCU.
8. Media is established between the MCU and the H.323 video endpoint.

Figure 14-23 Video Call Flow Into Video Administration

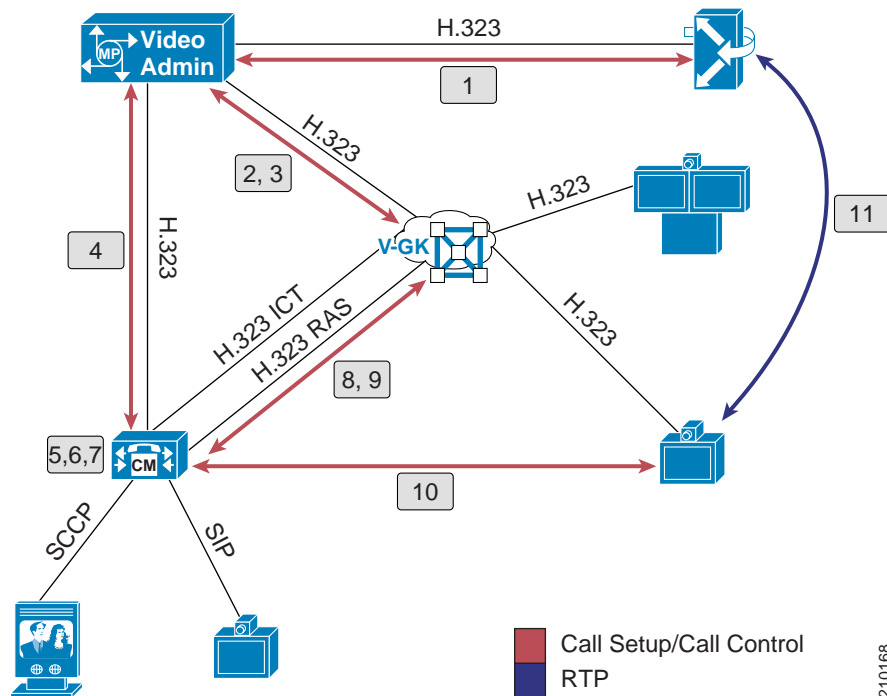


## Outbound Call to an H.323 Video Endpoint

Figure 14-24 illustrates the flow for this call scenario, which involves the following sequence of events:

1. H.225 setup sent from Video Administration to the MCU.
2. Location Request (LRQ) sent from Video Administration to the video gatekeeper.
3. Matches to the intercluster trunk (ICT) and Location Confirm (LCF) sent from the video gatekeeper, specifying Unified CM.
4. H.225 setup sent from Video Administration to Unified CM.
5. Incoming H.225 connection matches H.323 gateway defined for Video Administration.
6. Dial plan restrictions and digit manipulation performed by Unified CM.
7. Dialed number matches H.323 endpoint controlled by Unified CM.
8. Admission Request (ARQ) sent from Unified CM to the video gatekeeper across associated RASAggregator Trunk.
9. Admission Confirm (ACF) sent from the video gatekeeper to Unified CM, specifying the H.323 video endpoint.
10. H.225 setup sent from Unified CM to the H.323 video endpoint.
11. Media is established between the MCU and the H.323 video endpoint.

Figure 14-24 Video Call Flow Out of Video Administration



## Video Dial Plan

With the video component, video participants dial a prefix and meeting ID as a single dialed number. Because of the incorporated meeting ID, this dialed number is unique per conference and can be of fixed length with fixed-length meeting IDs or of variable length with variable-length meeting IDs.

Example:

<i>Video prefix</i>	72
<i>Meeting ID</i>	43221
<i>Dial-in number</i>	7243221

The video dial-in number for the specific meeting is incorporated into the notifications sent to users, the scheduled meeting information in Cisco Unified MeetingPlace Web, and the Connect box within the web collaboration session. Dial-out from the web collaboration session is also available to connect video endpoints.

Fixed-length meeting IDs ensure a fixed-length dialed number. They are very easy to implement from the standpoint of Unified CM, and they have the least impact to users. The use of vanity IDs, however, is not available with this method.

Variable-length meeting IDs become a challenge due to the unknown length of the dialed number. This factor can cause the need for multiple route patterns in Unified CM to accommodate the various possibilities. Some scenarios (detailed in [Variable-Length Meeting IDs, page 14-29](#)) might require the user to wait for inter-digit timeout to occur before the call is placed.

### Fixed-Length Meeting IDs

Restricting meeting IDs to one specific length eliminates issues associated with variable-length meeting IDs and allows for a simple, clean video dial plan implementation. Only one specific route pattern is needed in Unified CM, which will match and process all dialed numbers from video participants immediately.

Example:

<i>Video prefix</i>	72
<i>Meeting ID</i>	43221
<i>Route pattern</i>	72XXXXXX

### Variable-Length Meeting IDs

The following example shows meeting IDs of differing lengths and how they impact route pattern implementation and operation.

<i>Video prefix</i>	72
<i>Meeting ID #1</i>	43221
<i>Meeting ID #2</i>	5256

Multiple exact route patterns:

<i>Pattern 1</i>	72XXXX
<i>Pattern 2</i>	72XXXXXX

With this example, dialing into Meeting 1 (7243221) will connect immediately due to an exact match of Pattern 2, with no other possibilities. Dialing into Meeting 2 (725256) will cause the call to be delayed by inter-digit timeout due to the possibility of another, longer, match. Upon timeout, Pattern 1 is matched and the call is connected.

Universal route pattern:

*Pattern 1*            72!

With a single route pattern for all dialed numbers of any length, the inter-digit timeout must expire for every call placed. This is a simpler implementation because it does not depend on meeting ID length.

In addition, a second pattern can be added with a terminating # to give users the option of terminating the dialed number:

*Pattern 1*            72!

*Pattern 2*            72!#

If the dialed number is terminated by #, the inter-digit timeout is not a factor and the call is processed immediately. Calls not terminated by # will be subject to the inter-digit timeout.



#### Note

Inter-digit timeout is set to 15 seconds by default but can be changed if desired. Changing this value, however, impacts every call processed by that Unified CM cluster. To change the inter-digit timeout, adjust the Cluster Wide CCM Service Parameter, **T302 Timer**.

## Video Redundancy

This section explains some of the limitations of video redundancy and provides best practices for achieving the maximum redundancy possible for Cisco Unified MeetingPlace Video. This section focuses specifically on the video component and does not repeat any of the redundancy information provided previously in this chapter.

## Video Integration Component

The Video Integration component resides on all Cisco Unified MeetingPlace Web servers, but it can be active on only a single server, enabling that server as the web collaboration server for all conferences involving video. No automatic failover mechanisms exist for the Video Integration component. Failure of the supporting server would require manual intervention to configure and enable Video Integration on another server.

## Video Administration

Video Administration is limited to server component redundancy, and it does not have any software-level redundancy. Only one Video Administration server may be implemented per Cisco Unified MeetingPlace deployment. The server on which Video Administration is deployed should contain redundant components to minimize risk of downtime.

## Video Gatekeeper

Video Gatekeeper is no different than a standard gatekeeper with respect to redundancy abilities. In this environment, however, some special considerations must be taken into account. Of the following techniques for gatekeeper redundancy, only HSRP is fully compatible with this environment:

### Gatekeeper HSRP

Redundancy via Hot Standby Router Protocol (HSRP) provides for outbound calling redundancy from Video Administration. If the primary gatekeeper fails, call resolution requests are automatically sent to the backup gatekeeper. Video Administration does not need to know about the backup gatekeeper or primary gatekeeper state to accomplish this failover.

### Gatekeeper Clustering and Alternate Gatekeeper

With the gatekeeper clustering and alternate gatekeeper methods, an issue arises with outbound calls from Video Administration. Outbound calls from Video Administration are sent to the Video Gatekeeper without any registration to that gatekeeper. This prevents Video Administration from being aware of the gatekeeper state and alternate gatekeeper existence. Video Administration will continue blindly to send calls to the failed gatekeeper in this environment.

## Unified CM

Unified CM has three vital connections in the Cisco Unified MeetingPlace Video environment:

- H.323 gateway defined for Video Administration
- Intercluster trunk (ICT) registered to Video Gatekeeper
- RASAggregator Trunk registered to Video Gatekeeper

For the first two, H.323 gateway and ICT, the redundancy technique is fairly simple and straightforward. Only one Video Administration may exist, and Video Gatekeeper should be implemented with HSRP for reasons stated in the redundancy section on [Video Gatekeeper, page 14-31](#).

Placement in a redundancy group (Unified CM group and device pool) for the H.323 gateway and ICT allows node-to-node failover within a cluster and is the extent of redundancy available.

With RASAggregator Trunks, you would configure a redundancy group also, but be careful to ensure proper configuration. Improper configuration can easily lead to call failure. For details, see [Zones and RASAggregator Redundancy Groups with H.323 Video Endpoints on Unified CM, page 14-24](#).

