Cisco Rich Media Conferencing

Conferencing is an essential component of any collaboration system, especially when serving remote users and/or a large user base. Cisco Rich Media Conferencing offers features such as instant, permanent, and scheduled audio and video conferencing, as well as content sharing.

Conference bridges provide the conferencing function. A conference bridge is a resource that joins multiple participants into a single call (audio or video). It can accept any number of connections for a given conference, up to the maximum capacity allowed for a single conference on that device. The output display for a given party shows all connected parties minus the viewer’s own input.

Cisco Rich Media Conferencing solutions utilize various infrastructures to provide audio and video conferencing capability and content sharing. The conferencing infrastructure can be Cisco Unified CM using software or DSP resources, Cisco Meeting Server, or Cisco WebEx Collaboration Cloud, and this chapter covers the design details pertaining to each solution.

Cisco Rich Media Conferencing solutions are available as on-premises, cloud, or hybrid deployments. This allows an organization to integrate with the Collaboration solution in which they have already invested or, alternatively, to implement a service that is hosted "in the cloud." This is one of the more important distinctions between the various solutions, and it is the first decision point when determining which solution is the best fit for an organization.

Cisco WebEx Software as a Service (SaaS) offers a completely off-premises solution, while Cisco Collaboration Meeting Rooms (CMR) Hybrid is a hybrid solution with a mix of on-premises and off-premises equipment. Organizations that have deployed Cisco Collaboration System will benefit most from leveraging an on-premises solution. The later sections of this chapter provide more detailed deployment options for each conferencing solution.

Table 11-1 summarizes available solutions from an on-premises cloud perspective.
To provide a satisfactory end-user experience, careful planning and design should be done when deploying Cisco Conferencing solutions so that users are enabled with the conferencing functionality they require.

To aid in the design, this chapter starts with an introduction of the different types of conferences supported in the Cisco Conferencing solutions, followed by detailed discussions of the following main topics for each solution:

- **Architecture**
  This section introduces the main components of the Conferencing solution and describes its advantages as well as the different conferencing mechanisms available through the various components of a collaboration system. Supported deployment models, solutions, and recommendations are discussed here as well.

- **High availability**
  This section discusses best practices for designing a resilient Cisco Conferencing solution; it also contains guidance for redundancy and load balancing.

- **Capacity planning**
  This section provides best practices and design information related to capacity limits and scalability for the Cisco Conferencing solution.

- **Design considerations**
  This section discusses general recommendations and best practices for the Cisco Conferencing solution design.

This chapter contains discussions on the following Cisco Conferencing solutions:

- Cisco WebEx Software as a Service, (SaaS)
- Cisco WebEx Meetings Server – for private cloud
- Cisco WebEx Meeting Center Video Conferencing
- Cisco Meeting Server
- Cisco Collaboration Meeting Rooms (CMR) Hybrid

| Table 11-1 On-Premises, Cloud, and Hybrid Capabilities of Cisco Collaborative Solutions |
|---------------------------------|--------|--------|--------|--------|
| **Solution**                    | Audio  | Video  | Content Sharing |
|                                 | On-premises | Cloud | On-premises | Cloud | On-premises | Cloud |
| Cisco WebEx Meetings Server     | Yes    | No     | Yes¹      | No    | Yes        | No    |
| Cisco WebEx SaaS                | No     | Yes    | No¹       | Yes¹  | No         | Yes   |
| Cisco Meeting Server            | Yes    | No     | Yes       | No    | Yes        | No    |
| Cisco CMR Hybrid                | Yes    | Yes    | Yes       | Yes   | Yes        | Yes   |
| Cisco WebEx Meeting Center Video Conferencing | No    | Yes    | No       | Yes   | No         | Yes   |

1. Cisco WebEx webcam video only, and no support with standards-based video.
What’s New in This Chapter

This chapter has been updated with new support and updated designs for Cisco Collaboration System Release (CSR) 12.x. You should read this entire chapter before deploying Conferencing in your Cisco Collaboration System.

Table 11-2 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

<table>
<thead>
<tr>
<th>New or Revised Topic</th>
<th>Described in:</th>
<th>Revision Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Collaboration Meeting Rooms (CMR) Premises has been replaced by Cisco Meeting Server</td>
<td>Cisco Meeting Server, page 11-7</td>
<td>March 1, 2018</td>
</tr>
<tr>
<td>Content reorganization and other updates for Cisco Collaboration System Release (CSR) 12.x</td>
<td>Various sections of this chapter</td>
<td>March 1, 2018</td>
</tr>
</tbody>
</table>

Types of Conferences

The Cisco Rich Media Conferencing solution supports the following types of conferences:

- **Instant conference**
  
  An instant audio or video conference (also referred to as an ad hoc conference) is an impromptu conference. Instant conferences are not scheduled or arranged prior to the conference. For example, a point-to-point call escalated to a multipoint conference is considered to be an instant conference.

- **Permanent conference**
  
  Permanent conferences (also referred to as meet-me, static, or rendezvous conferences) are predefined addresses that allow conferencing without previous scheduling. The conference host shares the address with other users, who can call in to that address at any time.
  
  Permanent conference resources are used on a first-come-first-served basis (non-assured). For a guaranteed conference resource (assured), scheduled conferences should be used.

- **Scheduled conference**
  
  A scheduled conference is started by its initiator through a scheduling management system called Cisco TelePresence Management Suite (TMS). Conferences are booked via Cisco TMS with a start and end time and optionally with a predefined set of participants.

Cisco Rich Media Conferencing consists of the conferencing solutions described below. The details pertaining to each solution are described in each individual section that follows.

- **Cisco Unified CM Audio Conferencing, page 11-4**
  
  This solution allows Unified CM to use its internal software component or external hardware digital signal processors (DSPs) as the resources to perform audio conferencing.

- **Cisco Meeting Server, page 11-7**
  
  Cisco Meeting Server is an on-premises video conferencing solution. Each user has a personal Space that can be used to conduct meetings. Users can manage items such as Space creation, adding members to a Space, and PIN creation from the Cisco Meeting App.
Cisco Collaboration Meeting Rooms Hybrid, page 11-49
Cisco CMR Hybrid combines the on-premises video conference and the WebEx Meeting Center conference into a single meeting, which allows TelePresence and WebEx participants to join and share voice, video, and content. CMR Hybrid meetings can be either scheduled or non-scheduled.

Cisco WebEx Meeting Center Video Conferencing, page 11-34
Cisco WebEx Meeting Center Video Conferencing (formerly Cisco Collaboration Meeting Rooms (CMR) Cloud) is an alternate conferencing deployment model that does not require any on-premises conferencing resources or management infrastructure. It supports both scheduled and non-scheduled meetings as well as TelePresence, audio, and WebEx participants in a single call, all hosted in the cloud.

Cisco WebEx Meetings Server, page 11-41
Where cloud-based web and audio conferencing is not suitable, it is possible to use the on-premises WebEx Meetings Server solution. This product offers a standalone audio, video, and collaboration web conferencing platform.

Cisco Unified CM Audio Conferencing
Cisco Unified CM supports audio conferences using any of the following methods:
- Software Audio Conferencing, page 11-4
- Hardware Audio Conferencing, page 11-5
- Built-in Bridge, page 11-5
- Cisco Conference Now, page 11-5

Software Audio Conferencing
The software-based audio conference bridges are provided by the IP Voice Media Streaming Application on Unified CM. The application must be enabled on each individual node in a cluster. A software unicast conference bridge is a standard conference mixer that is capable of mixing G.711 audio streams and Cisco Wideband audio streams. Any combination of Wideband or G.711 a-law and mu-law streams may be connected to the same conference. The number of conferences that can be supported on a given configuration depends on the server where the conference bridge software is running and on what other functionality has been enabled for the application. However, 256 is the maximum number of audio streams for this type. With 256 streams, a software conference media resource can handle 256 users in a single conference, or the software conference media resource can handle up to 64 conferencing resources with four users per conference. If the Cisco IP Voice Media Streaming Application service runs on the same server as the Cisco CallManager Service, a software conference should not exceed the maximum limit of 48 participants.

The Cisco IP Voice Media Streaming Application is a resource that can also be used for several functions, and the design must consider all functions together (see Cisco IP Voice Media Streaming Application, page 7-3). Since the capabilities of the software audio conference bridge are limited, Cisco recommends using a software audio conference bridge only in centralized deployments or in deployments where the use of a G.711 codec is acceptable for instant and meet-me audio conferencing. It is also important to note that the use of a software audio conference bridge in Unified CM will result in a higher load on the system than otherwise would be present.
**Hardware Audio Conferencing**

Digital signal processors (DSPs) that are configured through Cisco IOS as conference resources load firmware into the DSPs that are specific to conferencing functionality only, and these DSPs cannot be used for any other media feature. Any Cisco PVDM hardware may be used simultaneously in a single chassis for voice termination but may not be used simultaneously for other media resource functionality. DSPs on PVDM hardware are configured individually as voice termination, conferencing, media termination, or transcoding, so that DSPs on a single PVDM may be used as different resource types. Allocate DSPs to voice termination first, then to other functionality as needed. The DSP resources for a conference are reserved during configuration, based on the profile attributes and irrespective of how many participants actually join.

Hardware audio conference bridges offer a wider range of capabilities and codec format support than the software conference bridges. Cisco recommends using hardware audio conference bridges where the enterprise requires a more versatile audio conference bridge and codec support for higher-complexity codecs such as G.729 to take advantage of bandwidth savings.

**Built-in Bridge**

Built-in bridge refer to the DSP resources that are hosted by one of the endpoints in the call. Certain Cisco IP Phones have an on-board DSP for the built-in bridge functionality. The IP phone built-in bridge is the only embedded audio resource in the Cisco Rich Media Conferencing architecture. The built-in bridge, however, has limited conference functionality and cannot be used to launch a full conference. The built-in bridge in the Cisco IP Phones allows a user to:

- Join calls across different lines that the IP phone might have, and convert those calls into a conference hosted on the built-in bridge.
- Barge into a call of a different endpoint that shares the line (if the call is not set to private), and convert the call into a conference hosted on the built-in bridge.
- Start a silent recording or monitoring session from the endpoint that is engaged on a call, and fork the media generated and received by the phone invoking the feature.

The built-in bridge of the Cisco IP Phones can encode and decode G.711 and G.729 codec formats. However, once the codec for the call has been selected, the built-in bridge codec selection is locked and the phone will be unable to change the codec used. Therefore, the best practice is to carefully analyze the call flow in which the built-in bridge might be invoked to avoid call drops.

The built-in bridge can mix a maximum of two calls and can fork only one call (two streams).

**Cisco Conference Now**

Cisco Conference Now is a Unified CM native application that provides permanent conference capability similar to Meet-Me. This application is targeted for small business customers who require a basic audio conferencing solution. With Cisco Conference Now, user can simply call into a centralized number and enter the appropriate meeting ID and a host or attendee PIN when prompted by the voice-guided system to join the conference.

Figure 11-1 shows the Cisco Conference Now architecture along with the components involved. Conference Now allows both external and internal callers to join a conference by dialing the Conference Now IVR directory number, which is a centralized conference assistant number. An IVR device is used
to guide and collect information from the caller to join the conference by playing announcements. The IVR is a media resource device that enables Unified CM to play prerecorded announcements (.wav files) to devices such as Cisco IP Phones and gateways.

Figure 11-1  Cisco Conference Now Architecture

The administrator can enable the Conference Now option for a user. If enabled, the user gets a meeting number and must configure a host PIN to start the meeting. Also, an optional attendee access code can be configured for attendees to join the meeting. Prior to the meeting, the conference host distributes the meeting number and the optional access code to all the participants. To start the meeting, the host dials into Conference Now and enters both the meeting number and the host PIN. To join the meeting, the attendees dial into Conference Now and enter the meeting number along with the optional attendee access code. If the attendee dials into the meeting before the host, the attendee will be placed on Music on Hold (MoH). Conference Now uses conference bridges configured in the media resource group (MRG) and media resource group list (MRGL) associated with the host's calling device to perform the conferencing function. Ensure that both the conference bridge and the IVR resources are available to Unified CM in order to use the Conference Now feature.

Using a conference bridge other than the software-based Cisco IP Voice Media Streaming Application (IPVMS) from Unified CM might not provide the conference party entry and exit tone. For the best user experience, we recommend using the software-based Cisco IPVMS conference bridge for Conference Now. For detail on conference party entry and exit tone support, refer to the latest version of the Feature Configuration Guide for Cisco Unified Communications Manager, available at

Consider the following points when implementing Cisco Conference Now:

- The IVR supports Out of Band DTMF only. Use an MTP to convert any DTMF capability mismatch.
- The IVR supports G.711 (a-law and mu-law), G.729, and Wide Band 256K. IPVMS supports G.711 and Wide Band 256K. For other codec support, use a transcoder.
- Conference Now does not support any advanced functionality such as a roster list or muting and un-muting attendees.

Cisco Meeting Server

Cisco Meeting Server utilizes the Cisco on-premises infrastructure to provide business quality video and audio conferences as well as content sharing. Each user in the system can have an always-on personal Space with an associated video address (DN and/or URI) for participants to dial in and join the meeting. Cisco Meeting Server enables rich conferencing collaboration capabilities for endpoints registered to Cisco Unified Communications Manager (Unified CM) or Cisco Expressway as well as the ability to integrate business-to-business audio and video systems and legacy H.323 video systems interworked via Cisco Expressway. This architecture provides a rich feature set by relying on a variety of components in the conferencing solution. The following sections present an overview of those components and their roles in the Cisco Meeting Server conferencing solution.

Architecture

Figure 11-2 illustrates the architecture of the conferencing solution using Cisco Meeting Server. Cisco Meeting Server provides and manages conference resources; Cisco TelePresence Management Suite (TMS) provides the provisioning and scheduling functions for the conference resources; Cisco Meeting Management provides the meeting control and management functions; and Cisco Unified Communications Manager (Unified CM) is the call control system. Alternatively, Cisco Expressway can be used in place of Cisco Unified CM as the call control system. Cisco Meeting Server supports SIP call control only but can use Cisco Expressway to interwork with legacy H.323 video systems. Cisco Meeting Server is the conference bridge that supports all conference types, and it connects with Unified CM via a SIP trunk.

Cisco Unified CM communicates with Cisco Meeting Server using XML-RPC over HTTPS to control the conference bridges for instant conferences. Cisco TMS uses the REST API connections to link the Cisco Meeting Server to provision and schedule conference resources. Cisco Meeting Management has two interfaces with Cisco Meeting Server: REST API and Call Detail Record (CDR). The REST API interface is used to perform operations on Cisco Meeting Server, while the CDR interface is used to receive call events from Cisco Meeting Server.
The scheduling architecture consists of an active and a passive node for both Cisco TMS and TelePresence Management Suite Extension for Microsoft Exchange (TMSXE), which are deployed behind a network load balancer. The active node processes the incoming requests, while the passive node runs in standby mode with its web pages and services locked down and refusing all incoming traffic. For large deployments, Cisco TMS and TMSXE must be installed on separate virtual machines, as indicated in Figure 11-3. Cisco TMS servers are installed in the customer data center that also hosts the organization's SQL deployment. All the server nodes function from an external Microsoft SQL database. Additionally, endpoints, Cisco Meeting Server, and Unified CM make up the complete conference components for scheduling.
Cisco Meeting Management runs on a separate server outside of Cisco Meeting Server and is dedicated to the Cisco Meeting Server deployment only. As mentioned previously, Cisco Meeting Management uses the REST API link to perform operations on Cisco Meeting Server. Cisco Meeting Management uses the CDR interface to receive call-related events from Cisco Meeting Server so that it knows when a meeting has started or ended, along with other call activities. When users log into the portal, they are authenticated against the LDAP directory. In addition, Cisco Meeting Management uses the groups configured inside the directory to determine the user’s role (video operator or administrator). Based on the user’s role, different options will be available on the Cisco Meeting Management portal. (See Figure 11-4.)

Note
Cisco Meeting Server 2.1.5 is the minimum version required to deploy Cisco Meeting Management, but version 2.2 or later is recommended.
Role of Cisco Meeting Server

Figure 11-5 illustrates the core conferencing components of Cisco Meeting Server that provide video conferencing capability. The call bridge component integrates with Cisco Unified CM for call control and provides resources to perform conference functions. All Cisco Meeting Server conferences are hosted on the Spaces. Spaces are virtual meeting rooms that have audio, video, and content sharing capability and are accessible using the Space URI or directory number. Cisco Meeting Server must integrate with a directory server such as Microsoft Active Directory to import users into the system. During the import process, Spaces are created using the field mapping expressions configuration. All the information for users and Spaces is stored in the database. Participants can join conferences using Cisco or third-party standard SIP video endpoints, Cisco Jabber clients, or the Cisco Meeting App. The XMPP server authenticates users logging in through the Cisco Meeting App. The Web Bridge connects WebRTC client users to the call bridge after they log in.
Cisco Meeting App is the client to Cisco Meeting Server, and it can be a native desktop or mobile application or a WebRTC browser application. With Cisco Meeting App, users can log in and join the conference with audio and video along with content sharing. With the WebRTC client, users without an account on Cisco Meeting Server can use a compatible browser to join the conference as a guest. In addition, users can use Cisco Meeting App to run their meetings and perform actions such as viewing participants, muting and/or removing participants, starting and stopping recording, as well as creating and editing their own Spaces.

**Note**

**Note**
Using Cisco Meeting Server for conferences has several benefits, including:

- Scaling easily for small or large deployments, allowing capacity to be added incrementally as needed
- Simplified, intuitive, and optimal conference experiences across all device types
- Unrestricted number of participants in a meeting, up to the limit of available underlying hardware when using multiparty licensing
- Single deployment model for all conference types

**Role of Cisco TelePresence Management Suite (TMS)**

Cisco TelePresence Management Suite (TMS) provides conference scheduling as well as conference room system reservations. Cisco Unified CM maintains the configuration control for endpoints, and Cisco TMS is then able to push the calendar information to those endpoints. Administrators are able to set the parameters for the default conference for their organization, and then individual conferences can be created according to this template.

**Role of Cisco TelePresence Management Suite Extension for Microsoft Exchange (TM SXE)**

When end users schedule a meeting in Microsoft Outlook with multiple conference room resources, the Exchange Web Services (EWS) feature of Microsoft Exchange synchronizes that event with Cisco TMS as a scheduled conference. This synchronization is bidirectional, allowing an administrator or support staff to update meetings as well without the need to access the meeting organizer's Outlook event. All endpoint resources within the organization that are intended to be in the conference must be listed in a single Microsoft Exchange meeting request.

**Role of Cisco Meeting Management**

Cisco Meeting Management is a standalone tool that does not require Cisco TMS, but together with Cisco TMS they provide the complete management functions for Cisco Meeting Server. Cisco Meeting Management has the Meeting Manager that can provide white glove service for customers. The Meeting Manager lists all active meetings, with full details on each meeting. Within a particular meeting, it lists all participants in the meeting and can start/stop recording or streaming, change layout, add/drop participants, and end the meeting. For an individual participant, it can mute/unmute audio/video, change layout, and display call statistics.

**Cisco Meeting Server Edge**

Cisco Meeting Server Edge allows external users to join conferences from the Internet utilizing Cisco Meeting App. In this deployment, the external users interact with the edge software components that in turn communicate with the core software components. Edge components reside in the DMZ while core components reside within the enterprise network. When an external user connects, the call is routed to the edge components and then the core components. There are two options for deploying the edge components: single combined deployment (Figure 11-6) and single split deployment (Figure 11-7).

In a single combined deployment, the edge and core components are deployed inside the same server. However, the edge components are put into the DMZ network while the core components are put into the enterprise network inside the firewall. In a single split deployment, the edge and core components...
are split into two different servers. The edge components are deployed on the server residing physically in the DMZ while the core components are deployed on a separate server residing inside the firewall in the enterprise.

**Figure 11-6  Single Combined Deployment**

External users using WebRTC clients connect directly to the Web Bridge in the DMZ. The TURN Server provides firewall media traversal technology that allows Cisco Meeting Server to be deployed behind a firewall or NAT. TURN is included with Cisco Meeting Server deployments without an additional license.

**Figure 11-7  Single Split Deployment**

External users using WebRTC clients connect directly to the Web Bridge in the DMZ. The TURN Server provides firewall media traversal technology that allows Cisco Meeting Server to be deployed behind a firewall or NAT. TURN is included with Cisco Meeting Server deployments without an additional license.
The Load Balancer provides a single point of contact for external Cisco Meeting App in the split deployment. It listens on an external interface and port for incoming connections. Also, the Load Balancer accepts incoming TLS connections from XMPP server, over which it can multiplex TCP connections from external clients. Thus, this creates a TLS trunk between the core and the edge components. The Load Balancer also does not require an additional license but it does require an enabled Call Bridge.

For more details on single combined deployments and single split deployments, refer to the respective deployment guides available at


Starting with Cisco Meeting Server 2.1.2 and Cisco Expressway X8.10, external users using a WebRTC client can connect to Cisco Meeting Server over Expressway. For deployment details, refer to the latest version of the Cisco Expressway Web Proxy for Cisco Meeting Server deployment guide, available at


Conference Call Flows

Cisco Unified CM provides device registration and routing of voice and video calls between the connected endpoints. Permanent, instant, and scheduled conference calls are all routed over a single SIP trunk to the call bridge on Cisco Meeting Server. Each call bridge requires a separate SIP trunk. An HTTPS connection is configured on the Unified CM node that carries the XML-RPC requests to the Cisco Meeting Server nodes for instant conferences (see Figure 11-8). When users press the conference softkey on their device to escalate a two-party call to a three-party call, Unified CM sends an API request to Cisco Meeting Server to create a temporary Space for hosting the conference via this HTTPS connection. Instant, permanent, and scheduled conferences are hosted on Spaces that are created by various components.

**Figure 11-8 Cisco Unified CM and Cisco Meeting Server SIP Trunk**
Instant call flows that are managed by Unified CM cannot be used to add participants to conferences created by any other method, such as scheduled conferences. Also, other call flows cannot be used to add participants to instant conferences. The instant call escalation method is supported only in an instant conference that was created by it, and conferences generated by other methods cannot be extended by the instant mechanism. This avoids any potential for chained conferences.

**Instant Conferences**

Instant conferences allow endpoints engaged in a two-party point-to-point call to be escalated to a three-party multipoint call using Unified CM conference bridge resources. Instant conferences use an HTTPS XML-RPC connection associated with the SIP trunk between Unified CM and the call bridge on Cisco Meeting Server. When a user presses the conference softkey to initiate an instant conference, Unified CM issues an API request through the HTTPS connection to create a temporary Space on Cisco Meeting Server. When the conference ends, Unified CM issues another API request to delete that Space from Cisco Meeting Server. Figure 11-9 illustrates an example of how an instant conference is initiated using Cisco Meeting Server.

**Figure 11-9  Initiation of an Instant Conference using Cisco Meeting Server**

Endpoint 1 places 2 on hold and calls to 3. After the call to 3 is complete, endpoint 1 joins both calls; this redirects all endpoints to the call bridge in Cisco Meeting Server. Resource allocation is on a first-come-first-served basis.

**Permanent Conferences with Cisco Meeting Server Spaces**

Permanent conferences are deployed using Cisco Meeting Server Spaces. Spaces provide a permanent-type conference and are created as part of the process of importing users from LDAP. Each Space has an associated video address (URI and/or DN) that users utilize to join the meeting. Administrators can specify the Space's attributes (for example, name, username, URIs, and so forth) through the field mappings so that the Spaces can be created using those mappings. Users can then log
in using Cisco Meeting App and add members to their Space. Also, users can log into Cisco Meeting App to create additional Spaces and add members. This conference type requires a SIP trunk between Unified CM and the call bridge on Cisco Meeting Server.

Permanent conferences can be initiated in several ways depending on the call control used by the conference initiator: IVR dial-in and preconfigured video address. Figure 11-10 illustrates an example of a permanent conference taking place by dialing a video address.

The permanent video address for a conference is always available after it has been preconfigured by the administrator, and the user can dial the video address to start or join the conference.

Figure 11-10 Example of a Permanent Conference

Conference organizer must communicate the dial-in number to all participants for a permanent conference.

Participants dial in from their respective endpoints. Shared resources may be supporting other conferences at the same time. Resource allocation is on a first-come-first-served basis.

Alternatively, users can dial in to the conferences via the Cisco Meeting Server built-in interactive voice response (IVR). Then, the IVR will prompt the users for the conference ID and the password (if one is configured) of the conference they want to join.

Scheduled Conferences

Cisco Meeting Server supports scheduling conferences with Cisco TMS. Scheduled conferences require a SIP trunk between Unified CM and the call bridge on Cisco Meeting Server. Unified CM routes the scheduled conference participants to the destination of the SIP trunk. Add Cisco Meeting Server to Cisco TMS to allow for issuing REST API requests on Cisco Meeting Server through the HTTPS connection. After the administrator configures a range of numeric IDs for scheduled conferences, Cisco TMS creates an inactive Space on Cisco Meeting Server for each numeric ID via the API link. Cisco TMS then randomly chooses a dial-in number from the range when an organizer schedules a meeting. When it is time to start the scheduled meeting, Cisco TMS activates the Space using the API so that the participants can join. Scheduled conferences can be joined in a variety of ways, as Table 11-3 describes.
Scheduling attempts to ensure endpoint and port resource availability and provides convenient methods to connect to the conferences. Most organizations already use calendaring applications to schedule conferences. In this case, calendar integration enables users to schedule conferences with their existing calendar client. TelePresence deployments often include a large quantity of endpoints and various infrastructure components. Without centralized management, component provisioning and resource allocation are difficult if not impossible. Management platforms greatly simplify these processes.

Scheduled meetings work by integrating conference resources and endpoints with corporate calendaring applications (see Figure 11-11). Cisco TelePresence Management Suite (TMS) resides between endpoints and calendaring applications to locate the proper bridge resource for each scheduled conference. Cisco recommends deploying scheduled conferencing with the TelePresence Management Suite and creating conferences by scheduling three or more endpoints.

### Table 11-3 Call Launch Options for Scheduled Conferences

<table>
<thead>
<tr>
<th>Launch Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Button to Push (OBTP)</td>
<td>- Conference dial-in information is automatically displayed on endpoints that support OBTP. For systems that do not support OBTP, an email with conference information is sent to the conference owner to forward to the participants.</td>
</tr>
<tr>
<td>Automatic Connect</td>
<td>- All endpoints are automatically connected at the specified date and time.</td>
</tr>
<tr>
<td>Manual Connect</td>
<td>- The conference cannot begin until a specific endpoint (usually the conference organizer’s endpoint) connects. After this endpoint connects, the remaining endpoints are either connected automatically or allowed to dial in manually.</td>
</tr>
<tr>
<td>Reservation</td>
<td>- This method reserves the endpoints but does not initiate any connections.</td>
</tr>
</tbody>
</table>

Scheduled Conference Using Integration with a Calendaring Application

Conference organizer schedules 3 or more endpoints. Cisco TMS allocates resource through Cisco Meeting Server to host and create a conference that will last between the scheduled start and stop times. Media (Video and Audio)
Cisco Unified CM supports secure conferencing with Cisco Meeting Server by using secure SIP trunks between them. With secure conferencing, Unified CM uses TLS for call signaling and SRTP for media payload encryption. However, the entire conference is secure only if all the participants’ endpoints support video encryption. The API interface between Cisco Unified CM and Cisco Meeting Server must be encrypted, and therefore HTTPS must be used for this.

Note
Cisco Meeting Server 2.3 and later releases use TLS version 1.2 for all connections by default.

Cisco Meeting Server uses secure connections to communicate with external components as well as between internal components, and certificates are required. Both self-signed and certificate authority (CA) signed certificates are supported, but CA signed certificates are recommended in the deployment. For details on certificates deployment and requirements, refer to the latest version of Cisco Meeting Server Certificate Guidelines document, available at https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html

Another level of security can be added to restrict access to the conferences themselves with PINs or passwords. Any scheduled conference or permanent conference can have a PIN set so that all participants are challenged to enter the PIN before being allowed to connect.

For more information about secure conferencing, see the chapter on Cisco Collaboration Security, page 4-1.

High Availability for Conferencing

High availability must be considered at several levels with the conferencing solution and is achieved in different ways depending on the service being considered.

For both scheduled and non-scheduled conferences, high availability involves Cisco Unified CM, Cisco Meeting Server, and Cisco TMS.

Cisco Unified CM High Availability

To provide conference services with high availability, the link between Cisco Meeting Server and Cisco Unified CM must be redundant so that, if the link to one Cisco Meeting Server node goes down, the backup link can provide the services. These links include media resource groups and lists for instant conferences, and route groups and route lists for routing calls to Cisco Meeting Server.

Media Resource Groups and Lists

When a user of a Cisco Collaboration endpoint that uses Cisco Unified CM as its call control activates the CONF softkey, Unified CM uses the Media Resource Manager to select conference bridges. Conference bridge resources are configured in the media resource groups (MRGs). The media resource group lists (MRGLs) specify a prioritized list of MRGs and can be associated with the endpoints. The Media Resource Manager uses MRGLs of the endpoints to select the conference bridge. How you group
the resources is completely at your discretion, but Cisco recommends grouping the resources by using a logical model of the geographical placement whenever possible so that all endpoints at a given site use the conference bridges closest to them.

Cisco Unified CM selects conference bridges based on the following criteria, in the order listed here:

1. The priority order in which the media resource groups (MRGs) are listed in the media resource group list (MRGL)
2. Within the selected MRG, the resource that has been used the least

For further information about media resource design, see the chapter on Media Resources, page 7-1.

Route Groups and Lists

Route lists and route groups are common call routing mechanisms of reliability for calls that leave the Cisco Unified CM domain. For media resources integrated with Cisco Unified CM as a trunk, route lists and route groups should be used to achieve high availability if backup conference bridges exist. Call admission control can be preserved by setting the locations of the media resources based on the trunk being used for the call.

To learn more about route list and route group resiliency mechanisms, see the chapter on Dial Plan, page 14-1.

Cisco Meeting Server High Availability

Deploying additional instances of components on one or more servers can provide resiliency for Cisco Meeting Server so that the component instances can share the load, and if one of them fails, the backup instance would pick up the load. In addition, XMPP servers, call bridges, and databases can be clustered together to operate as a single instance, as shown in Figure 11-12.

Figure 11-12  Minimum Configuration for Cisco Meeting Server Cluster with High Availability
A standard Cisco Meeting Server cluster consists of two or more (up to 8) nodes with call bridge service enabled. Maximum round trip time (RTT) between nodes is 300 ms. Call bridge cluster peers are connected to each other in full mesh via the distribution link. This link is an HTTPS connection used for passing call signaling and control status messages between nodes. Calls can be sent to any nodes in the cluster. If one node goes down, Unified CM can route calls to the remaining call bridge nodes to join the conferences. In the event that a call bridge fails during a live conference, those calls will be dropped and participants will need to dial the same number to join the conference on a new call bridge. Using the Unified CM route group and route list construct, calls can be distributed through the SIP trunks to Cisco Meeting Server.

The database cluster consists of one master and multiple slaves, up to a maximum of 5 nodes with maximum RTT of 200 ms between nodes. The database master can perform both read and write operations, while slaves can only read. Call bridges always connect to the database master for read and write operations, and all changes made on the master are replicated to the slaves. Call bridges with a local database automatically connect to the master of the local database cluster, while call bridges with no local database have to be connected manually to the database cluster. If the master fails, one of the slaves will become the new master, and other slaves will re-register with this new master. After correcting the failure, the old master will become the slave and register with the new master. In cases where a network partition occurs, only database nodes that can see more than half of the cluster members are considered for promotion to become a master. Likewise, any existing master that cannot see more than half of the cluster members will be demoted to a slave. This ensures that multiple masters are not created. Thus, if a database cluster consists of an even number (2 or 4) of nodes and the network is partitioned into 2 segments with an equal number of nodes on each segment, the master on one side will be demoted to a slave because it cannot see more than half of the cluster members. In that case, there will be no master in the cluster, and the call bridges can still take calls but no database write operations will be possible. For this reason, we recommend having an odd number of nodes in the database cluster to ensure that a master is always elected. As a result, the minimum number of database nodes in a cluster is 3.

XMPP resiliency provides failover protection for a client that is unable to reach a specific XMPP server. The XMPP server cluster must be configured using an odd number of XMPP server nodes, with a minimum of 3 nodes. This is due to the master election algorithm requirement that more than half of the cluster nodes should be available in order for Cisco Meeting Server to elect an XMPP server master. If no XMPP server master is available in the cluster, Cisco Meeting App users cannot log in. Each XMPP server knows the location of the others, with links established between them. They use keep-alive messages to monitor each other and elect a master. XMPP messages can be sent to any server and are forwarded to the master XMPP server. If the master fails, a new master is elected and the other XMPP servers will forward messages to the new master. The call bridge uses the DNS SRV record (_xmpp-component) to connect with an available XMPP server based on the configured priority and weight with the SRV record. A call bridge connects to one XMPP server at a time. If a network problem results in the call bridge losing connection to the XMPP server, the call bridge will attempt to reconnect to another XMPP server. All call bridges must be configured inside each XMPP server.

Figure 11-12 illustrates the minimum configuration for a Cisco Meeting Server cluster with high availability. In this configuration, a minimum of 3 servers is required to host 3 instances of the database and XMPP servers. Enable at least 2 instances of each component service (Web Bridge and Call Bridge) in separate servers, and put the call bridges into a group. There is no need to activate all services inside each server; activate only the ones that are required. If the deployment requires more capacity than the two call bridges can handle, additional call bridge can be set up in the third server (no need to acquire a fourth server for just the call bridge).
Cisco TMS High Availability

High availability of a large Cisco TMS deployment includes two TMS front-end servers, two servers running TMSXE, a network load balancer, and an external Microsoft SQL database (see Figure 11-3). TMS resiliency supports only two servers (one active node and one passive node), and this model does not increase or decrease the capacity of the TMS deployment. The network load balancer (NLB) is deployed in front of the TMS servers. Inbound traffic to TMS goes through the NLB, which forwards it to the active node. Outbound traffic from TMS is sent directly to the destination without going through the NLB. If the NLB detects a failure on the existing active node, it automatically switches to the new active node without any user intervention.

Cisco Meeting Management High Availability

Cisco Meeting Management does not have the built-in cluster functionality to provide resiliency. However, if customers want to have high availability, they can configure two individual Cisco Meeting Management instances with exactly the same configuration managing the same Cisco Meeting Server instance(s), and they can then put a network load balancer in front of the two Cisco Meeting Management instances. Users can then connect to the Cisco Meeting Management portal through the load balancer. The load balancer configuration and availability of the Cisco Meeting Management server will determine which one of the Cisco Meeting Management servers will be used.

Scaling the Conferencing Solution

The conferencing solution can be scaled by adding more call bridges (up to 8) to a standard Cisco Meeting Server cluster.

In this deployment, based on the dial plan and route group and route list configuration with the SIP trunks in Unified CM, calls can be routed to any call bridge within the cluster. If calls for the same conference are routed to different call bridges, the audio and video of the last 4 active speakers are exchanged between call bridges so that participants on one bridge can see the active speakers on the other bridge.

Note: Cisco Meeting Server supports clustering with more than 8 call bridges, but deployment requires prior approval by Cisco. Contact your local Cisco account team for details.

Each call bridge can support 450 participants. Thus, the maximum number of participants per conference is 450 with a single server, and up to 2,600 participants can be supported across multiple servers in a single cluster. Additional scalability information can be found in the latest version of Cisco Meeting Server and Cisco Meeting App Data Sheet, available at


Using call bridge groups, a Cisco Meeting Server cluster can intelligently load balance calls across the call bridges within the same location or across nodes in different locations to increase the scale within a deployment. The intelligent decision making to determine where calls end up is handled by Cisco Meeting Servers. The call control system needs to be able to handle the SIP messages from Cisco Meeting Servers in order to move calls to the correct location. Call bridges that are configured as a cluster can be put into one or more call bridge groups. For call bridges within the group, Cisco Meeting Server intelligently load balances calls across them and sends calls for the same conference to the same call bridge whenever possible in order to minimize the creation of distribution links between call bridges.
For inbound SIP calls to a call bridge, Cisco Meeting Server decides to reject or accept the call based on the current load in the call bridge. If the current load is less than the preset threshold, the call will be accepted. Otherwise, the call will be rejected and Unified CM will reroute the call to another call bridge in the call bridge group using the dial plan configuration. If Unified CM cannot find any call bridge that accepts the call, the whole call will be rejected. After a Cisco Meeting Server accepts the call, the call could be hosted on the call bridge of this Cisco Meeting Server or moved to another call bridge with highest priority according to an internal ordered list for the conference. When the call is moved, the target Cisco Meeting Server with the call bridge enabled sends an INVITE with Replaces to Unified CM to take over the call. By default, a call bridge in a call bridge group will reject all calls for new participants at 80% load, and only new distribution calls will be allowed.

For outbound SIP calls, Cisco Meeting Server uses the outbound dial rule to locate the highest priority rule that matches the domain, and it load balances the call using a call bridge group. If the rule applies to a local call bridge, calls will be load balanced using the local call bridge group. Otherwise, calls will be load balanced using the call bridge group where the remote call bridge is a member. Also, for an outbound call made using an API, a call bridge group or a call bridge can be specified as a parameter. For a call bridge group, the call is load balanced among the call bridges within that group. For a call bridge, the call is made using that call bridge.

For Cisco Meeting App (including WebRTC) clients, users can join the conference as members of the Space, as non-members of the Space with accounts on Cisco Meeting Server, or as guests. When a user is added as a member to the Space via an API, a call bridge group or a call bridge can be specified as a parameter. For a call bridge group, when the Cisco Meeting App user joins the meeting, the call will be load balanced using that group. For a call bridge, when the Cisco Meeting App user joins the meeting, the call will be handled by that call bridge. When the user is not a Space member or is a guest that joins the meeting via Cisco Meeting App, the first call bridge that the user connects to is determined. If that call bridge is part of a call bridge group, then the call is load balanced using that group. In order to load balance Cisco Meeting App calls, ensure that each call bridge in the call bridge group has a connection to the XMPP cluster or to a single XMPP server.

There are some network requirements that must be satisfied in order to successfully move calls between call bridges within the call bridge group. The maximum RTT should be 100 ms between call bridges inside the group and 300 ms between any two call bridges within the cluster.

For setup and deployment details for call bridge groups, refer to the latest version of the white paper on Load Balancing Calls Across Cisco Meeting Servers, available at:


Note

If call bridge groups and load balancing are not used, then calls will not be rejected but the quality of all calls will be reduced when the load limit is reached. If this happens often, we recommend deploying additional hardware.

Considerations for Multiple Unified CM Clusters

For large deployments with multiple Cisco Unified CM clusters, use a single Cisco Meeting Server cluster configured with multiple call bridge groups, and dedicate one group to each Unified CM cluster. For example, if your deployment has three Unified CM clusters, then you should deploy a single Cisco Meeting Server cluster with three call bridge groups, one for each Unified CM cluster. Each Unified CM cluster should have a SIP trunk to each call bridge in its local call bridge group. All incoming conference calls to a Unified CM cluster will be handled by the local call bridge group. Call bridges should have their distribution links connected to their peers inside and outside of the groups in full mesh. For the
same conference, users can dial in from their Unified CM cluster to reach the local call bridge group, and the call bridges in different groups will exchange the audio and video of the last 4 active speakers with their peers so that participants can see each other across the bridges. (See Figure 11-13.)

Figure 11-13  Cisco Meeting Server Deployment with Multiple Unified CM Clusters

The following guidelines apply when expanding the Cisco Meeting Server cluster into different regions for multiple Unified CM clusters:

- A single Cisco Meeting Server cluster should be used for deployment of one or more Cisco Unified CM clusters.
- You may deploy up to 8 call bridges for the standard Cisco Meeting Server cluster. If the cluster exceeds 8 call bridges, acquire Cisco account team approval before deployment.
- Deploy a maximum of 5 databases and an odd number of nodes in the Cisco Meeting Server cluster.
- Deploy an odd number of XMPP service nodes in the Cisco Meeting Server cluster.
- Round-trip-time (RTT) network requirements:
  - Maximum of 300 ms between call bridges and 200 ms between databases in the Cisco Meeting Server cluster
  - Maximum of 100 ms between call bridges inside the group
Cisco Meeting Server supports both Multiparty licensing and Cisco Meeting Server Capacity Units, but Multiparty licensing is recommended. Multiparty is a user-based licensing model, and it should be applied to every node that has the call bridge enabled. It comes with two variations: Personal and Shared. Personal Multiparty Plus (PMP+) is for specific named hosts, while Shared Multiparty Plus (SMP+) is for conference room systems or for sharing between users. By default, all users in the system use Shared Multiparty Plus (SMP+); and if Personal Multiparty Plus (PMP+) is desired, PMP+ should be assigned to users via the Cisco Meeting Server API. Each license entitles a user to host a conference with unlimited participants and up to 1080p video resolution. Table 11-4 summarizes the features included in the Personal and Shared Multiparty licenses.


Cisco Meeting Management does not require any additional license for Cisco Meeting Server customers, and it can be downloaded from https://www.cisco.com.

### Table 11-4  Cisco Personal and Shared Multiparty Plus License Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Personal Multiparty Plus (PMP+)</th>
<th>Shared Multiparty Plus (SMP+)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tied to a named host</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Availability</td>
<td>Included in Cisco UWL Meeting</td>
<td>A la carte or discounted with room system</td>
</tr>
<tr>
<td>Minimum order</td>
<td>25</td>
<td>1</td>
</tr>
<tr>
<td>Maximum conference size</td>
<td>Unrestricted, within the limit of available hardware capacity</td>
<td></td>
</tr>
<tr>
<td>Maximum resolution</td>
<td>1080p60 (full HD) for video and 1080p30 for content on single-screen or multi-screen endpoints</td>
<td></td>
</tr>
<tr>
<td>Rich media sessions for business-to-business or business-to-customer</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Cisco TMS, TMSXE, and Skype for Business and Lync Interoperability Licenses</td>
<td>Included</td>
<td>New customers buy with Starter Pack¹</td>
</tr>
<tr>
<td>Support for instant, permanent, and scheduled conferences</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

¹ If only the Cisco TMS and related product licenses are required, a TMS Starter Pack can be purchased.
Capacity Planning

The capacity of Cisco Meeting Server depends on the platform of choice and the number of conferencing nodes running in the deployment. The main purpose of sizing a deployment is to determine the number of required concurrent connections to the Cisco Meeting Servers. Considerations include:

- Geographical location — Each region served by Cisco Unified CM should have dedicated conferencing resources. For example, there could be one central location for the US where Unified CM, Cisco Meeting Servers, and other servers are installed, and one central location for EMEA.
- Preference for Cisco Meeting Server platforms — Virtualized or appliance
- Type of conferences — Audio and/or video; scheduled and/or non-scheduled
- Conference video resolutions — Higher quality conferences use more resources.
- Large conference requirements — For example, all-hands meetings

Conference resources are generally dedicated to a region in order to keep as much of the conference media as possible on the regional network; therefore, sizing can be considered on a region-by-region basis. To properly size the conferencing deployment, use the Cisco Collaboration Sizing Tool, available (with a valid login account) at https://cucst.cloudapps.cisco.com.

Consult with your Cisco sales representative for assistance on sizing the conferencing resources for your particular environment.

For additional sizing details, see the section on Collaborative Conferencing, page 25-44.

Depending on the Cisco Meeting Server platform types and the number of Cisco Meeting Server clusters to be managed by Cisco Meeting Management, different deployment size will be required. For details, refer to the latest Cisco Meeting Management release notes, available at https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-release-notes-list.html
Design Considerations

In summary, consider the following recommendations when deploying Cisco Meeting Server:

- Use Multiparty Licensing (PMP+ and/or SMP+) for Cisco Meeting Server deployments.
- Cisco Meeting Server deployments require certificates to secure both internal and external connections and should use the CA signed certificates.
- The Cisco Meeting Server cluster supports up to 8 nodes with call bridges. More than 8 nodes (up to 24) can be deployed, but this requires Cisco approval before deployment.
- When the deployment involves clustering the database or XMPP service, a minimum of 3 databases or XMPP nodes is required due to the master selection algorithm requirement for clustering.
- In a large distributed Cisco Meeting Server deployment, use call bridge groups to group the call bridges together within the region to minimize the creation of distributed links between call bridges.
- Network requirements for Cisco Meeting Server cluster deployment are 300 ms between call bridges, 200 ms between databases, and 100 ms between call bridges inside a call bridge group.
- Cisco TelePresence Management Suite (TMS) provides conference scheduling and endpoint management, while Cisco Meeting Management provides meeting management. These two applications provide the complete management solution for Cisco Meeting Server.
- Cisco Meeting Management can be deployed without an extra license, but it requires a separate server from Cisco Meeting Server.

Cisco WebEx Software as a Service

Cisco WebEx is a collaborative conferencing solution that does not require any hardware to be deployed on-site. All services (audio, video, and content sharing) are hosted in the Internet through the Cisco WebEx Collaboration Cloud. This is often referred to as software-as-a-service (SaaS). Meetings can be initiated and attended from anywhere, anytime, on any device, and do not require connectivity back into the enterprise apart from an Internet connection. This section describes solution characteristics and provides design guidance for deploying WebEx SaaS.

Architecture

Cisco WebEx SaaS utilizes the Cisco WebEx Collaboration Cloud to deliver the conferencing solution to the customers. The Cisco WebEx Collaboration Cloud is a global network created with a carrier-class information switching architecture, and only Cisco Collaboration traffic flows over this network. Figure 11-14 shows the Cisco WebEx Collaboration Cloud architecture.
This network is purpose-built for real-time communications and has been specially formulated to minimize latency associated with TCP-layer flows. The network consists of application-specific multimedia switches at key peering points to handle rapid session traffic and to guarantee a high quality of service for WebEx meetings. These switches are housed in highly secure Cisco data centers interconnected via dedicated lines that circumvent the public internet. These data centers are located near the major internet access points to route meeting traffic around the globe securely and reliably. In addition to these large data centers housing major meeting nodes, Cisco deploys nodes around the world. The network is built on fully redundant clusters with Global Site Backup. These services and other facilities form part of the Cisco WebEx Collaboration Cloud Operational Support System.

Users can connect to a WebEx meeting using the meeting application running on a computer or mobile device or even an HTML5 browser-based web application. Once the connection is established, the WebEx Collaboration Cloud manages all synchronous real-time interactions that make up a WebEx meeting, as depicted in Figure 11-14. Users access WebEx applications via browsers through the WebEx Collaboration Cloud, which resides within the Web Zone. The Applications Program Interface (API) ties the WebEx applications to the switching platform in the Meeting Zone within the WebEx Collaboration Cloud core. Numerous clusters of interconnected and distributed collaboration switches, their associated databases, and the logical and physical network infrastructure make up the WebEx Collaboration Cloud core. Multi-layer security components and the WebEx Operational Support System encircle the network with an additional layer of protection.

The WebEx Collaboration Cloud delivers real-time traffic reliably using intelligent routing, Global Site Backup (GSB), and Global Server Load Balancing (GSLB). Based on the geographic location of WebEx meeting participants, the WebEx Collaboration Cloud determines the point of presence that offers the lowest latency and best performance. WebEx meeting hosts automatically get a backup site physically located in a geographically distant Cisco data center within the same region. In the unlikely event that the primary WebEx site becomes unavailable, GSB automatically switches all meeting activity to the...
backup site. GSLB is a load-balancing design that directs traffic to the least congested switch in the WebEx Collaboration Cloud in order to minimize the delays. Thus, if one meeting switch has congestion, traffic is directed to an alternate switch, resulting in faster screen updates and synchronization among participants, and a better meeting experience.

In the WebEx deployment model shown in Figure 11-15, all the content, voice, and video traffic from every client traverses the internet and is mixed and managed in the cloud at the WebEx data center. The WebEx data center is logically divided into the Meeting Zone and the Web Zone. The Web Zone is responsible for things that happen before and after a web meeting. It incorporates tasks such as scheduling, user management, billing, reporting, and streaming recordings. The Meeting Zone is responsible for switching the actual meeting once it is in progress between the endpoints.

![WebEx Deployment Diagram](image)

The Meeting Zone consists of two subsystems. Within the Meeting Zone there are collaboration bridges that switch meeting content. The multimedia platform is responsible for mixing all of the VoIP and video streams within a meeting. To join a WebEx session, an attendee first connects to the Web Zone. The Web Zone traffic flows only before or after the meeting, is relatively low bandwidth, and is mainly non-real time. The real-time meeting content share flows to and from the Meeting Zone and can be bandwidth intensive. Its real-time nature can place a heavy burden on enterprise access infrastructure. For further details regarding network traffic planning, see Capacity Planning, page 11-33.
Meeting Center uses the H.264 AVC/SVC codec to provide high-definition video for the conference. Higher network bandwidth is needed for those deployments. For further details regarding network traffic optimization for high-definition video, see Capacity Planning, page 11-33.

Each WebEx Meeting Center host has a Personal Room with a fixed customizable URL. The host can use his room to conduct meetings, and participants can enter the room using that fixed URL. Lobby management functions are available to the host, such as maintaining privacy by locking the room to prevent others from entering while the meeting is in progress.

Starting with Cisco WebEx Meeting Center version WBS32.4, Meeting Center supports audio noise detection functionality that can distinguish between users who are actively speaking and background noise. When audio is connected via the Call Using Computer option, Meeting Center can automatically warn users and prompt them to mute if active background noise (such as knocking, typing, a siren, or dogs barking) is detected. However, users have the option to disable the noise detection function if desired.

Note
Audio noise detection supports the Call Using Computer audio option only.

Security

By default, all WebEx meeting data is encrypted using 128-bit SSL encryption between the client and Cisco's Collaboration Cloud. SSL accelerators within the cloud decrypt the content sharing information and send it to a WebEx conference bridge that processes the content and sends it back through an SSL accelerator, where it is re-encrypted and sent back to the attendees. All Web Zone and Meeting Zone traffic is encrypted using 128-bit SSL where SSL accelerators are used to off-load the SSL function from the Web and Meeting Zone servers.

After the meeting ends, no session data is retained in the WebEx cloud or an attendee's computer. Only two types of data are retained on a long-term basis: billing and reporting information and optionally network based recordings, both of which are accessible only to authorized enterprise users.

Some limited caching of meeting data is carried out within the Meeting Zone, and this is done to ensure that users with connectivity issues or who may be joining the meeting after the start time receive a currently fully synchronized version of the meeting content.

Independent third parties are used to conduct external audits covering both commercial and governmental security requirements, to ensure the WebEx cloud maintains its adherence to documented security best practices. WebEx performs an annual SSAE 16 audit in accordance with standards established by the AICPA, conducted by Price Waterhouse Coopers. The controls audited against WebEx are based on ISO-27002 standards. This highly respected and recognized audit validates that WebEx services have been audited in-depth against control objectives and control activities (that often include controls over information technology and security related processes) with respect to handling and processing customer data.

For customers that require enhanced security, there is also an option to perform end-to-end 256 bit AES encryption for collaboration bridge and multimedia content so that traffic is never decrypted in the cloud. End-to-end encryption results in some lost features such as NBRs. For more information on enhanced WebEx security options, refer to the white paper Unleash the Power of Highly Secure, Real-Time Collaboration, available at


Note
End-to-end encryption options are available for Meeting Center and Support Center meetings without additional cost.
Site administrators can enforce the use of passwords to access the network-based recordings. When the host schedules the meeting, he/she can require all attendees joining the meeting to sign in with Single Sign-On (SSO) authentication and can restrict the meeting to invited attendees only. In addition, site administrators can enable an option to allow only authenticated attendees to enter a host's unlocked Personal Room, while the unauthenticated attendees must wait in the lobby until the host admits them to enter the room.

Scheduling

With respect to scheduling and initiating meetings, WebEx provides cloud-based web scheduling capability, but most organizations prefer to schedule from their corporate email system (Exchange, Lotus Notes, and so forth) or other enterprise applications. The WebEx Productivity Tools is a bundle of integrations with well known desktop tools incorporated into a single application. A WebEx administrator can control the specific integrations that are provided through the tool to their organization's user population. It can be downloaded and installed from the WebEx site, or it can be pushed out locally using standard desktop management tools. To learn more about WebEx Productivity Tools, refer to the information available at

https://www.webex.com/support/productivity-tools.html

User Profile

There are several options for creating WebEx user profiles for an organization in the cloud. Security considerations for the actual usernames and passwords, as well as for handling a large number of user accounts, should be considered. A WebEx administrator can create user profiles manually by bulk import of a CSV template or by a programmatic approach. A programmatic approach uses one or a combination of the WebEx APIs, URL, and XML, or a Federated SSO solution. The programmatic approach can be used by a customer portal, which is an application such as a CRM tool or a Learning Management System that integrates directly into WebEx. In addition, the user can sign up for an account from the company's WebEx site, and the user profile will be created after the request has been approved.

For integrating directly with an organization's LDAP directory, Federated SSO with Security Assertion Markup Language (SAML) is the preferred approach. For more information regarding Federated SSO, refer to the white papers and technical notes available at


High Availability

The Cisco WebEx Collaboration Cloud has a very high level of redundancy built in and is managed by Cisco. It is designed for continuous service with a very robust cut-over to the redundant meeting nodes during outages. In addition to the primary WebEx site, every customer has a backup site physically located in a geographically distant WebEx data center within the same region. If a customer's primary site is unavailable, Global Site Backup (GSB) automatically moves all meeting activity to the backup site. Neither the hosts nor the participants notice that they are being redirected to the backup site. The GSB system facilitates continuous accessibility to WebEx meetings globally, and all attributes, address books, preferences, meeting schedules, and other real-time data are kept in sync between the primary and backup sites. Because of this synchronization, GSB provides redundancy and disaster recovery both before and after the meetings.
Cisco WebEx Cloud Connected Audio

Cisco WebEx Cloud Connected Audio (CCA) is an audio conferencing solution based on a hybrid deployment model that uses the on-premises IP telephony network to provide an integrated audio experience for an organization's WebEx meetings. WebEx CCA implements a SIP trunk connection from the organization's IP telephony network into the WebEx cloud infrastructure (see Figure 11-16). The audio conferencing traffic traverses through this SIP connection instead of the service provider PSTN connection and, thus, WebEx CCA provides significant savings on audio cost and maintains the same integrated and intuitive user experience as other WebEx audio options.

As shown in Figure 11-16, a typical WebEx CCA high-level design consists of the on-premises IP telephony network and the WebEx cloud infrastructure that are connected via the dedicated IP Peering Connections provided by the customer. The on-premises IP telephony network consists of a Cisco Unified Communications Manager (Unified CM) cluster and Cisco Unified Border Element. Cisco Unified Border Elements are deployed in the WebEx cloud infrastructure and they mark the entry point for an organization's IP telephony network. The Cisco Unified Border Elements in the cloud and at the customer site communicate with each other via SIP. WebEx CCA requires the customer to have two IP Peering Connections that connect with different WebEx data centers residing in geographically separated locations for redundancy purpose. The redundant IP links are configured in active/standby.
mode. All conferencing audio traffic flows through the primary link and fails-over to the secondary link if the primary link goes down. WebEx CCA also requires the gateway routers to support Border Gateway Protocol (BGP) and Bidirectional Forwarding Detection (BFD) protocol. BGP and BFD offer a significant faster re-convergence time in the event of a network failure.

Note

The WebEx data center equipment, audio bridge, and servers run over the shared infrastructure along with other customers in the WebEx CCA solution.

Cisco Unified CM has a SIP connection with the WebEx cloud through the Cisco Unified Border Element at the customer site to handle telephony signal. The conference dial-in number is owned by the customer and is terminated at the customer site. Call routing is handled at the customer site, call signaling and audio traffic is handled over the redundant IP peering connections, and call mixing is handled in the cloud. When users dial the conference number within the enterprise, Cisco Unified CM routes the call over the dedicated SIP trunk through the Cisco Unified Border Element to the WebEx cloud without traversing through the PSTN. When the conference users request callback, WebEx sends the call to the Cisco Unified Border Element at the customer site that routes it to the destination end-point. If the conference users reside outside of the enterprise network, calls are routed through the PSTN before terminating or after leaving the customer's IP telephony network. WebEx CCA supports only the G.711 audio codec, RFC 2833 DTMF, and SIP signaling.

WebEx CCA has the highly available and fully redundant architecture that is designed to ensure continuous service operation. Every major component has two instances in active and standby mode, backing up each other. There are two IP Peering Connections handled by two independent pairs of routers, two pairs of Cisco Unified Border Elements, and two audio conferencing bridges. If any of these components fails, its standby counterpart takes over. If the active peering link fails, the network will converge via the standby connection. All existing calls continue, but with a very brief interruption of the media flow. Cisco Unified Border Elements use the Out-of-Dialog OPTIONS ping mechanism to monitor the operational state of each other. Cisco Unified Border Elements at the customer site also monitor the Cisco Unified CM cluster using the Out-of-Dialog OPTIONS ping mechanism. Failure in responding to the ping results in removal of the unresponsive element from the dial-peer list of the sender, which commences routing all new calls via the standby instance. In case the active WebEx audio bridge fails, all calls associated with the bridge are terminated and the standby WebEx audio bridge is activated. WebEx will then prompt the users with a new number to connect to the newly activated bridge, which also re-dials all system-originated calls (callbacks) from before the failure.

Consider the following guidelines when deploying Cisco WebEx Cloud Connected Audio:

- Cisco recommends using Cisco Unified CM 8.5 or later release with the WebEx CCA deployment.
- Cisco recommends using a dedicated Cisco Unified Border Element for the WebEx CCA deployment to ensure a sound architecture and easy troubleshooting.
- Cisco Unified Border Element can be deployed on either a Cisco Integrated Services Router (ISR) or an Aggregated Services Router (ASR), depending on the audio port capacity requirements.
- Use an access control list (ACL) instead of packet inspection to restrict traffic in the firewall on the IP Peering link.
- The system administrator must provide at least one toll and one toll-free number for guest dial-in.
- If an audio codec other than G.711 is desired, use a transcoder to transcode the audio stream to G.711 before sending it to WebEx.
- One Direct Inward Dialing (DID) Digital Number Identification Service (DNIS) must be passed to the WebEx cloud via the Cisco Unified Border Element for all conferencing numbers.
For more information on Cisco WebEx Cloud Connected Audio, refer to the documentation available at
https://www.cisco.com/go/cwcca

Capacity Planning

For a given customer, the actual number of concurrent meetings is essentially unlimited. Different WebEx conferencing types have different capacities with respect to number of attendees. For a detailed product comparison table, refer to the Cisco WebEx Web Conferencing Product Comparison, available at

Network Traffic Planning

With the increased traffic out to the internet, it is important to consider network traffic planning. When planning for network traffic, the way that users use WebEx will make quite a bit of difference in the amount of traffic generated by the meeting. For example, if attendees use native presentation sharing (where the document is loaded to the WebEx site prior to sharing), it generates far less data than if they share their desktops. For a large enterprise, this can be important to understand to ensure correct traffic engineering, especially at the choke points in the network, such as the Internet access points. A preliminary estimate should be made around the average number of meetings to be hosted during the busy hour, along with the average number of attendees. Then, depending on the type and characteristics of these meetings, some projections on bandwidth requirements can be made. For more information regarding network traffic planning, please see the Cisco WebEx Network Bandwidth white paper, available at

Design Considerations

Observe the following design considerations when implementing a Cisco WebEx SaaS solution:

- Collaborative meeting systems typically result in increased top-of-the-hour call processing loads. Cisco partners and employees have access to capacity planning tools with parameters specific to collaborative meetings to help calculate the capacity of the Cisco Unified Communications System for large configurations. Contact your Cisco partner or Cisco Systems Engineer (SE) for assistance with sizing of your system. For Cisco partners and employees, the Cisco Collaboration Sizing Tool is available at https://cucst.cloudapps.cisco.com/landing.

- All connections from WebEx clients are initiated out to the cloud. Typically, opening pinholes in network firewalls is not required as long as the firewalls allow intranet devices to initiate TCP connections to the Internet.


- Based upon business requirements, design decisions have to be made about the following:
  - User creation and authentication options (see User Profile, page 11-30, for details)
  - Meetings scheduling options (see Scheduling, page 11-30, for details)
Cisco WebEx Meeting Center Video Conferencing

Cisco WebEx Meeting Center Video Conferencing provides a consistent, scalable virtual meeting room experience that combines business quality video, audio, and data sharing capabilities into a single solution delivered through Cisco WebEx Collaboration Cloud. Cisco WebEx Meeting Center Video Conferencing is included as part of the Cisco WebEx Meeting Center subscription purchase. It integrates with the Cisco Collaboration infrastructure and applications such as Cisco Unified CM and Cisco Expressway. Participants can join Cisco WebEx Meeting Center Video Conferencing meetings using WebEx clients, Cisco TelePresence, Cisco Jabber, or other third-party standards-based endpoints (SIP or H.323). It also provides a simple and highly secure collaboration solution from the Cisco WebEx Collaboration Cloud, and participants can join the meeting regardless of their location using any device of their choice (desktop, mobile, or video endpoint). With Cisco WebEx Meeting Center Video Conferencing, users can invite others to join their personalized, always-available meeting rooms anytime, or the meeting organizer can reserve the needed rooms and resources for scheduled meetings using the productivity tools.

Architecture

Figure 11-17 illustrates the Cisco WebEx Meeting Center Video Conferencing architecture using SIP video. This architecture consists of the enterprise collaboration network and the WebEx Collaboration Cloud where all the conferencing resources are hosted, and they are connected via the Internet. The enterprise collaboration network encompasses Cisco Unified Communications Manager (Unified CM) and Cisco Expressway, and Unified CM connects with Cisco Expressway-C over a SIP trunk. Cisco Unified CM provides the call routing and call control functions for the registered video devices. Cisco Expressway provides a secure firewall traversal mechanism for calls between the enterprise and WebEx Collaboration Cloud, and it routes the video calls to the WebEx Cloud via the DNS zone configured inside Cisco Expressway-E. In addition, Cisco Expressway provides mobile and remote access capability to the supported Cisco video endpoints so that they can register with Unified CM outside of the enterprise. In order for a participant to join the meeting and share content, the SIP device must support URI dialing and Binary Floor Control Protocol (BFCP). Without BFCP, content cannot be shared and will be seen embedded in the main video.

Note

For existing Cisco VCS customers, using VCS Control as a SIP Registrar for SIP endpoints and VCS Expressway for firewall traversal is supported with the deployment.
Cisco WebEx Meeting Center Video Conferencing architecture also supports H.323 video devices (see Figure 11-18). In this architecture, Cisco VCS Control is the gatekeeper and provides call control for the registered H.323 endpoints. Cisco VCS Expressway provides a secure firewall traversal mechanism for calls between the enterprise and WebEx Cloud, and it routes the video calls to WebEx Cloud via the DNS zone configured inside Cisco VCS Expressway. In order for a participant to join the meeting and share content, the H.323 device must support Annex O for URI dialing and H.239 for content sharing. Without H.239, content cannot be shared and will be seen embedded in the video. In addition, H.323 devices must support either the H.245 User Input or RFC 2833 method of DTMF signaling in order to use interactive voice response (IVR) to start a meeting as a host or to join a meeting before the host joins.
Alternatively, Cisco WebEx Meeting Center Video Conferencing can be deployed using H.323 video without a call control system (see Figure 11-19). In this architecture, the H.323 device does not register to any gatekeeper; and when the user dials the URI, the call is routed using DNS through the firewall to the WebEx Cloud. Make sure the necessary ports on the firewall are opened so that signaling and media can pass through. For port range details, refer to the Collaboration Help article available at https://collaborationhelp.cisco.com/article/en-us/WBX264.

Figure 11-19 Cisco WebEx Meeting Center Video Conferencing Architecture Using H.323 Video Without a Call Control System

Starting with Cisco WebEx Meeting Center version WBS32.9, users can join meetings from H.323 video systems by dialing the regional IP address as shown in the meeting invite. However, if the user dials another region’s IP address (IP address not shown in the meeting invite), the user will not be allowed to join the meeting.

Irrespective of SIP or H.323 devices used in the deployment, WebEx Cloud can perform the interworking between protocols. There are requirements for video devices to be used in a Cisco WebEx Meeting Center Video Conferencing deployment. For details, refer to the Cisco WebEx Meeting Center Enterprise Deployment Guide for Video Device-Enabled Meetings, available at https://collaborationhelp.cisco.com/article/en-us/nmdp0hq

For each participant on a video device, the audio, video, and content sharing are sent over the IP connection to WebEx Cloud, where the media are mixed with other participants, and the mixed audio, active speaker video, and content sharing are sent back to the device for display.

Cisco WebEx Meeting Center Video Conferencing uses H.264 video for active speaker and content sharing. Depending on the capability of the device and the bandwidth available, Cisco WebEx Meeting Center Video Conferencing supports active speaker video up to 720p at 30 frames per second (fps) and content video up to 720p on video devices as well as WebEx clients. The WebEx meeting client has a video floor of 180p for active speaker video at a minimum bit rate of 1.2 Mbps. If the minimum bit rate cannot be maintained due to network conditions (severe packets loss, for example), the WebEx client will stop receiving the active speaker video, but it still receives content sharing as well as conference audio and sends its video to other participants. The WebEx client will periodically perform bandwidth retest and automatically reestablish active speaker video when network conditions stabilize. During the meeting, WebEx allocates the bandwidth based upon the least capable device among all WebEx clients in the conference (excluding devices running below the video floor), with a maximum bandwidth of 4 Mbps. However, if the least capable device leaves the conference, the bandwidth will be reallocated based upon the next least capable device that runs the WebEx meeting client. The allocated bandwidth determines the resolution used to display the video on the WebEx clients.
Each Cisco WebEx Meeting Center Video Conferencing session has an associated video address URI and URL. Participants dial the URI or receive callback on the video device or click on the URL to bring up the WebEx meeting client to join the meeting. A Cisco WebEx Meeting Center Video Conferencing meeting can be one of the following types:

**Scheduled meeting**

Users can use WebEx Productivity Tools (PT) to schedule Cisco WebEx Meeting Center Video Conferencing meetings. Productivity Tools is a suite of tools, including an Outlook plug-in, that allows users to schedule meetings quickly and easily within the email client. This tool suite provides seamless integration with the user's calendar, and users can schedule meetings and send the invitations to all participants directly inside the email client with a single transaction. Alternatively, users can schedule Cisco WebEx Meeting Center Video Conferencing meetings from the WebEx portal, but the host must first schedule the meeting from WebEx and then create an invitation with meeting details attached and send it to all the participants.

Using Cisco TMS 15.2 and TMSXE 5.2, WebEx Productivity Tools can be utilized to schedule Cisco WebEx Meeting Center Video Conferencing meetings with One Button to Push (OBTP). Internally, Cisco TMS creates an externally hosted conference using the SIP URI to Cisco WebEx Meeting Center Video Conferencing as the dial string. Also, Cisco TMS must have the default conference type set to OBTP.

**Note**

Using Cisco TMS and TMSXE for Cisco WebEx Meeting Center Video Conferencing OBTP does not require integration with the on-premises video conferencing infrastructure. On the other hand, if TMS and TMSXE are integrated with the on-premises video conferencing infrastructure, they can be used for Cisco WebEx Meeting Center Video Conferencing OBTP at the same time.

Beginning with Cisco WebEx Meeting Center version WBS32.6, users can schedule and start meetings on their WebEx Personal Room directly from their Google Calendar. In order to use this feature, users need to install Cisco WebEx Scheduler extension from the Google Web Store, and the site administrator needs to enable the Google Calendar option for the WebEx site. When a user signs into the Cisco WebEx Scheduler extension with his WebEx account, this allows the user's Google account to use the WebEx service. Only one WebEx account can be linked to the user's Google account. For details on Cisco WebEx Scheduler for Google Calendar configuration and limitations, refer to the following articles:


**Permanent meeting**

Meetings can be hosted in the user's personal room. Personal rooms can be enabled at the site level or per-user level in the WebEx site. When personal rooms are enabled, a fixed URI and URL are assigned to each user, and participants can use them to join the user's personal room. This personal room belongs to the designated user and is always on. Thus, the user can use his room for his meetings and can send an invitation to all participants with his room's URI and URL attached. With Cisco Spark Calendar Service, users can add @webex to the location field of an Outlook calendar invitation, and Calendar Connector will automatically populate the invitation with the user's personal room information. See the chapter on Mobile Collaboration, page 21-1, for more details.

**Instant meeting**

A user can create an instant meeting from the WebEx portal or by using the WebEx Productivity Tools, and the meeting will start immediately. Using the Meet Now configuration option, the instant meeting can be initiated from the Meeting Center, the user's personal room, or Cisco Jabber Desktop.
Security

Cisco WebEx Meeting Center Video Conferencing supports encrypted signaling and media, or a combination of encrypted and non-secure signaling and media, between the enterprise network and WebEx Cloud. For end-to-end encryption, customers can turn on encrypted signaling and media in the enterprise and use encrypted signaling and media between the enterprise network and the WebEx Cloud. A certificate has to be uploaded to Cisco Expressway-E to ensure that proper handshaking takes place for encrypted signaling to be functional. That certificate can be either self-signed or signed by a trusted Root Certificate Authority (CA). For more information, refer to the latest version of the Cisco WebEx Meeting Center Video Conferencing Enterprise Deployment Guide, available at https://www.cisco.com/c/en/us/support/conferencing/webex-meeting-center/products-installation-and-configuration-guides-list.html

For SIP-based calls, Cisco WebEx Meeting Center Video Conferencing supports four levels of security (in order of preference):

- Encrypted TLS signaling with CA-signed certificates and SRTP media encryption
- Encrypted TLS signaling with self-signed certificates and SRTP media encryption
- Non-secure TCP signaling with SRTP media encryption
- Non-secure TCP signaling with non-secure RTP media

Make sure to open the network ports on the firewall so that inbound and outbound traffic for signaling and media can pass through. For port range details, refer the WebEx article available at https://collaborationhelp.cisco.com/article/en-us/WBX264.

All Cisco WebEx Meeting Center Video Conferencing meetings require the presence of the host to start the meeting. If the guests join before the host, they will be in the waiting room and cannot talk to each other until the host joins. In addition, a host PIN is required when the host joins the meeting from a video device.

Inside the user's personal meeting room, a Lock Room button is available that can be used to lock the room and prevent other participants from entering the user's personal room. When the room is locked and a participant tries to enter the room, that participant will be blocked until the host admits him or unlocks the room. This button is useful in case a user's personal room is used for back-to-back meetings and the host has not finished with the first meeting. The host can lock the room to prevent participants of the second meeting from entering until he finishes with the first meeting and unlocks the room.

Audio Deployment Options

For Cisco WebEx Meeting Center Video Conferencing participants using video devices, their audio, video, and content sharing are sent and received over the IP connection between the WebEx Cloud and the video devices. For WebEx client participants, Cisco WebEx Meeting Center Video Conferencing supports all audio options available for the classic WebEx Meeting Center, which include:

- WebEx Cloud Connected Audio
- WebEx Audio using VoIP
- WebEx Audio using PSTN
- Teleconferencing service provider audio
High Availability

In the enterprise collaboration network, utilize the clustering option with Cisco Unified CM and Cisco Expressway to provide redundancy for call control with video devices and firewall traversal calls. If the primary server fails, the backup server can take over the call control and call handling functions.

For Cisco Unified CM clustering, see the chapter on Call Processing, page 9-1.


Capacity Planning

Cisco WebEx Meeting Center Video Conferencing meetings support up to 25 standards-based video devices, 500 WebEx participants with video enabled, and 500 WebEx participants with audio only.

**Note**

Each screen in a multi-screen video device counts as one video device. For example, if a triple-screen immersive system joins the Cisco WebEx Meeting Center Video Conferencing meeting, it consumes 3 video devices from the video device capacity limit.

Capacity planning for Cisco WebEx Meeting Center Video Conferencing involves sizing of the components running within the enterprise. The components could include:

- **Cisco Unified CM**
  
  Ensure that Unified CM has enough resources and capacity to handle the traffic generated by the video endpoints and IP phones for Cisco WebEx Meeting Center Video Conferencing meetings. For capacity details, see the chapter on Collaboration Solution Sizing Guidance, page 25-1.

- **Cisco Expressway**
  
  Cisco Expressway must provide enough resources to handle the traversal call traffic for the deployment. For capacity details, see the chapter on Collaboration Solution Sizing Guidance, page 25-1.
Network Traffic Planning

Network traffic planning for Cisco WebEx Meeting Center Video Conferencing consists of the following elements:

- **WebEx Clients bandwidth**
  
  The WebEx meeting client uses Scalable Video Coding (SVC) technology to send and receive video. It uses multi-layer frames to send video, and the receiving client automatically selects the best possible resolution to receive video that typically requires 1.2 to 3 Mbps of available bandwidth. For more information regarding network traffic planning for WebEx clients, refer to the *Cisco WebEx Network Bandwidth* white paper, available at
  

- **Bandwidth for video device from enterprise to WebEx Cloud**
  
  For optimal SIP audio and video quality, Cisco recommends setting up the video bandwidth for at least 1.5 Mbps per device screen in the region associated with the endpoint registering with Cisco Unified CM. For example, if a triple-screen device registers with Unified CM, video bandwidth of 4.5 Mbps should be allocated in the associated region.

Design Considerations

Consider the following recommendations when deploying Cisco WebEx Meeting Center Video Conferencing:

- **Enable UDP for media streaming in the firewalls for the optimal video experience.**

- **Open network ports on firewalls to allow inbound and outbound signaling and media traffic.** For details, refer to the latest version of the *Cisco WebEx Meeting Center Video Conferencing Enterprise Deployment Guide*, available at
  

- **Ensure that Binary Floor Control Protocol (BFCP) is enabled in the Unified CM Neighbor Zone in Cisco Expressway-C and that BFCP is also enabled in the SIP profile associated with the SIP trunk between Unified CM and Expressway-C.**

- **For information on the video devices tested with Cisco WebEx Meeting Center Video Conferencing, refer to the *WebEx Video Compatibility and Support* article available at**
  
Cisco WebEx Meetings Server

Cisco WebEx Meetings Server is a highly secure, fully virtualized, private cloud conferencing solution that combines audio, video, and web conferencing in a single solution. Cisco WebEx Meetings Server addresses the needs of today’s companies by presenting a comprehensive conferencing solution with all the tools needed for increased employee productivity as well as support for more dynamic collaboration and flexible work styles. Existing customers can build on their investment in Cisco Unified Communications and extend their existing implementation of Cisco Unified Communications Manager to include conferencing using the SIP architecture. In addition, Cisco WebEx Meetings Server leverages many capabilities from Cisco Unified CM to perform its functions; for example:

- Use the SIP trunk connection with Unified CM to conduct teleconferencing
- Utilize Unified CM's SIP trunk secure connection support for secure conferencing
- Integrate with legacy or third-party PBXs through Unified CM
- Leverage Unified CM's dual stack (IPv4 and IPv6) capability to support IPv6

These capabilities are discussed in more detail in the following sections.

Architecture

Cisco WebEx Meetings Server is a fully virtualized, software-based solution that runs on Cisco Unified Computing System (UCS). It uses the virtual appliance technology for rapid deployment of services. Virtual appliance simplifies the task of managing the system. For example, using the hypervisor technology, system components can easily be moved around for maintenance, or system components can easily be rolled back to a working version if problem arises. The virtual appliance is distributed in the form of an industry standard format, Open Virtual Appliance (OVA). All the software components required to install WebEx Meetings Server are packaged inside the OVA. Traditionally, using an executable installer to install individual software components would take hours to deploy the software. However, using OVA can significantly reduce the amount of time required to deploy the software because all software components are pre-packaged inside the file. Thus, virtual appliance technology can help tremendously to reduce the deployment time for Cisco WebEx Meetings Server.

Figure 11-20 shows the high-level architecture for Cisco WebEx Meetings Server using the non-split horizon network topology. (For details on the non-split horizon network topologies, refer to the Cisco WebEx Meetings Server Planning Guide, available at https://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html.) Inside the virtual appliance, there could be one or more virtual machines (VMs) running. These are the administration, web, and media virtual machines. The administration and web virtual machines serve as the back-end processing for the administration and WebEx sites. These sites handle tasks that happen before and after the meeting, such as configuration, scheduling/joining meetings, and recording playback. The media virtual machine provides resource allocation, teleconference call control, and media processing (voice, video, and data) during the meeting. The number of virtual machines running inside the virtual appliance depends on the capacity desired and on whether high availability is needed. This provides various options for deployment size.
Cisco WebEx Meetings Server offers the option of deploying the Internet Reverse Proxy (or edge servers) in the DMZ to facilitate external access. This option provides two advantages. First, all external participants can securely access the WebEx conferences from the internet without going through a VPN. Second, mobile users can join the meetings from a mobile device anywhere as long as there is internet connectivity. Note that the Internet Reverse Proxy is mandatory if mobile client access is enabled.

Internet Reverse Proxy is used to terminate all inbound traffic from the internet inside the DMZ. The content is then forwarded to the internal virtual machines through an encrypted Secure Socket Layer (SSL) or Transport Layer Security (TLS) tunnel. This encrypted tunnel is established by the internal virtual machines connecting outbound to the Internet Reverse Proxy. Therefore, there is no need to open TCP ports inbound from the DMZ to the internal network on the internal firewall. However, some outbound ports from the internal network need to be opened on the internal firewall to allow communication with the Internet Reverse Proxy in the DMZ.

All end-user sessions are 100% encrypted using industry standard Secure Socket Layer (SSL) and Transport Layer Security (TLS). All traffic between the virtual machines is sent over the secure channel. Federal Information Processing Standard (FIPS) encryption can also be turned on by a single policy setting, providing US Department of Defense (DoD) level security. Alternatively, the Internet Reverse Proxy can be deployed behind the internal firewall as shown in Figure 11-21.
For security concerns, an organization would typically take several months to get approval in deploying a component inside the DMZ. Using this methodology, it could eliminate any DMZ components and bypass the approval process to get the WebEx Meetings Server deployment done quickly. All internet traffic (HTTP on port 80 and SSL on port 443) to the external firewall should be forwarded to the internal firewall. This will minimize the number of ports that need to be opened in the external and internal firewalls. However, placing the Internet Reverse Proxy inside the internal network implies that inbound internet traffic will terminate in the internal network. Although direct internet access to the internal network could be controlled by the firewalls, not all organizations allow terminating internet traffic directly on their internal network. Ensure that this deployment does not violate your organization's IT policy before choosing this option.

In a large enterprise deployment, an organization would require the Single Sign On (SSO) capability to allow end users to sign in using their corporate credentials. Cisco WebEx Meetings Server can connect to the corporate LDAP directory using the industry standard SAML 2.0 for SSO.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco WebEx Meetings Server supports Meeting Center only.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting with Cisco WebEx Meetings Server 1.1, Cisco Jabber integrated with the Cisco Unified CM IM and Presence Service can be used to join or start meetings hosted on WebEx Meetings Server. For Cisco Jabber support details, refer to the Cisco WebEx Meetings Server System Requirements, available at <a href="https://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html">https://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html</a>.</td>
</tr>
</tbody>
</table>
Cisco Unified CM Integration

Cisco WebEx Meetings Server support both Cisco Unified CM and Session Management Edition (SME). Cisco Unified CM is a central piece of the WebEx Meetings Server architecture that allows the following:

- Attendees joining the teleconference by means of Cisco IP Phone or PSTN
- Integration of legacy or third-party PBXs with Cisco WebEx Meetings Server

Cisco Unified CM integrates with WebEx Meetings Server by means of SIP trunks to provide inbound and callback call control. Customer can choose to turn on security and run Transport Layer Security (TLS) and Secured Real-time Transport Protocol (SRTP) over the SIP trunk connection. A SIP trunk is configured in Unified CM with a destination address of the Load Balancer in WebEx Meetings Server, and then a route pattern (match the call-in access number configured in WebEx Meetings Server) must be used to route calls via the SIP trunk. A second SIP trunk is configured in Unified CM with a destination address of the Application Server in WebEx Meetings Server, and then a SIP route pattern must be used to route calls via the SIP trunk. When an attendee dials the access number to join the meeting, the first SIP trunk is used to send the call. After the call is connected and the caller enters the meeting ID, the Load Balancer issues a SIP REFER to Unified CM to send the caller to the Application Server that hosts the meeting via the second SIP trunk.

The system administrator can configure a SIP trunk in WebEx Meetings Server that points to a Unified CM to perform callback. Attendees can provide a callback number and have the system out-dial the number to the attendees to join the bridge. In the case of attendees requesting callback, the WebEx Meetings Server sends the SIP request to Unified CM along with the callback number via the configured SIP trunk. It is imperative for Unified CM to be able to resolve all dial strings received from a callback request to join the meetings. Callbacks may also be disabled system-wide by means of site administration settings. Unified CM is in control of all toll restrictions to various countries or other numbers that most enterprises will block, because WebEx Meetings Server does not have any toll restriction blocking itself.

WebEx Meetings Server supports the bidirectional SIP OPTIONS ping mechanism. The ping response from the remote end indicates that the remote end is active and whether it is ready to accept calls. Based on the response, WebEx Meetings Server or Unified CM can determine whether to send calls on the current SIP trunk or look for an alternate SIP trunk (if configured) to send calls. Note that SIP OPTIONS ping is supported in Cisco Unified CM 8.5 and later releases. Due to this reason, Cisco recommends using a compatible Cisco Unified CM version that supports SIP OPTIONS ping for Cisco WebEx Meetings Server deployment. For the list of compatible Unified CM versions, refer to the compatibility matrix in the Cisco WebEx Meetings Server System Requirements, available at https://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html

Note

Cisco WebEx Meetings Server supports SIP trunk connection with Cisco Unified CM only.
Legacy PBX Integration

Some organizations that have a legacy PBX and are not ready to fully migrate to a Cisco Unified Communications solution, might want to use Cisco WebEx Meetings Server with their system for conferencing. Cisco Unified CM can be used to bridge the legacy PBX and Cisco WebEx Meetings Server together. Cisco WebEx Meetings Server can see only Unified CM and does not even know the PBX is behind Unified CM. As long as Unified CM can interoperate with the organization's PBX, Cisco WebEx Meetings Server can integrate with the organization's PBX. This integration can provide several benefits:

- Allow users in the legacy system to experience the new technology
- Allow an organization to adopt the new technology gradually, at its own pace
- Protect the customer's investment in existing technology while allowing them to migrate to Cisco technology gradually


IPv6 Support

Cisco WebEx Meetings Server supports IPv4 only or dual stack (IPv4 and IPv6) addressing for telephony audio, while telephony signaling remains at IPv4. Audio streams can be IPv4, IPv6, or a mix of IPv4 and IPv6 in the same meeting. Cisco WebEx Meetings Server supports Alternate Network Address Types (ANAT) to enable both IPv4 and IPv6 media addressing in the Session Description Protocol (SDP) during the SIP Offer and Answer exchange on the SIP trunk with Unified CM to establish a media connection using the preferred addressing scheme.

Both IPv4 and IPv6 devices can be used for teleconferencing. With IPv6 devices, Cisco WebEx Meetings Server leverages Unified CM's capacity to translate the IPv6 signaling to IPv4 and transport it over a SIP trunk to the Cisco WebEx Meetings Server. With the telephony media addressing, Cisco WebEx Meetings Server can convert between IPv4 and IPv6. Therefore, Cisco WebEx Meetings Server can support IPv6 without any expensive MTP resources.

With ANAT, Cisco WebEx Meetings Server can support IPv6 telephony audio without the support of IPv6 telephony signaling. However, ANAT must be supported on both ends of the Unified CM SIP trunk. Be sure to enable ANAT on the Unified CM SIP trunk, otherwise there will be a failure to establish the call when attendees request callback or attempt to dial in.

If the WebEx Meetings Server has IPv6 enabled, ANAT headers will be included in the media offer. WebEx Meetings Server will always answer with ANAT headers if the media offer includes ANAT headers. The following paragraphs describe the media address version selection process between the IPv6-enabled WebEx Meetings Server and the dual-stack Unified CM using the ANAT header.

When WebEx Meetings Server sends a call to Unified CM, the SDP offer contains both IPv4 and IPv6 media addresses. If the called device is IPv6, Unified CM chooses IPv6 for the media connection and answers with the IPv6 media address in the SDP; if the called device is dual-stack, Unified CM uses the IP Addressing Mode Preference for Media parameter to determine the address version in the answer SDP. If the parameter is set to IPv6, then IPv6 will be used for the media connection.
When Unified CM sends a call to the WebEx Meetings Server through the SIP trunk, WebEx Meetings Server receives the SDP offer with an ANAT header. If the SDP offer contains both IPv6 and IPv4 media addresses, WebEx Meetings Server answers with the higher precedence address version specified in the ANAT header, which would be IPv6 in this case. If the SDP contains only an IPv6 address, WebEx Meeting Server answers with an IPv6 media address.

For information on deploying IPv6 in a Cisco Unified Communications system, refer to the latest version of Deploying IPv6 in Unified Communications Networks with Cisco Unified Communication Manager, available at

https://www.cisco.com/go/ucsrnd

High Availability

Cisco WebEx Meetings Server uses the N+1 redundancy scheme to ensure system availability in the event of component failures. High availability is achieved by adding a local, redundant system to the primary system within the same data center. At the system level, virtual machines and components inside run in active/active mode. If one component goes down, the system restarts the component. Status information is exchanged between system components. Using this status information, the system is able to distribute the requests evenly among the active components. Depending on the deployment size, the number of virtual machines in the backup or redundant system might or might not be the same as in the primary system.

In the high availability system, when the virtual machine hosting the meeting goes down, affected meeting clients will automatically reconnect to the available service within a short period of time. However, depending on the nature of the failure and which component has failure, not all clients and meetings would be affected. For descriptions of high availability system behavior after a component failure, refer to the latest version of the Cisco WebEx Meetings Server Administration Guide, available at


Virtual IP Address

Inside the high availability system, there is a second network interface in the active administration and Internet Reverse Proxy virtual machine that is configured with the virtual IP address. The administration and WebEx site URLs use this virtual IP address to access the administration and WebEx sites. In the event of failover, the virtual IP address is moved over to the new active virtual machine. Thus, it provides access redundancy to the administration and WebEx site.

Multiple Data Center Design

Cisco WebEx Meetings Server can be deployed in multiple data centers (up to maximum of 2) for geographic redundancy or disaster recovery. In this deployment, there are two WebEx Meetings Server systems with identical deployment size, one in each data center, that are joined together to form a single logical system running in active/active mode. The first system added to the multi-data center system is the primary, and the system that is added after that is the secondary. When the secondary system is added to the multi-data center system, all its global data are overwritten with the data from the primary system and only configuration parameters local to the data center are preserved. Refer to the Cisco WebEx Meetings Server Administration Guide for details on the types of data that will be overwritten and preserved. Within each data center, there are local Unified CM instances for handling teleconferencing. System status is exchanged, and information about users and meetings is synchronized across data center
peers over an encrypted SSL link. Administrators use a single URL to manage the systems, and participants use a single URL or one set of dial-in numbers to join the meeting. When participants join a meeting via the client, the system automatically chooses the data center closest to the participant to host the meeting, and the meeting is cascaded across data centers.

In the event of failure, if one component goes down in the data center, the system restarts that component. If the whole data center goes down, the surviving data center takes over without any manual intervention, and the system still runs with full capacity. When this happens, affected meeting clients automatically reconnect to the service in the surviving data center within a short period of time. However, depending on the nature of the failure and state of the client, the recovery mechanism might be different and would follow the same behavior as the high availability system. For detail descriptions, refer to the latest version of the *Cisco WebEx Meetings Server Administration Guide*, available at


Consider the following information when using the multiple data center design:

- Configure NTP in all data centers.
- A multi-data center license is required for the WebEx Meetings Server system in each data center. Install the licenses onto the primary data center system before joining the data centers.
- A deployment size of 50 users per system is not supported, but larger system sizes are supported.
- Running a high availability system within the data center is not supported.
- Deploy local Unified CM instances in each data center.
- Joining the systems together will not increase the total system capacity.
- Either both data centers or neither data center can have Internet Reverse Proxy deployed.

**Capacity Planning**

The capacity of WebEx Meetings Server depends on the platform of choice and the number of conferencing nodes running in the deployment. For capacity planning details, see the section on Collaborative Conferencing, page 25-44.

**Storage Planning**

If recording meetings is a requirement, sufficient disk space should be allocated on the Network Attached Storage (NAS) device to store the recordings. For disk space allocation detail, refer to the *Meeting Recordings* section in the *Cisco WebEx Meetings Server Planning Guide*, available at

Network Traffic Planning

Network traffic planning for WebEx Meetings Server collaboration consists of the following elements:

- Call control bandwidth
  Call control bandwidth is extremely small but critical. Co-locating the WebEx Meetings Server with Unified CM helps protect against issues with call control. Remote locations need proper QoS provisioning to ensure reliable operation. Call control bandwidth is used for establishment of calls between WebEx Meetings Server and Unified CM, and the amount of bandwidth required for each call depends on how the attendees join the meeting. For an attendee dialing into the meeting, the call consumes approximately the same amount of bandwidth as making two SIP calls. For an attendee requesting callback, the call consumes approximately the same amount of bandwidth as making one SIP call. For details about call control bandwidth estimation for SIP calls and QoS provisioning, see the chapter on Network Infrastructure, page 3-1.

- Real-Time Transport Protocol (RTP) traffic bandwidth
  RTP traffic consists of voice and video traffic. Voice bandwidth calculations depend on the audio codec used by each device. (See the chapter on Network Infrastructure, page 3-1, for bandwidth consumption by codec type.) Video bandwidth can be calculated the same way as WebEx SaaS. (See Network Traffic Planning, page 11-33.)

- Web collaboration bandwidth
  Web collaboration bandwidth for WebEx Meetings Server can be estimated the same way as WebEx SaaS. (See Network Traffic Planning, page 11-33.)

- Multiple data center deployment
  For proper operation and optimal user experience with this deployment, there are network requirements for maximum round-trip delay time (RTT) and minimum guaranteed bandwidth plus additional bandwidth for each cascaded meeting between data centers. For network requirement details, refer to the latest Cisco WebEx Meetings Server Planning Guide and System Requirements, available at https://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html

Design Consideration

The following additional design considerations apply to WebEx Meetings Server deployments:

- For scenarios where any WebEx Meetings Server components are separated by network firewalls, it is imperative to ensure the correct pinholes are opened for all required traffic.

- Collaborative meeting systems typically result in increased top-of-the-hour call processing load. Capacity planning tools with specific parameters for WebEx Meetings Server are available to Cisco partners and employees to help calculate the capacity of the Cisco Unified Communications System for large configurations. Contact your Cisco partner or Cisco Systems Engineer (SE) for assistance with sizing of your system. For Cisco partners and employees, the Cisco Collaboration Sizing Tool is available at https://cucst.cloudapps.cisco.com/landing.

- Using Transport Layer Security (TLS) and Secured Real-time Transport Protocol (SRTP) have no effect to the WebEx Meetings Server capacity. However, using TLS and SRTP does have an impact on Cisco Unified CM capacity.

- WebEx Meetings Server has no built-in line echo cancellation. Use an external device such as a Cisco Integrated Service Router (ISR) to provide echo cancellation functionality.
For more details on the various Cisco Collaboration client offerings and how they fit into Cisco conferencing solutions, see the chapter on Collaboration Endpoints, page 8-1.

Call admission control with WebEx Meetings Server is performed by Unified CM. With locations-based call admission control, Unified CM can control bandwidth to the WebEx Meetings Server system by placing the SIP trunk specific to WebEx Meetings Server in a location with a set amount of audio bandwidth allowed. Alternatively, Unified CM supports the use of Resource Reservation Protocol (RSVP), which can also provide call admission control. For further information regarding call admission control strategies, see the chapter on Bandwidth Management, page 13-1.

Cisco recommends marking both the audio streams and video streams from WebEx Meetings Server as AF41 (DSCP 0x22) to preserve lip-sync. These values are configurable in WebEx Meetings Server Administration.

Web conferencing traffic is encrypted in SSL and is always marked best-effort (DSCP 0x00).

Reference Document

For network requirements, network topology, deployment size options, and other deployment requirements and options for WebEx Meetings Server, refer to the Cisco WebEx Meetings Server Planning Guide, available at


Cisco Collaboration Meeting Rooms Hybrid

Cisco Collaboration Meeting Rooms (CMR) Hybrid is a collaboration conferencing platform that combines the video experience of Cisco TelePresence Conferencing with the presentation experience of Cisco WebEx Meeting into a single meeting. Cisco WebEx and TelePresence are optimized to work with standards-based video endpoints and WebEx meeting clients. They help customers to extend the reach of the meetings and simplify the experience for all participants. Attendees on TelePresence endpoints and WebEx meeting clients can securely share two-way video, audio, and content among themselves. This platform brings together the user experiences from two conferencing systems and extends the collaboration to more users on more devices in more locations.

Cisco CMR Hybrid allows an organizer to schedule meetings using the familiar interface of Microsoft Outlook enabled by the WebEx Productivity Tools or with the Cisco TelePresence Management Suite (TMS). The host selects the participants, adds the preferred endpoints and the WebEx information, and sends the invitation to all attendees. Using the productivity tools, the attendees receive one meeting invitation with all the information about how to join through TelePresence or WebEx. The meetings can be launched using One Button To Push (OBTP) from the TelePresence endpoint, or Cisco TMS can automatically connect the endpoints with the meetings at the scheduled start time.
Architecture

As shown in Figure 11-22, the high-level architecture of Cisco CMR Hybrid consists of the enterprise collaboration network and the WebEx Cloud infrastructure that are connected through an IP connection. The enterprise collaboration network consists of Cisco Unified Communications Manager (Unified CM), Cisco Expressway-C and Expressway-E, TelePresence Bridge pools that are managed by TelePresence Conductor, and Cisco TelePresence Management Suite (TMS). Cisco Unified CM is the call processing platform that provides call routing and call control for the TelePresence endpoints within the enterprise. Cisco Expressway-C and Expressway-E route calls between the enterprise network and WebEx Cloud. Cisco Unified CM connects with Cisco Expressway-C and Cisco TelePresence Conductor over separate Best Effort Early Offer SIP trunks.


Note

For existing Cisco VCS customers, deployment using Cisco VCS Control and Expressway in place of Cisco Expressway-C and Expressway-E is supported.

Note

Deployment using a Best Effort Early Offer SIP trunk between Unified CM and the TelePresence Bridge without TelePresence Conductor is supported, but using TelePresence Conductor is recommended.

Cisco TelePresence Conductor selects a TelePresence Bridge from the pool to host the TelePresence conference. The TelePresence Bridge mixes the audio from the TelePresence endpoint participants and sends the mixed audio, the active speaker video, and the content sharing video to the WebEx Cloud using SIP. Similarly, the TelePresence Bridge receives the media (mixed audio, active speaker, and content sharing video) from the WebEx Cloud, cascades the audio into the TelePresence conference, and sends the content sharing video to the TelePresence endpoints. If the TelePresence Bridge detects that the active speaker is from the WebEx side, it switches the TelePresence endpoints to the active speaker video. If the active speaker is from the TelePresence side, the TelePresence Bridge sends the previous active speaker video to the TelePresence endpoint of the current active speaker.
In the DMZ, Cisco Expressway-E handles the traversal calls between the enterprise and WebEx Cloud, and it allows the signal and media to traverse through the internal and external firewalls. Cisco Expressway-E connects with the WebEx Cloud through the configured DNS Zone and routes calls to WebEx via DNS lookup. Cisco Expressway-E communicates with WebEx Cloud via an encrypted connection using TLS and secured RTP for SIP signal and media. Customers have an option to turn on encryption for the SIP signal and media traffic within the enterprise. TelePresence endpoints outside of the enterprise can register with Unified CM through Expressway-C and Expressway-E, and thus participants on these endpoints can join the CMR Hybrid meetings.

When the WebEx Cloud receives the traversal calls and media sent from the enterprise network, the WebEx audio bridge cascades the audio into the WebEx conference, and WebEx switches to the active speaker video and displays the content sharing on the WebEx meeting clients. Similarly, WebEx Cloud sends the conference mixed audio, the active speaker, and content sharing video from the WebEx side to the enterprise via Cisco Expressway-C and Expressway-E, which routes them to the TelePresence Bridge.

Cisco CMR Hybrid supports H.264 video for active speaker and content sharing. It utilizes Binary Floor Control Protocol (BFCP) for content sharing and G.711 codec for audio. While Cisco WebEx uses H.264 video and G.711 audio codec, TelePresence can still use other video formats or codecs that are supported by the endpoints. The TelePresence Bridge will handle the audio and video interoperability between the TelePresence endpoints and WebEx meeting clients. In addition, there is a flow control on the link between the TelePresence Bridge and WebEx Cloud that regulates the bandwidth available for handling the media. For media from WebEx, the TelePresence Bridge always allocates 4 Mbps to ensure that WebEx sends the best quality of video possible to the TelePresence Bridge. For media from the TelePresence Bridge, the WebEx meeting client has a video floor of 180p for active speaker video at the minimum bit rate of 1.2 Mbps. If the minimum bit rate cannot be maintained due to network conditions (severe packets loss, for example), the WebEx client will stop receiving the active speaker video but still
receives content sharing as well as conference audio and sends its video to other participants. The WebEx client will periodically perform bandwidth retest and automatically reestablish active speaker video when network conditions stabilize. Depending on the capability of the device running the WebEx meeting client and on bandwidth available, the WebEx client supports active speaker video up to HD 720p at 30 frames per second (fps) and content video up to 1080p. During the meeting, WebEx allocates the bandwidth based upon the least capable device among all WebEx clients in the conference (excluding devices running below the video floor), with a maximum bandwidth of 4 Mbps. However, if the least capable device leaves the conference, the bandwidth will be re-allocated based on the next least capable device that runs the WebEx meeting client. The allocated bandwidth determines the resolution and frame rates used to display TelePresence video on WebEx clients. Depending on the TelePresence endpoints deployed, video resolution required, screen layout desired, and deployment options chosen, customers can deploy the TelePresence Bridge using the Cisco TelePresence Server (appliance or virtualized platforms) or Cisco TelePresence MCU, but the pool must consists of bridges of the same type only (either TelePresence Server or TelePresence MCU). For TelePresence Conductor deployment details, see to the section on Cisco Collaboration Meeting Rooms Premises in the Cisco Rich Media Conferencing chapter of the Cisco Collaboration System 11.x SRND, available at


WebEx and TelePresence participants can join the CMR Hybrid meeting from within the enterprise or anywhere from the internet. For WebEx participants, they join the meeting using the WebEx meeting clients with either PSTN or VoIP audio. For TelePresence participants, they join the meeting via the One Button To Push (OBTP) or Auto Connect feature with the supported endpoints or by calling directly into the TelePresence Bridge. Once the participants successfully join the meeting, they can see the live video of each other from the endpoints and meeting clients. For presentation sharing with a WebEx user, either the user can make himself the presenter or the host can assign the presenter privilege to the user before he can start sharing the presentation. There is the WebEx site configuration to control this behavior. For presentation sharing with a TelePresence user, the user can connect the video display cable to his computer or press a button on the endpoint to start sharing his presentation without involving the host.

Note
Staring with Cisco TMS 14.6 and TMSPE 1.4, Cisco Collaboration Meeting Rooms Premises can be integrated with Cisco WebEx, allowing participants to join a meeting in the user's personal room from the WebEx meeting client.

Scheduling
Cisco TelePresence Management Suite (TMS) is the key component for scheduling Cisco CMR Hybrid meetings. It provides a control link to the Cisco WebEx meeting scheduler. This link enables Cisco TMS to create new meetings on Cisco WebEx calendar and to obtain Cisco WebEx meeting information that is distributed to meeting participants. The following options are available to schedule CMR Hybrid meetings:

- WebEx Productivity Tools
  WebEx Productivity Tools is a suite of tools that allows users to schedule WebEx sessions quickly and easily. Productivity Tools includes an Outlook plug-in that allows an organizer to schedule WebEx Meetings, TelePresence resources, and CMR Hybrid meetings. Cisco TelePresence Management Suite Extension for Microsoft Exchange (TMSXE) is required for the productivity tool to interface with Cisco TMS for booking the meetings. This option provides a seamless integration for users to schedule CMR Hybrid meetings and to send the invitations to all participants directly inside the email client with a single transaction.
• Smart Scheduler

Smart Scheduler is a web-based tool that is hosted on Cisco TelePresence Management Suite Provisioning Extension (TMSPE), and it allow users to schedule CMR Hybrid meetings using a browser. This could provide an option for users who would like to schedule meetings on mobile devices.

Note As long as the Cisco TMSPE option key has been installed, there is no extra license required for using Smart Scheduler.

• WebEx Scheduling Mailbox

In this option, the network administrator needs to create a special mailbox account in Microsoft Exchange Server. When an organizer schedules a CMR Hybrid meeting, he should include this special mailbox account in the invitees list. Cisco TMSXE monitors this account and requests Cisco TMS to book a CMR Hybrid meeting if it sees this account in the recipients list. This option provides a convenient way, but with limited control of settings, for users to schedule meetings using any email clients that are supported by Exchange, such as Outlook Web Access (OWA).

• Cisco TMS Booking Interface

With this option, the meeting organizer has to log in to the Cisco TMS portal and schedule the CMR Hybrid meetings from the Booking interface. This interface provides users with control of advanced settings for the meetings, and typically IT or help desk personnel uses this option to schedule meetings.

For Cisco TMS configuration details with these options, refer to the Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide, available at


Scheduling a CMR Hybrid meeting is a two-steps process. First, a request is sent to the WebEx Cloud to schedule the meeting on the WebEx calendar, and the WebEx Cloud responds with the meeting details that are passed to Cisco TMS. Second, Cisco TMS schedules the TelePresence meeting in its calendar. When it is the meeting start time, Cisco TMS pushes the meeting details to the TelePresence Bridge for joining the meeting on WebEx. The meeting details returned from WebEx include the date and time for the meeting, dial-in information, subject, meeting number, URL for joining the meeting, and so forth. Once the meeting has been scheduled, details for the WebEx and TelePresence portions of the meeting are sent to the host, and the host can forward the details to all participants. However, if the productivity tool is used, the meeting details are automatically included in the invitation that the host creates and sends to the meeting participants.
Single Sign On

Cisco CMR Hybrid supports scheduling the WebEx portion of the meeting in Cisco TMS using Single Sign On (SSO). This feature requires the WebEx site to have Cisco TMS provisioned as the delegated partner and to have the Partner Delegated Authentication configured. With SSO enabled in Cisco TMS, only the user’s WebEx username is stored in the Cisco TMS user profile without the need of the WebEx password. When the user schedules a CMR Hybrid meeting, WebEx trusts Cisco TMS and requires only the WebEx username stored in Cisco TMS to schedule the meeting in the WebEx calendar. For Cisco TMS configuration details with SSO, refer to the latest version of the Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide, available at


For more information regarding SSO with Cisco WebEx, refer to the white papers and technical notes available at


Security

All communications between the enterprise network and the WebEx Cloud are encrypted (using TLS and secured RTP). Customers also have an option to turn on encryption for the SIP signal and media within the enterprise. A certificate has to be uploaded to the Cisco Expressway-E to ensure that proper handshaking takes place for the TLS connection to be functional. That certificate must be signed by a trusted Root Certificate Authority. For the list of the trusted Root Certificate Authorities, refer to the Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide, available at


A password is required when the TelePresence Bridge calls into WebEx to join the meeting. The password is allocated for each CMR Hybrid meeting scheduled on the WebEx calendar and is embedded in the SIP URI that is returned as part of the meeting details from the WebEx Cloud. This password is encoded into 22 bytes and qualifies for the security standards. At the start of the meeting, the TelePresence Bridge calls into WebEx using this SIP URI, and WebEx validates the password to authorize the call to join the meeting.

Deployment Options

When it is the start time for the CMR Hybrid meeting, Cisco TMS initiates the conference on the TelePresence Bridge through TelePresence Conductor for the TelePresence participants. The TelePresence Bridge makes a SIP call through TelePresence Conductor out to the WebEx Cloud using the SIP URI that was returned as part of the scheduling process and to join the conference on the WebEx side. As a result, the TelePresence Bridge establishes separate audio, active speaker video, and content sharing video streams with the cloud for the meeting. The active speaker video, content sharing video, and conference control always travels over the IP network, but the audio can travel over either the IP network or the PSTN, depending on the deployment options chosen. The various audio options available for CMR Hybrid are:

- WebEx Audio Using SIP, page 11-55, including Cloud Connected Audio
- WebEx Audio Using PSTN, page 11-55
- Teleconferencing Service Provider Audio, page 11-57
WebEx Audio Using SIP

Figure 11-22 shows the deployment of Cisco CMR Hybrid using WebEx Audio with SIP. In this option, the conference audio is established with the WebEx audio bridge through the SIP connection when the TelePresence Bridge calls out to the WebEx Cloud at the start of the meeting. The audio, active speaker video, content sharing video, and conference control are sent on the IP network from the TelePresence Bridge to the WebEx Cloud through Cisco Expressway-C and Expressway-E. As a result, the audio connection from the TelePresence Bridge cascades into the WebEx audio bridge.

WebEx Audio Using PSTN

For Cisco CMR Hybrid deployment where the in-country rule does not allow toll bypass, WebEx Audio using the PSTN could be an option. Figure 11-23 depicts this deployment. In this option, the active speaker video, content sharing video, and conference control are sent over the IP network, but the audio is established with the WebEx audio bridge through the PSTN. This option requires the deployment of a voice gateway to connect the audio call between the IP network and the PSTN. During the scheduling process, when the meeting is scheduled on the WebEx calendar, WebEx passes the dial-out number and the meeting number to Cisco TMS. At the start of the meeting, the TelePresence Bridge initiates a SIP call to the WebEx Cloud to establish the active speaker video and content sharing video. At the same time, the TelePresence Bridge dials out through the PSTN to establish an audio connection with the WebEx audio bridge. After connecting with the WebEx audio bridge, the TelePresence Bridge sends out the meeting number as a DTMF dial sequence so that WebEx can associate the audio and video call legs. As a result, the audio connection from the TelePresence Bridge cascades into the WebEx audio bridge.
The dial-out number returned from WebEx is in full E.164 number format (for example, +14085551212). The dial plan design in Cisco Unified CM should take into account the handling of E.164 numbers. For dial plan design with Cisco Unified CM, see the chapter on Dial Plan, page 14-1.
Teleconferencing Service Provider Audio

The Teleconferencing Service Provider (TSP) Audio option is for customers who prefer to use the audio bridge hosted by their third-party teleconferencing service provider. The TSP Audio configuration is very similar to WebEx Audio using the PSTN configuration, except that the audio bridge is hosted by the teleconferencing service provider (see Figure 11-24). The TSP link between WebEx and TSP provides the advanced conference control features.

**Figure 11-24  Cisco CMR Hybrid Using Teleconferencing Service Provider (TSP) Audio**

During the scheduling process, in addition to the dial-out number and meeting number, extra digits for navigating through the IVR prompts on the TSP audio bridge are passed from WebEx to Cisco TMS. At the scheduled meeting start time, the TelePresence Bridge initiates a SIP call to the WebEx Cloud to establish the video connections. At the same time, the TelePresence Bridge dials out to the TSP audio bridge through the PSTN. Then the TelePresence Bridge plays out the meeting number as a DTMF dial sequence, along with additional DTMF digits to navigate through the IVR prompts on the audio bridge to start the meeting. On the WebEx side, WebEx participants start the WebEx session using the meeting client and dial into the TSP audio bridge or have callback from the audio bridge. Thus, the audio streams from TelePresence and WebEx participants are cascaded. From this point onward, information about the loudest speaker, participant list, and so forth in the WebEx side, is passed from the TSP to WebEx through the TSP link and then into the enterprise collaboration network.
The dial-out number returned from WebEx is in full E.164 number format (for example, +14085551212). The dial plan design in Cisco Unified CM should take into account the handling of E.164 numbers. For dial plan design with Cisco Unified CM, see the chapter on Dial Plan, page 14-1.

**High Availability**

There are two areas that must be considered when designing high availability for CMR Hybrid: the enterprise collaboration network and the WebEx Cloud. The WebEx Cloud is managed by Cisco and already has the redundancy built into the infrastructure. For details, see the section on Cisco WebEx Software as a Service, page 11-26.

In the enterprise collaboration network, utilize the clustering option from Cisco Unified CM and Cisco Expressway to provide redundancy for call control and call routing on the TelePresence endpoints. In case the primary server fails, the backup server can take over the call control and call routing functions. In addition, resiliency of the TelePresence conferencing infrastructure must be considered to handle failure of conference bridges.

For Cisco Unified CM clustering, see the chapter on Call Processing, page 9-1.


For resiliency of the TelePresence conferencing infrastructure, see the section on Cisco Meeting Server, page 11-7.

**Capacity Planning**

The WebEx Cloud has the built-in capability to evenly distribute the traffic and dynamically add more capacity if thresholds are exceeded. Capacity planning for Cisco CMR Hybrid involves sizing of the components running within the enterprise. The components include:

- **Call Processing Platforms**
  
  Cisco Unified CM must provide enough resources to handle the traffic generated by the TelePresence endpoints. For details, see the section on Capacity Planning for Collaboration Endpoints, page 8-44.

- **TelePresence Conferencing**

  The Cisco TelePresence Conductor, Cisco TelePresence Server, or Cisco TelePresence MCU must provide enough resources to handle the conference traffic. For details, see the information on capacity planning in the section on Cisco Collaboration Meeting Rooms Premises in the Cisco Rich Media Conferencing chapter of the Cisco Collaboration System 11.x SRND, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/confernc.html

- **Cisco Expressway**

  Cisco Expressway must provide enough resources to handle the traversal call traffic for the deployment. For capacity details, see the chapter on Collaboration Solution Sizing Guidance, page 25-1.
Network Traffic Planning

Network traffic planning for Cisco CMR Hybrid consists of the following elements:

- **WebEx Clients Bandwidth**
  The WebEx meeting client uses the Scalable Video Coding (SVC) technology to send and receive video. It uses multi-layer frames to send video and it allows the receiving client to automatically select the best possible resolution to receive video. For more information regarding network traffic planning for WebEx clients, refer to the *Cisco WebEx Network Bandwidth* white paper available at [https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white_paper_c11-691351.html](https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white_paper_c11-691351.html)

- **Bandwidth from Enterprise to WebEx Cloud**
  For each call to the WebEx Cloud, a minimum network bandwidth of 1.1 Mbps is required between the enterprise and the WebEx Cloud. For example, if a customer is expecting five simultaneous CMR Hybrid meetings, network bandwidth of 5.5 Mbps is required. At the same time, a maximum bandwidth of 4 Mbps is supported per call.

For optimal SIP audio and video quality between the TelePresence Bridge and the WebEx Cloud, Cisco recommends setting up the video bandwidth of at least 1.3 Mbps in the region associated with each endpoint registering with Cisco Unified CM.

Design Considerations

The following design considerations apply to Cisco CMR Hybrid deployments:

- **Upgrade from previous versions of CMR Hybrid that use the Cisco TelePresence MultiPoint Switch infrastructure is not supported, and customers using those previous versions should plan for migration.**
- **Every user who wants to schedule a CMR Hybrid meeting must have a host account with Cisco TelePresence Session type assigned in the WebEx site.**
- **Any endpoints that can register with Cisco Unified CM and that are supported by the TelePresence Bridge can be used to join the Cisco CMR Hybrid meeting.**
- **Only devices managed by the Cisco TelePresence Management Suite (TMS) can use One Button to Push (OBTP) or the Auto Connect feature to join the CMR Hybrid meeting.**
- **Ensure that the Cisco Unified CM Neighbor Zone in Cisco Expressway-C is configured with Binary Floor Control Protocol (BFCP) enabled.**
- **Provision Hybrid Audio in the WebEx site to allow the use of SIP audio for the TelePresence Bridge and PSTN audio for WebEx participants.**
- **Cisco CMR Hybrid does not support Cisco WebEx Meetings Server.**
- **The TelePresence Bridge becomes the default host if no host is present when it joins the CMR Hybrid meeting, and the host privilege is reassigned to the host when he joins using the WebEx meeting client.**
- **The TelePresence Bridge will call into the WebEx Cloud at meeting start time even if no TelePresence or WebEx participant has joined yet.**
- **The organizer’s WebEx account and Outlook time zone should match; otherwise, the meeting scheduled in WebEx and in the Cisco TMS calendar will have different start times.**
- **Enable UDP for media streaming in the firewalls for the optimal video experience.**