CHAPTER 22

Cisco Collaboration Services

Revised: January 15, 2015; OL-30952-03

Cisco offers a wide range of collaboration technologies that have the ultimate goal of allowing users to work in collaborative environments that result in faster, more efficient decision-making processes and increased productivity. There are many technologies that fall under the large collaboration umbrella, but this chapter focuses on design guidance surrounding the Cisco offerings in collaborative conferencing through audio, video, and rich content sharing capabilities. This chapter also explores the differences in the various solutions and provides suggestions on when one solution may be a better fit than another.

The Cisco Collaboration services discussed in this chapter are available as on-premises, cloud, or hybrid deployments. This allows an organization to integrate with a Unified Communications 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. This chapter contains sections on the following topics:

- Cisco WebEx Software as a Service, page 22-5, (SaaS)
- Cisco WebEx Meetings Server, page 22-13, for private cloud
- Cisco Collaboration Meeting Room Hybrid, page 22-21 (formerly, Cisco WebEx Enabled TelePresence)
- Cisco Collaboration Meeting Room Cloud, page 22-31

Each section defines the high-level architecture of the solution, followed by design guidance for high availability, capacity planning and other design considerations pertinent to the solution.

What's New in This Chapter

This chapter incorporates new material to bring together design discussions surrounding Cisco's collaboration offerings. If you are reading this chapter for the first time, Cisco recommends reading the entire chapter.

Table 22-1 lists the topics that are new in this chapter or that have changed significantly from the previous release of this document.

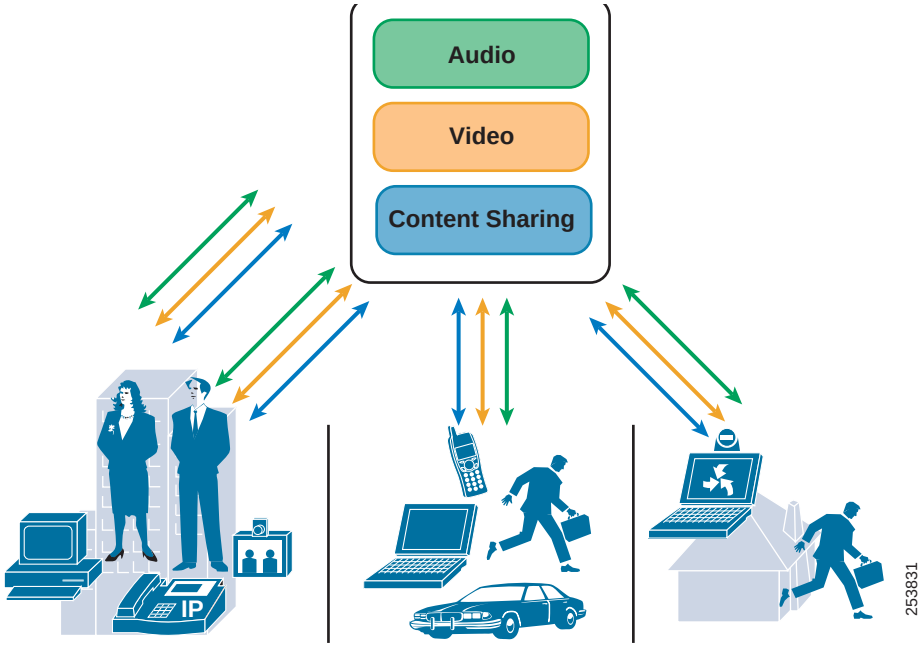
Table 22-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:	Revision Date
Cisco Collaboration Meeting Room (CMR) Hybrid (formerly, Cisco WebEx Enabled TelePresence)	Cisco Collaboration Meeting Room Hybrid, page 22-21	January 15, 2015
Cisco Collaboration Meeting Room (CMR) Cloud	Cisco Collaboration Meeting Room Cloud, page 22-31	January 15, 2015
Multiple data centers	Multiple Data Center Design, page 22-18	January 15, 2015
Removed information on Cisco Unified MeetingPlace, Cisco WebEx Social, and Cisco WebEx Meetings	No longer in this document	January 15, 2015
Minor updates for Cisco Collaboration Systems Release 10.0	Design Considerations, page 22-30, and various other sections of this chapter	November 19, 2013

Collaborative Conferencing Architecture

At a high level, collaborative conferencing involves receiving audio, video, and content from some or all of the attendees in a meeting, mixing those streams, and then sending the mixed audio, video, and content back to the attendees. Figure 22-1 illustrates a logical conference involving both internal and external participants, mobile and remote workers, or even attendees from other organizations.

Figure 22-1 Logical View of Collaborative Conferencing



These three aspects of a collaborative conference – audio, video and content sharing – are not exclusive. Cisco collaborative conferencing solutions integrate the three to create an enhanced user experience. Features such as the ability to determine active speakers, muting users from the content share interface, or choosing the video layout displayed in the content share, all imply that these three elements are integrated by the solution. All the collaborative conferencing solutions discussed in this chapter use the Cisco WebEx interface for content sharing. This provides a very consistent user experience across all the solutions.

When considering which conferencing solution is best for a given organization, many factors should be evaluated. Characteristics of an organization's users (number of remote workers, access capabilities, and video usage) as well as the range of available endpoints and their capabilities are important to consider. Video requirements such as high definition or interworking with an existing video infrastructure can also dictate a solution. The nature of the meetings themselves (for example, training scenarios, collaborative meetings, or how many meeting participants are external to the organization) is a critical characteristic to identify. Of course, initial cost, maintenance costs, and return on investment (ROI) all play a role as well.

One of the first delineations between the solutions is whether the resources performing each type of conferencing (or mixing) are located on-premises or off-premises. Access to cloud services, the size of the mobile workforce, and support staff levels are all considerations. Cisco WebEx Software as a Service (SaaS) offers a completely off-premises solution, while Cisco Collaboration Meeting Room (CMR)

Hybrid is a hybrid solution with a mix of on-premises and off-premises equipment. Organizations that have deployed Cisco Unified Communications will benefit most from leveraging an on-premises solution. The later sections provide more detailed deployment options for each collaborative conferencing solution.

Table 22-2 summarizes available solutions from an on-premises cloud perspective.

Table 22-2 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	Yes[1]	No	Yes	No
Cisco WebEx SaaS	No	Yes	No	Yes[1]	No	Yes
Cisco CMR Hybrid	Yes	Yes	Yes	Yes	Yes	Yes
Cisco CMR Cloud	No	Yes	No	Yes	No	Yes

1. Cisco WebEx webcam video only and no support with standards-based video.

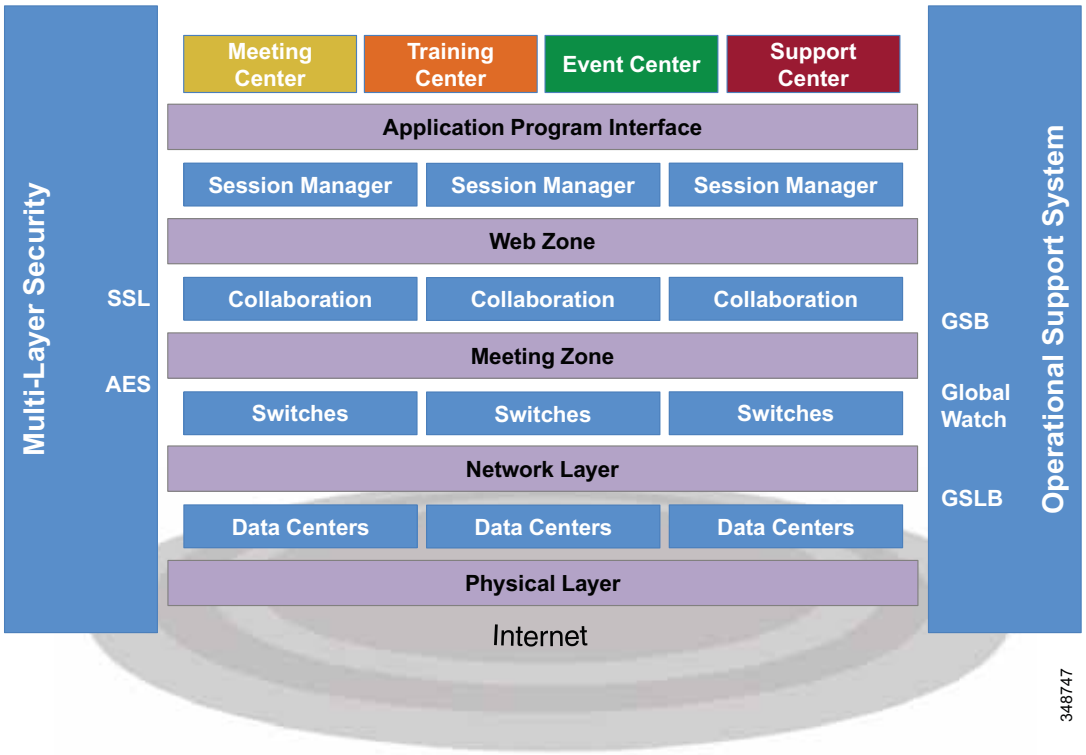
Cisco WebEx Software as a Service

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, and do not require connectivity back into the enterprise. 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 22-2 shows the Cisco WebEx Collaboration Cloud architecture.

Figure 22-2 Cisco WebEx Collaboration Cloud Architecture



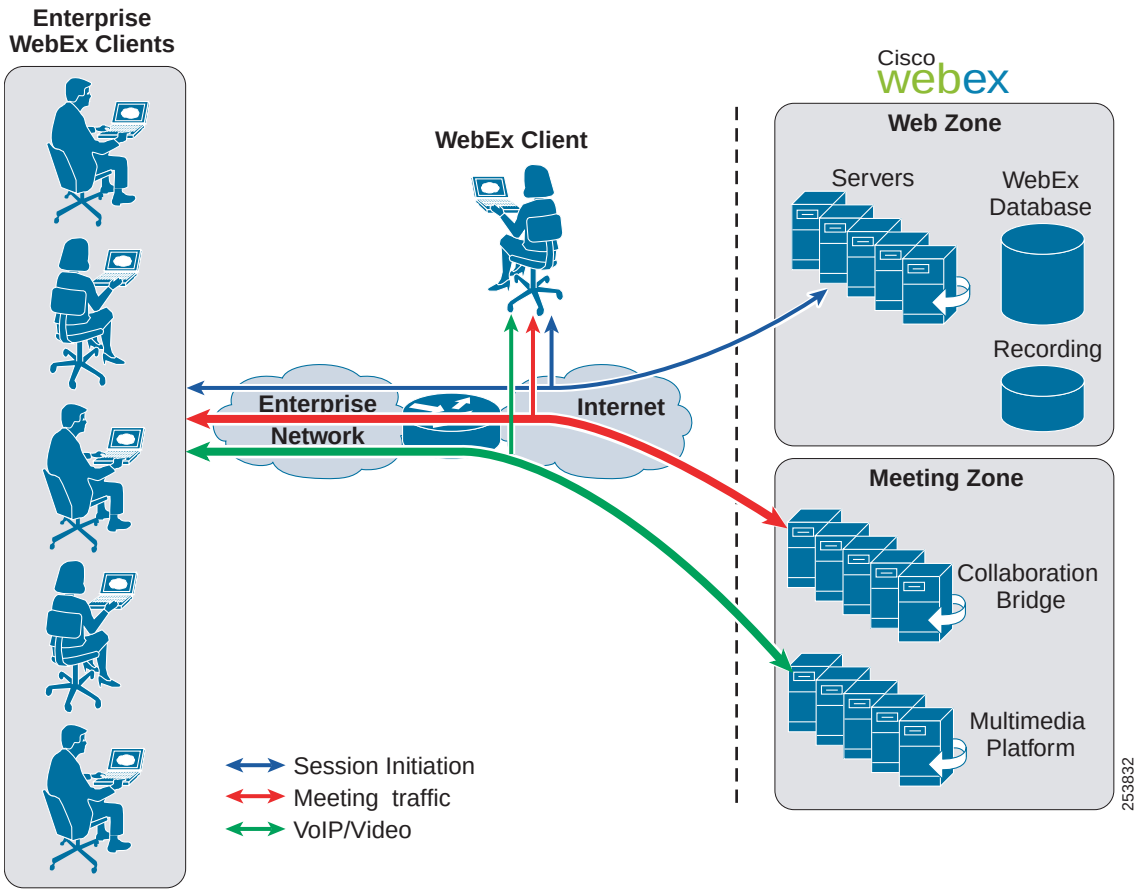
This network is purpose-built for real-time communications and has been specially formulated to minimize latency associated with TCP-layer flows. The network consists of application-specific multimedia switches at key peering points to handle rapid session traffic and to guarantee a high quality of service 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 client running on the computer or mobile device. 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 22-2. 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 22-3, 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.

Figure 22-3 WebEx Deployment



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 22-12.

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 22-12.

For details on IM and Presence services delivered by WebEx Collaboration Cloud, see the chapter on Cisco Unified CM IM and Presence Service, page 20-1.

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 current 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

http://www.cisco.com/en/US/products/ps12584/prod_white_papers_list.html

Note Enhanced WebEx security options are available only for Meeting Center meetings. The WebEx security options come at no additional cost.

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. For more information on WebEx Productivity Tool, refer to the WebEx *Productivity Tools FAQs*, available at

https://welcome.webex.com/docs/T27LD/mc0805ld/en_US/support/productivitytools_faq.htm

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

https://developer.cisco.com/site/webex-developer/develop-test/sso/reference/

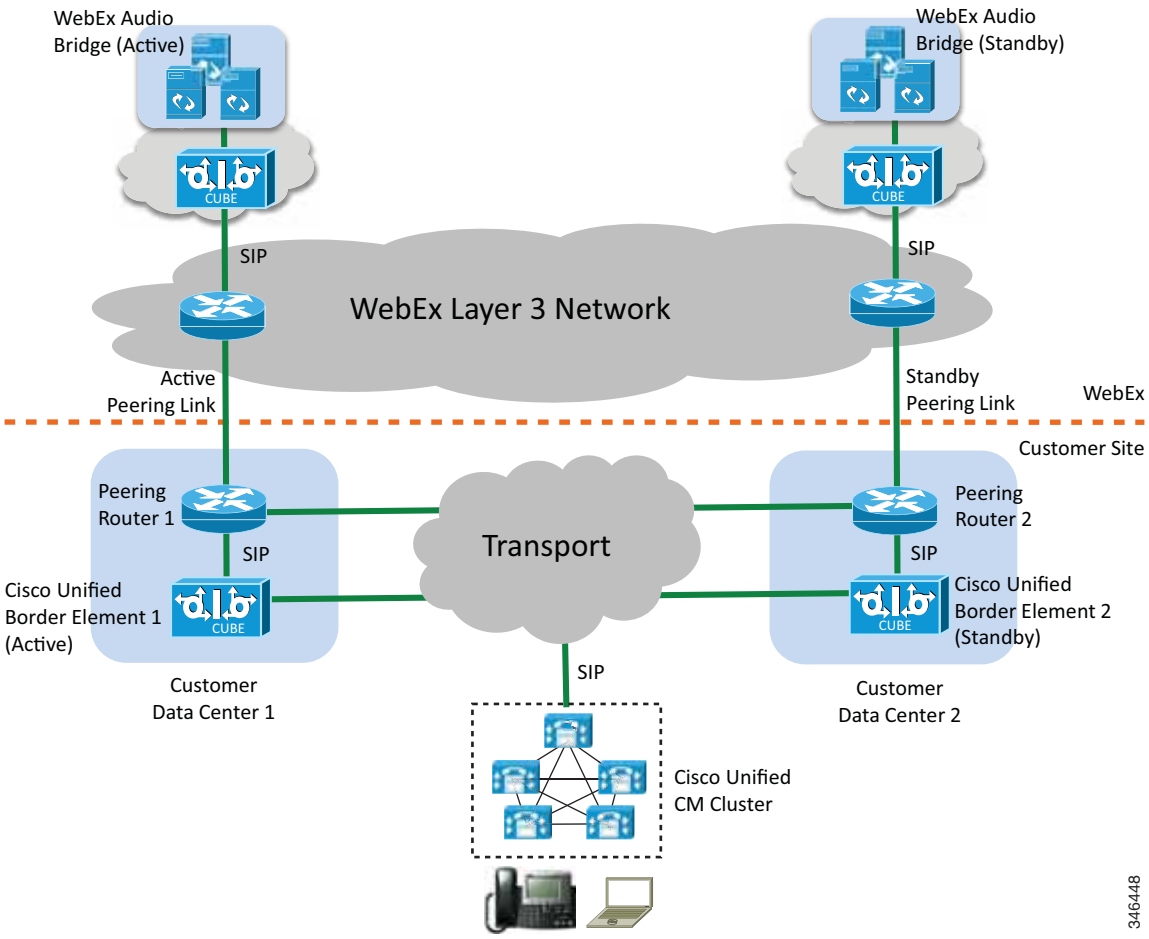
High Availability

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 22-4). 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.

Figure 22-4 Cisco WebEx Cloud Connected Audio High-Level Design



As shown in Figure 22-4, 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 customer the 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

http://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

http://www.cisco.com/en/US/prod/ps10352/product_comparison.html

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

http://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white_paper_c11-691351.html

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 Unified Communications Sizing Tool is available at http://tools.cisco.com/cucst.
- 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.
- Provision sufficient bandwidth for conference video and data traffic. See Network Traffic Planning, page 22-19, for details.
- Based upon business requirements, design decisions have to be made about the following:
  - User creation and authentication options (see User Profile, page 22-9, for details)
  - Meetings scheduling options (see Scheduling, page 22-8, for details)
- Cisco WebEx SaaS uses the multi-layer security model, and security extends from the WebEx infrastructure to the organization and individual meeting layer. There are various security options available, and depending on the business requirements., an organization can implement different levels of security. For security options and considerations, refer to the white paper *Unleash the Power of Highly Secure, Real-Time Collaboration*, available at

  http://www.cisco.com/en/US/products/ps12584/prod_white_papers_list.html

- For more details on the various Cisco collaborative client offerings and how they fit into collaborative conferencing solutions, see Cisco Collaboration Clients, page 21-1.

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

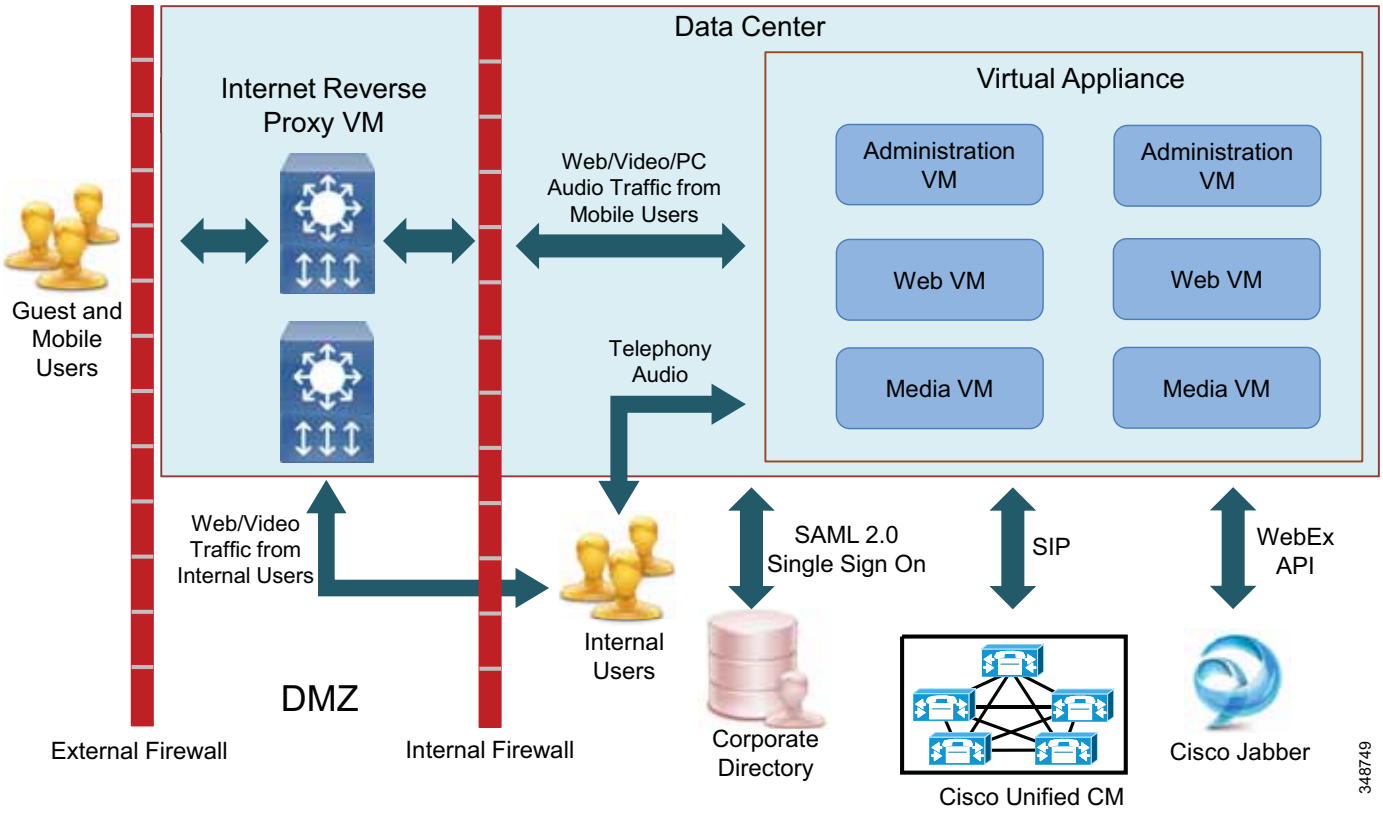
These capabilities are discussed in more detail in the following sections.

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 22-5 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 http://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.

Figure 22-5 Cisco WebEx Meetings Server High-Level Architecture

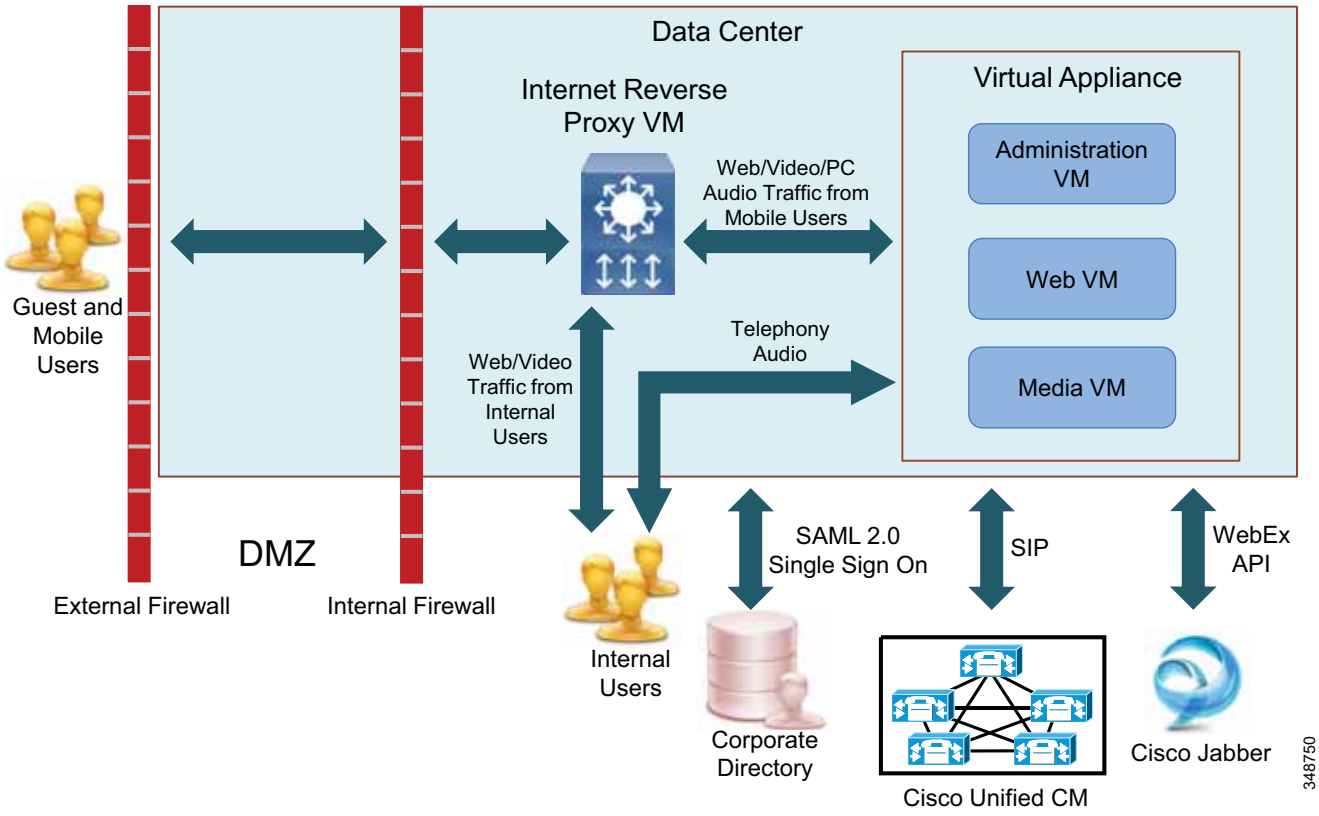


Cisco WebEx Meetings Server offers the option of deploying the Internet Reverse Proxy (or edge servers) in the DMZ to facilitate external access. This option provides two advantages. First, all external participants can securely access the WebEx conferences from the internet without going through a VPN. 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 22-6.

Figure 22-6 Internet Reverse Proxy Behind the Internal Firewall



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.

Note Cisco WebEx Meetings Server supports Meeting Center only.

Note 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 http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

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

http://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

For further details on PBX interoperability with Unified CM, refer to the documentation available at

http://www.cisco.com/en/US/solutions/ns340/ns414/ns728/networking_solutions_products_genericcontent0900aecd805b561d.html

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

http://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

http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html

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 participant 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

http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html

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 27-42.

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

http://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html

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 22-12.)

- Web collaboration bandwidth

  Web collaboration bandwidth for WebEx Meetings Server can be estimated the same way as WebEx SasS. (See Network Traffic Planning, page 22-12.)

- 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

  http://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 Unified Communications Sizing Tool is available at http://tools.cisco.com/cucst.
- 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 collaborative client offerings and how they fit into collaborative conferencing solutions, see the chapter on Cisco Collaboration Clients, page 21-1.
- 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 Call Admission Control, 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

http://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html

Cisco Collaboration Meeting Room Hybrid

Cisco Collaboration Meeting Room (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 22-7, 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.

For details on integrating Cisco Unified CM with Cisco Expressway, refer to the latest version of the *Cisco Expressway and CUCM via SIP Trunk Deployment Guide*, available at

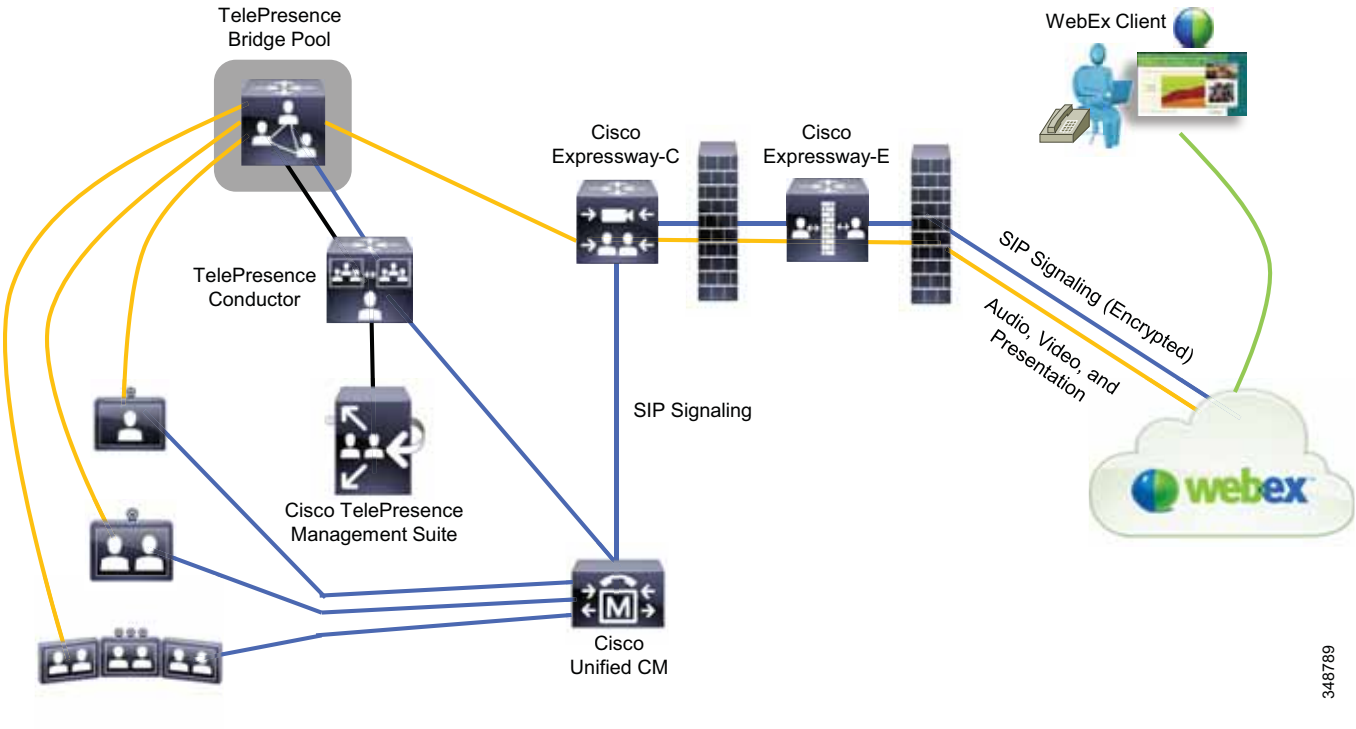
http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

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.

Figure 22-7 Cisco CMR Hybrid Using WebEx Audio with SIP



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-E and Expressway-C, 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. Starting with WBS 29.11, 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, refer to the chapter on Cisco Rich Media Conferencing, page 11-1.

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 Room 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

http://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html

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 *Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide*, available at

http://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html

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

http://developer.cisco.com/web/webex-developer/sso-reference

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 can be either self-signed or 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

http://www.cisco.com/en/US/products/ps11338/products_installation_and_configuration_guides_list.html

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 22-26, including Cloud Connected Audio
- WebEx Audio Using PSTN, page 22-26
- Teleconferencing Service Provider Audio, page 22-27

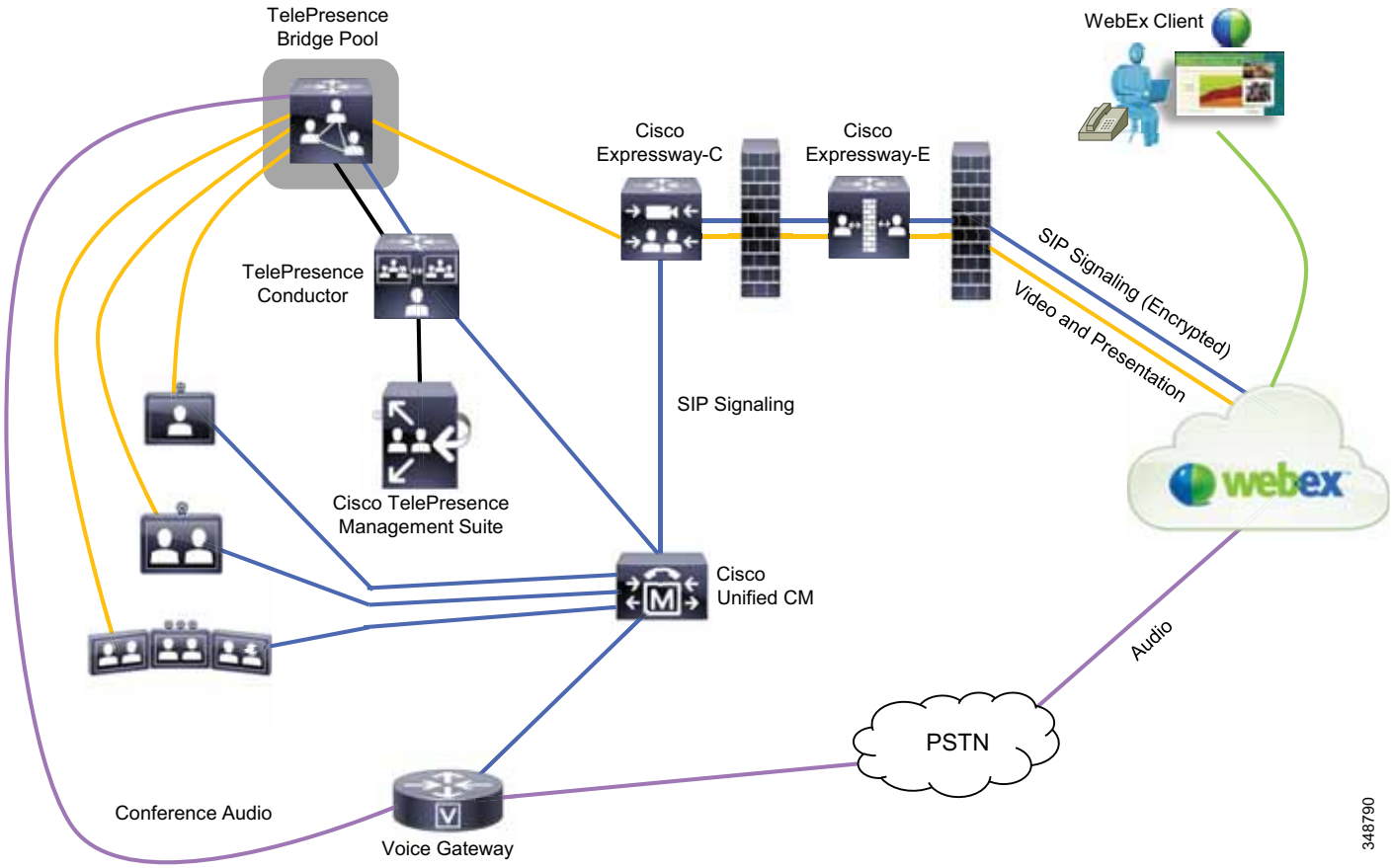
WebEx Audio Using SIP

Figure 22-7 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 22-8 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.

Figure 22-8 Cisco CMR Hybrid Using WebEx Audio with PSTN

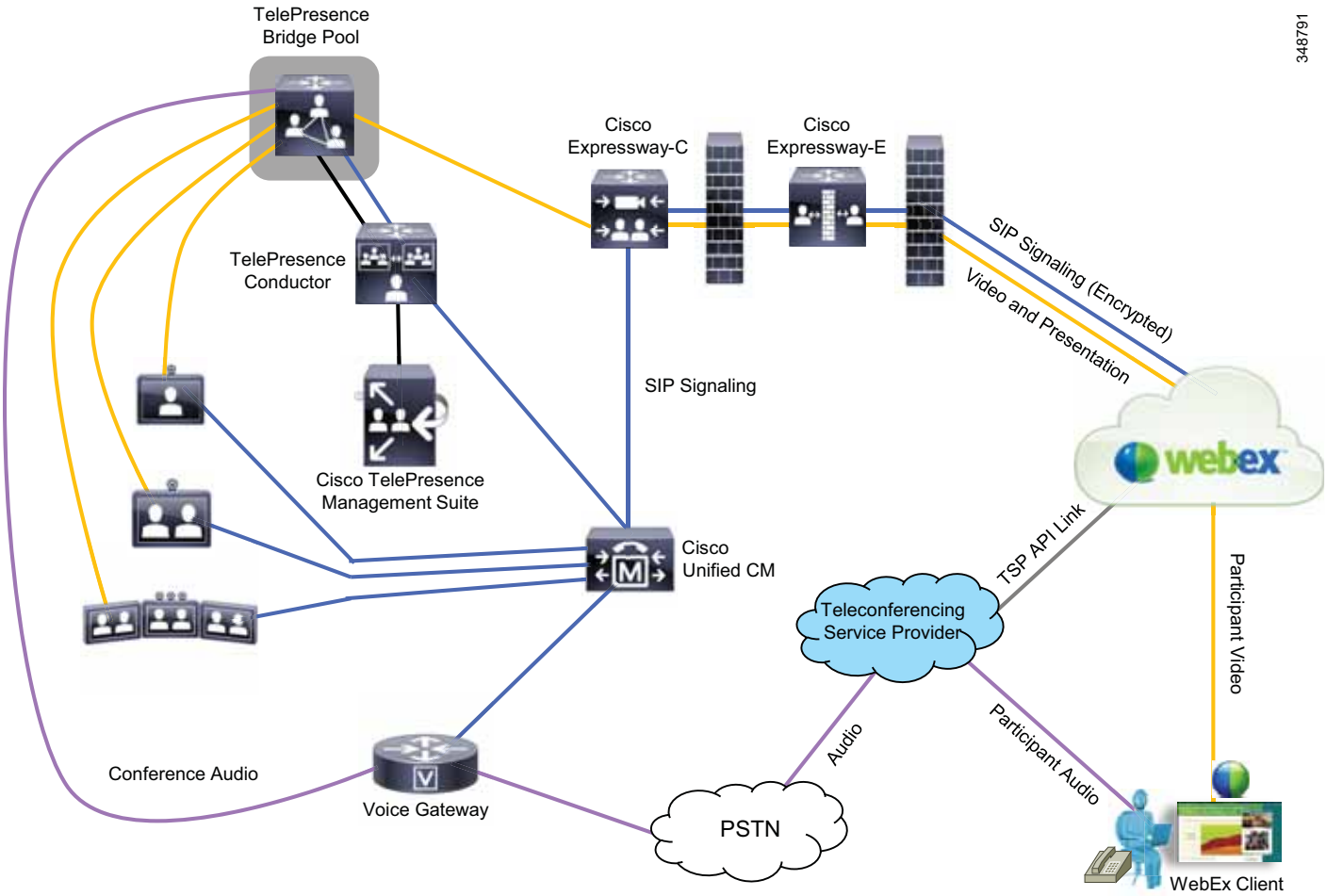


The dial-out number returned from WebEx is in full E.164 number format (for example, +14085551212). The dial plan design in Cisco Unified CM should take into account the handling of E.164 numbers. For dial plan design with Cisco Unified CM, see the chapter on Dial Plan, page 14-1.

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 22-9). The TSP link between WebEx and TSP provides the advanced conference control features.

Figure 22-9 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 22-5.

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 Cisco Expressway clustering, refer to the latest version of the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, available at

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

For resiliency of the TelePresence conferencing infrastructure, see the chapter on Cisco Rich Media Conferencing, page 11-1.

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 8-39.

- 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 section on Capacity Planning for Cisco Rich Media Conferencing, page 11-37.

- 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 27-1.

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

  http://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.

Cisco Collaboration Meeting Room Cloud

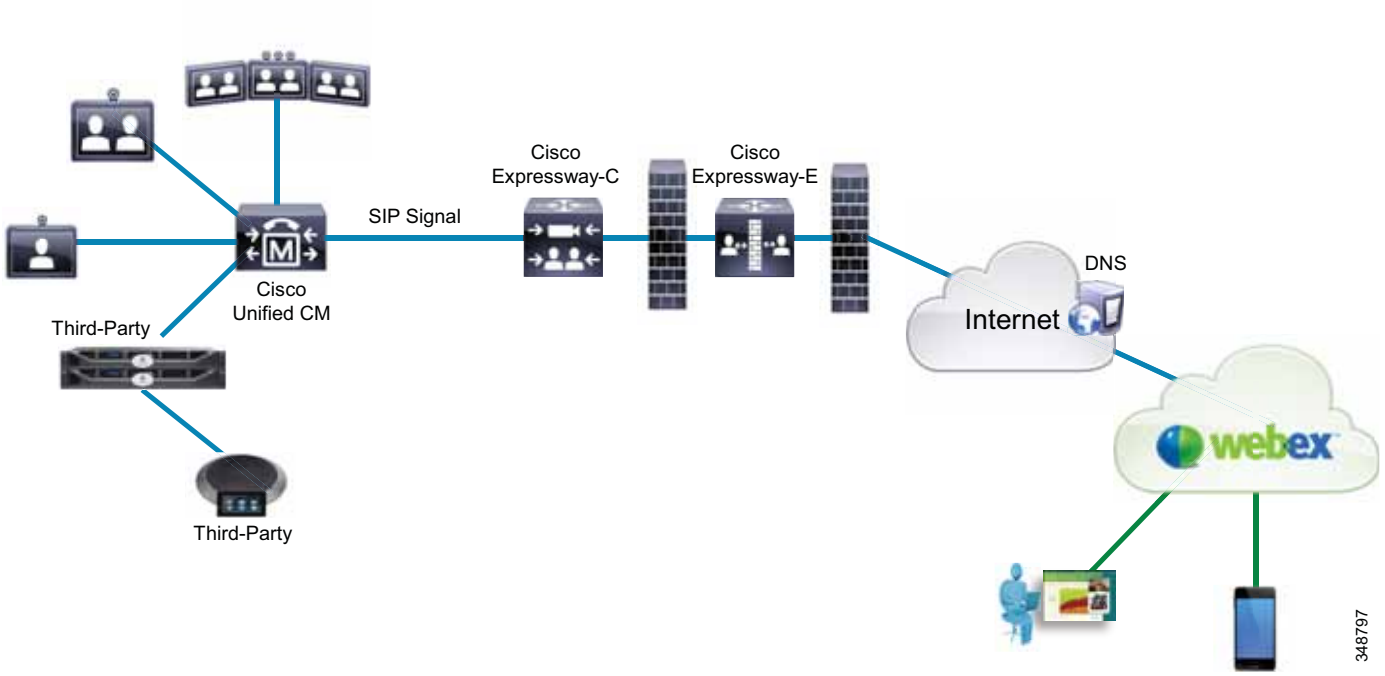
Cisco Collaboration Meeting Room (CMR) Cloud is an enterprise-grade collaboration service that provides a consistent, scalable virtual meeting room experience that combines business quality video, audio, and data sharing capabilities into a single solution delivered through Cisco WebEx Collaboration Cloud. It integrates with the Cisco Collaboration infrastructure and applications such as Cisco Unified CM, Cisco Expressway, and Cisco WebEx. Participants can join CMR Cloud 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 Cloud, and participants can join the meeting regardless of their location using any device of their choice (desktop, mobile, or video endpoint). With CMR Cloud, 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 22-10 illustrates the Cisco CMR Cloud 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 Cloud, and it routes the video calls to 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 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.

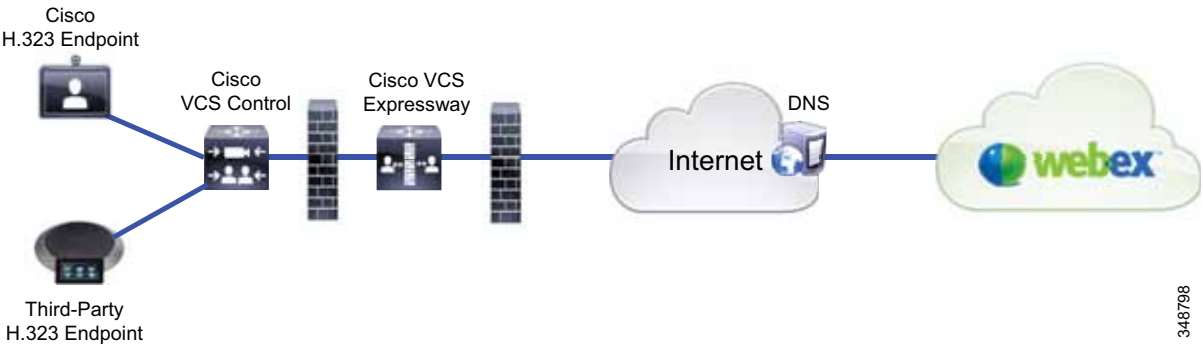
Note For existing Cisco VCS customers, using VCS Control as a SIP Registrar for SIP endpoints and VCS Expressway for firewall traversal is supported with the deployment.

Figure 22-10 Cisco Collaboration Meeting Room Cloud Architecture Using SIP Video



Cisco CMR Cloud architecture also support H.323 video devices (see Figure 22-11). 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.

Figure 22-11 Cisco Collaboration Meeting Room Cloud Architecture Using H.323 Video



Alternatively, Cisco CMR Cloud can be deployed using H.323 video without a call control system (see Figure 22-12). 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.

Figure 22-12 Cisco Collaboration Meeting Room Cloud Architecture Using H.323 Video Without Call Control System

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 CMR Cloud deployment. For details, refer to *Cisco Collaboration Meeting Rooms (CMR Cloud) Enterprise Deployment Guide*, available at

http://www.cisco.com/c/en/us/support/conferencing/webex-meeting-center/products-installation-and-configuration-guides-list.html

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 CMR Cloud uses H.264 video for active speaker and content sharing. Depending on the capability of the device and the bandwidth available, CMR Cloud 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. 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 condition (severe packets loss, for example), 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. Starting with release WBS 29.11, 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 CMR Cloud meeting has an associated video address URI and URL. Participants dial the URI on the video device or click on the URL to bring up the WebEx meeting client to join the meeting. A CMR Cloud meeting can be one of the following types:

- Scheduled meeting

  Users can use WebEx Productivity Tools to schedule Cisco CMR Cloud 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, user can schedule CMR Cloud meetings from the WebEx portal but the host has to first schedule the meeting from WebEx, and then create an invitation with meeting detail attached and send it to all the participants.

- 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 enabled, a fixed URI and URL are assigned to the 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.

- 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 instantiated from the Meeting Center or the user's personal room.

Security

Cisco CMR Cloud 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 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 the list of the trusted Root Certificate Authorities, refer to *Cisco Collaboration Meeting Rooms (CMR Cloud) Enterprise Deployment Guide*, available at

http://www.cisco.com/c/en/us/support/conferencing/webex-meeting-center/products-installation-and-configuration-guides-list.html

For SIP based calls, Cisco CMR Cloud 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 to *Cisco Collaboration Meeting Rooms (CMR Cloud) Enterprise Deployment Guide*.

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

- 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.

For Cisco Expressway clustering, refer to the latest version of the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, available at

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

Capacity Planning

Cisco CMR Cloud 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 CMR Cloud meeting, it consumes 3 video devices from the video device capacity limit.

Capacity planning for Cisco CMR Cloud 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 CMR Cloud meetings. For capacity details, see the chapter on Collaboration Solution Sizing Guidance, page 27-1.

- Cisco Expressway

  Cisco Expressway must provide enough resources to handle the traversal call traffic for the deployment. For capacity details, see the chapter on Cisco Collaboration Services, page 22-1.

Network Traffic Planning

Network traffic planning for Cisco CMR Cloud 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 the receiving client automatically selects the best possible resolution to receive video that typically requires 1.2 to 3 Mbps available bandwidth. For more information regarding network traffic planning for WebEx clients, refer to the *Cisco WebEx Network Bandwidth* white paper, available at

  http://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white_paper_c11-691351.html

- 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 CMR Cloud:

- 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 port range details, refer to *Cisco Collaboration Meeting Rooms (CMR Cloud) Enterprise Deployment Guide*, available at

  http://www.cisco.com/c/en/us/support/conferencing/webex-meeting-center/products-installation-and-configuration-guides-list.html

- 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.