Preferred Architecture for Cisco Webex Hybrid Services

Cisco Validated Design (CVD) Guide

Revised: May 31, 2019

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

First Published: October 28, 2014

Preface

Revised: May 31, 2019

Cisco Validated Designs (CVDs) explain important design and deployment decisions based on common use cases and current system releases. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented the guidelines within the CVDs in order to provide faster, more reliable, and fully predictable deployments. CVDs provide a tested starting point for Cisco partners and customers to begin designing and deploying systems using their own setup and configuration.

Documentation for Collaboration Solutions

Cisco Preferred Architecture (PA) Design Overview guides help customers and sales teams select the appropriate architecture based on an organization's business requirements; understand the products that are used within the architecture; and obtain general design best practices. These guides support sales processes.

Cisco Validated Design (CVD) guides provide detailed steps for deploying the Cisco Preferred Architectures. These guides support planning, design, and implementation of the Preferred Architectures.

Cisco Collaboration System Solution Reference Network Design (SRND) guide provides detailed design options for Cisco Collaboration solutions. The SRND should be referenced when design requirements are outside the scope of Cisco Preferred Architectures.

About This Guide

This Cisco Validated Design guide for the Webex Hybrid Services Preferred Architecture is for:

- Sales teams that sell, design, and deploy collaboration solutions
- Customers and sales teams who want detailed design best practices and ordered steps for deploying Webex Hybrid Services

Readers of this guide should have a general knowledge of Cisco voice, video, and collaboration products and a basic understanding of how to deploy those products. We recommend that readers review the Preferred Architecture for Cisco Webex Hybrid Services, Design Overview before reading this CVD document.

The design decisions within this CVD are in line with the framework outlined in the latest version of the Cisco Collaboration SRND. While the SRND offers many design and deployment options, in this document a single deployment recommendation is selected based on fundamental assumptions for the Preferred Architecture design. Different assumptions can certainly lead to different design decisions, which then should be validated against the SRND. For large deployments with unique needs and advanced customization, we recommend working with your Cisco Account Manager for guidance beyond that contained in this CVD or the SRND.

This guide simplifies the design and sales process by:

- Building upon the product and design recommendations of the Preferred Architecture for Cisco Webex Hybrid Services, Design Overview
- Detailing a collaboration architecture, identifying best practices, and explaining the reasoning behind those recommendations

This CVD guide is organized into the following discrete modules that integrate together to form the overall hybrid services solution:

- Cisco Webex Hybrid Directory Service — Simplifies user on-boarding by integrating directory services between the on-premises LDAP directory and the common identity service within the customer's Webex organization. This chapter describes, at a high level, how to deploy Webex Hybrid Directory Service within the Webex Hybrid Services solution.
- Cisco Webex Hybrid Calendar Service — Improves the end-user experience for managing meeting invitations, content, and communications with participants by synchronizing enterprise calendar services with the Webex Hybrid Calendar Service. This chapter describes, at a high level, how to deploy Webex Hybrid Calendar Service within the Webex Hybrid Services solution.
- Cisco Webex Video Mesh — Allows organizations to deploy an instance of Webex media processing on-premises so that Webex Teams endpoints and applications can terminate media on-premises instead of sending all media to the cloud. This chapter describes, at a high level, how to deploy Webex Video Mesh within the Webex Hybrid Services solution.
- Cisco Webex Hybrid Call Service — Provides integration of Cisco Unified Communications Manager call services with Webex. This chapter describes, at a high level, how to deploy Webex Hybrid Call Service within the Webex Hybrid Services solution.
- Bandwidth Management — Seeks to provide the best possible user experience end-to-end for all media capable endpoints, clients, and applications in the collaboration solution. This chapter describes, at a high level, how to deploy recommended bandwidth management techniques within the Webex Hybrid Services solution.
- Sizing Cisco Webex Hybrid Services — This chapter provides simplified examples to illustrate how to size the components of the Preferred Architecture for Webex Hybrid Services to fit the requirements of your deployment.

Revision History

This CVD guide may be updated at any time without notice. You can obtain the latest version of this document online at:

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

Visit the above website periodically and check for documentation updates by comparing the revision date of your copy with the revision date of the online document.

Table 1 lists the revision history for this document.

Table 1 Revision History for This CVD Guide

Revision Date	Comments
May 31, 2019	The architecture was updated to remove Call Service Aware. Other changes and corrections were made in various chapters.
February 11, 2019	Minor errors were corrected in several sections.
June 1, 2018	This document was updated with information for a new release of Cisco Webex Hybrid Services.
December 21, 2017	Initial release of this document.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Conventions

This document uses the following conventions:

bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Warning **Statements using this symbol are provided for additional information and to comply with regulatory and customer requirements.**

Introduction

Revised: May 31, 2019

The Preferred Architecture (PA) for Cisco Webex Hybrid Services is a Cisco Validated Design (CVD) built upon the foundation of the PA for Cisco Collaboration Enterprise on-premises deployments. It requires many of the same products and infrastructure components as well as the architecture and planning incorporated in the PA for on-premises deployments. Therefore we expect you to follow and implement the latest version of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*, available at https://www.cisco.com/go/pa, prior to deploying the PA for Cisco Webex Hybrid Services.

As part of implementing the PA for Webex Hybrid Services, there are a number of products and integrations covered in the latest version of the Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments that overlap with, and thus are not part of, the PA for Webex Hybrid Services. The areas of overlap include Cisco Meeting Server, Cisco Unified Communications Manager IM and Presence Service, and Cisco Jabber. This does not mean that these products and services cannot be deployed in an environment with Webex Hybrid Services, but that this PA for Webex Hybrid Services will not discuss or treat any design considerations around these on-premises products and services when they overlap with those included in the Webex Hybrid Services solution.

Note Please be aware that the Webex Hybrid Call Service architecture discussed in this document is currently going through a transitional phase. To better understand the future changes and how they will impact your deployment of the Webex Hybrid Services architecture, we recommend that you contact your Cisco account team before deploying the architecture described in this document.

Architectural Overview

The PA for Webex Hybrid Services provides end-to-end collaboration targeted for deployments where a collaboration solution based on Cisco Unified Communications Manager has been deployed. This architecture incorporates high availability for critical applications. The consistent user experience

provided by the overall architecture facilitates quick user adoption. Additionally, the architecture supports an advanced set of collaboration services that extend to mobile workers, partners, and customers through the following key services:

- Voice and video communications
- Messaging
- Meetings that incorporate high-definition video, web conferencing, and content sharing capabilities
- Services for mobile and remote workers

Because of the adaptable nature of Cisco endpoints and their support for IP networks, this architecture enables an organization to use its current data network and the Internet to support both voice and video calls. The preferred architecture provides a holistic approach to bandwidth management, incorporating an end-to-end QoS architecture and video rate adaptation and resiliency mechanisms to ensure the best possible user experience for deploying pervasive video over managed and unmanaged networks.

The PA for Webex Hybrid Services, shown in Figure 1-1, provides highly available and centralized on-premises and cloud services. These services extend easily to remote offices and mobile workers, providing availability of critical services even if communication to headquarters is lost. Centralized on-premises and cloud-based services also simplify management and administration of an organization's collaboration deployment.

Figure 1-1 Preferred Architecture for Cisco Webex Hybrid Services

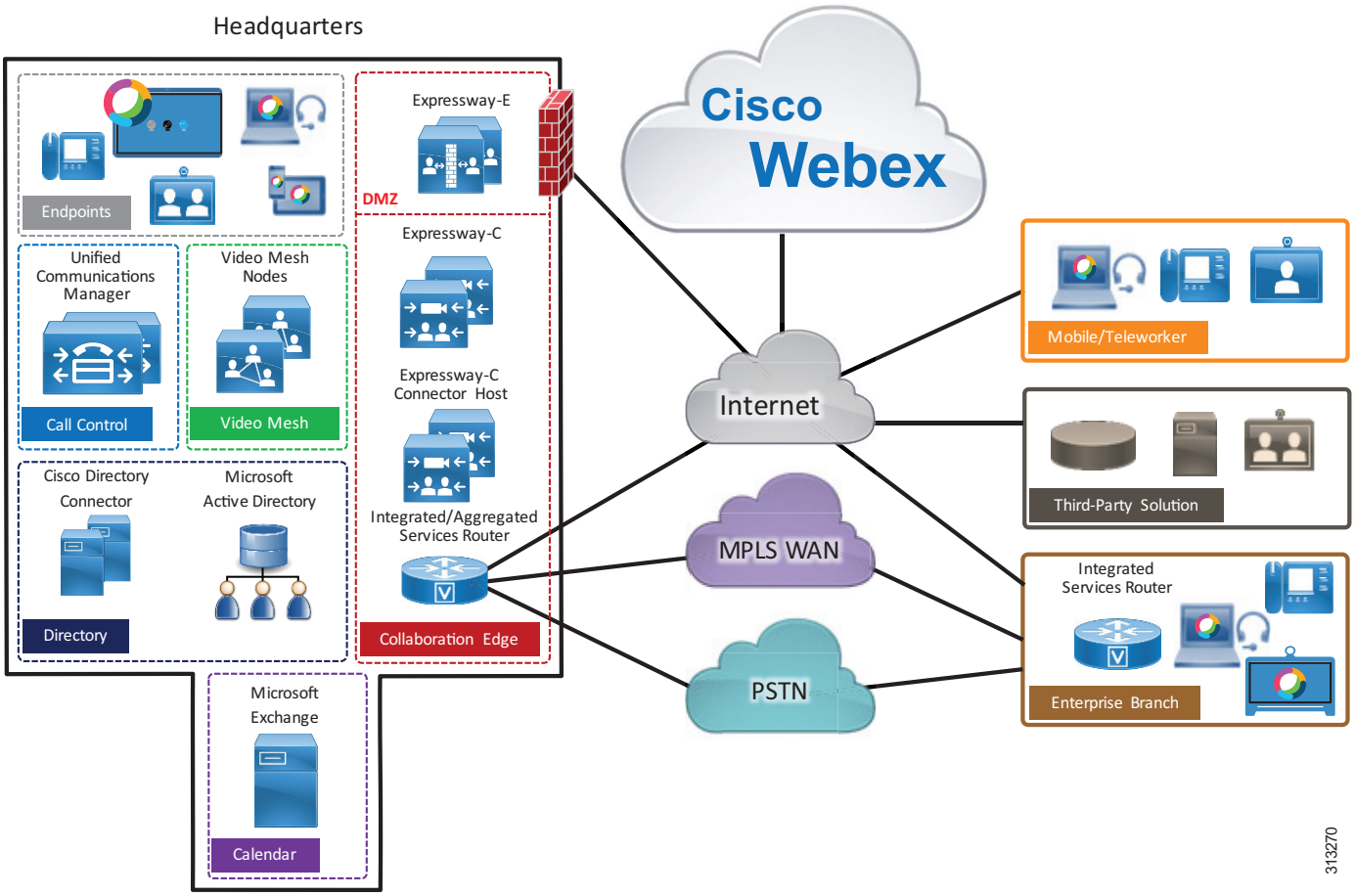


Table 1-1 lists the components in this architecture. For simplicity, the components are grouped into modules to help categorize and define their roles. The content in this guide is organized in the same modules.

Table 1-1 Components of the Preferred Architecture for Cisco Webex Hybrid Services

Module	Component	Description
Collaboration Endpoints	Cisco IP Phones, Cisco Video Endpoints and Room Devices, and Cisco Webex Teams	Enable real-time message, meeting, and voice/video communications for users
Webex Core Services	Cisco Webex Control Hub	Web portal that enables provisioning and management of enterprise Webex Teams users and services; registration of endpoints, clients, and Expressway-C Connector Host to Webex; and Expressway Connector upgrades
	Cisco Webex Messaging	Provides persistent messaging and content sharing in 1:1 and group-based spaces
	Cisco Webex Meetings	Provides audio/video meetings, with content sharing and web conferencing capabilities for meetings
	Cisco Expressway-C Connector Host Management Connector	Enables connectors hosted on Expressway-C to be managed by the Webex Control Hub
Cisco Webex Hybrid Directory Service	Cisco Directory Connector	Provides directory synchronization between Microsoft Active Directory and Webex
	Microsoft Active Directory	Provides the full list of corporate resources and users and their attributes
Cisco Webex Hybrid Calendar Service	Cisco Expressway-C Connector Host Calendar Connector	Provides integration between the enterprise calendaring application and Webex
	Microsoft Exchange	Provides corporate calendaring services
Cisco Webex Video Mesh	Cisco Webex Video Mesh Node	Provides on-premises media processing capabilities for Webex. This includes voice, video, and desktop sharing for on-premises and cloud registered devices.
Cisco Webex Hybrid Call Service	Cisco Unified Communications Manager (Unified CM)	Provides endpoint registration, call processing, and media resource management
	Cisco Expressway-C Connector Host Call Connector	Provides integration between on-premises call processing services and Webex
	Cisco Expressway-C and Expressway-E	Enables interoperability and firewall traversal with Webex

High Availability

The PA for Webex Hybrid Services provides high availability for all deployed on-premises applications by means of the underlying clustering mechanism present in all Cisco Unified Communications applications. Clustering replicates the administration and configuration of deployed applications to backup instances of those applications. Likewise, cloud services are natively redundant by virtue of elastic compute and highly available service distribution within the cloud platform.

If an instance of an application or services fails, Cisco on-premises and cloud-based services such as endpoint registration, call processing, messaging, and many others continue to operate on the remaining instance(s) of the application or service. This failover process is transparent to the users. In addition to clustering, the PA for Webex Hybrid Services provides high availability through the use of redundant power, network connectivity, and elastic storage.

Sizing Considerations

Sizing a deployment can become complex for large enterprises with sophisticated requirements. This PA for Webex Hybrid Services presents some examples that simplify the sizing process. For details, see the chapter on Sizing Cisco Webex Hybrid Services.

Licensing

Details about the individual licenses for the endpoints and infrastructure components in the PA for Webex Hybrid Services are beyond the scope of this document. Information about Cisco Collaboration Flex Plan licensing is available at

https://www.cisco.com/c/en/us/products/unified-communications/collaboration-flex-plan/index.html

Collaboration Endpoints

The recommendations within this Preferred Architecture assume a deployment of Cisco voice and video endpoints, including the Webex Teams application. Some of the endpoint use SIP to register to Cisco Unified Communications Manager (Unified CM) on-premises, while others use HTTPS to connect to the Webex Hybrid Services. Table 1-2 lists the preferred endpoints for optimal features, functionality, and user experience.

Table 1-2 Cisco Collaboration Endpoints

Product	Description
Mobile: • Cisco Webex Teams for Android • Cisco Webex Teams for iPhone and iPad **Desktop:** • Cisco Webex Teams for Mac • Cisco Webex Teams for Windows **Web browser:** • Cisco Webex Teams web client	Application with cloud-based integrated voice/video meeting, calling, messaging, and content sharing for mobile devices, personal computers, and web browsers.
Cisco IP Phone 8800 Series	General office use, multiple-line audio and video phones
Cisco IP Phone 8832	IP conference phone
Cisco Webex DX80	Personal TelePresence endpoint for the desktop
Cisco Webex Room Kit Series	TelePresence multipurpose and integrator room endpoints

Table 1-2 Cisco Collaboration Endpoints (continued)

Product	Description
Cisco Webex Room Series	TelePresence multipurpose and integrator room endpoints with built-in single or dual screens
Cisco Webex Board	All-in-one presentation, white board, and audio/video multipurpose room endpoint

Webex Core Services

The PA for Webex Hybrid Services includes the following foundational components and services that underlie the entire Webex Hybrid Services solution. All of these services and components are relevant for the deployment of the PA for Webex Hybrid Services, and they are referenced as appropriate in the remainder of this document.

Cisco Webex Control Hub

The web-hosted online Webex Control Hub, available at https://admin.webex.com/, is used to administer and manage an organization's Webex services.

After logging into the control hub, the administrator is presented with the overview screen, which provides a one-screen snapshot of the organization and the status and utilization of cloud services. Clickable tiles on the overview screen allow quick drill-down to more information and configuration for various features and services.

The left-hand navigation menu of the Webex Control Hub provides links to various management and provisioning areas within the web-based portal, including:

- Users — Area for managing users and provisioning them for cloud services.
- Places — Area for managing physical locations containing a device (for example, a meeting room).
- Services — Area for managing and configuring cloud services, including Webex Hybrid Services.
- Devices — Area for managing and provisioning cloud-registered room systems and Cisco Webex Boards.
- Reports — Area for viewing diagnostics and reports and reviewing and analyzing cloud and hybrid service metrics, including service and device utilization, call quality, and other statistics.
- Support — Area for finding documentation and other support resources.
- Settings — Area for managing base global organizational settings.

Cisco Webex Messaging

One of the key features of the Webex Teams application and the Webex platform is one-to-one and group messaging with file sharing. This feature delivers persistent instant messaging with Webex Teams spaces, where users can message and share files. Spaces are manually or dynamically created based on user work flows, and spaces can be grouped into teams to provide team-focused spaces across organizations.

Cisco Webex Meetings

Meetings are another key feature of the Webex platform utilized by Webex Teams applications and endpoints. Webex Meetings provides voice and video conferencing along with screen sharing by leveraging the Webex conferencing service. Webex Meetings builds upon and leverages the messaging and file sharing capabilities of Webex Messaging. Webex Meetings also enables permanent Personal Meeting Rooms (PMR) to provide users with personalized permanent voice and video meeting spaces.

Cisco Expressway-C Connector Host Management Connector

The Cisco Expressway-C Connector Host is a standard Cisco Expressway-C server deployed within the customer's organization to provide an integration point between the on-premises and cloud collaboration services. The integration between the Cisco Expressway-C server and Webex is facilitated via micro-services installed and managed on the Expressway-C Connector Host by Webex. These micro-services enable integration of Webex Hybrid Services.

The Management Connector is included in the Expressway-C base software and is used by the administrator to register Expressway to Webex and to link the Expressway interface with the Webex management interfaces.

The Management Connector plays an important role as the coordinator of all connectors running on the Expressway server or cluster. It provides the administrator with a single point of control for connector activities. The Management Connector enables Webex-based management of the on-premises connectors, handles initial registration with Webex, manages the connector software life cycle, and provides status and alarms.

The Management Connector requires that certificates of the Certification Authorities (CA) that signed the certificates in use by Webex must be in the trusted list of the Expressway-C connector host, so that the HTTPS connection can be established. The administrator can decide to allow Webex to upload CA certificates to the Expressway-C trust store. Or, in cases where security policies prevent Webex from uploading trusted CA certificates on Expressway-C, the administrator may upload them manually.

Cisco Webex Hybrid Directory Service

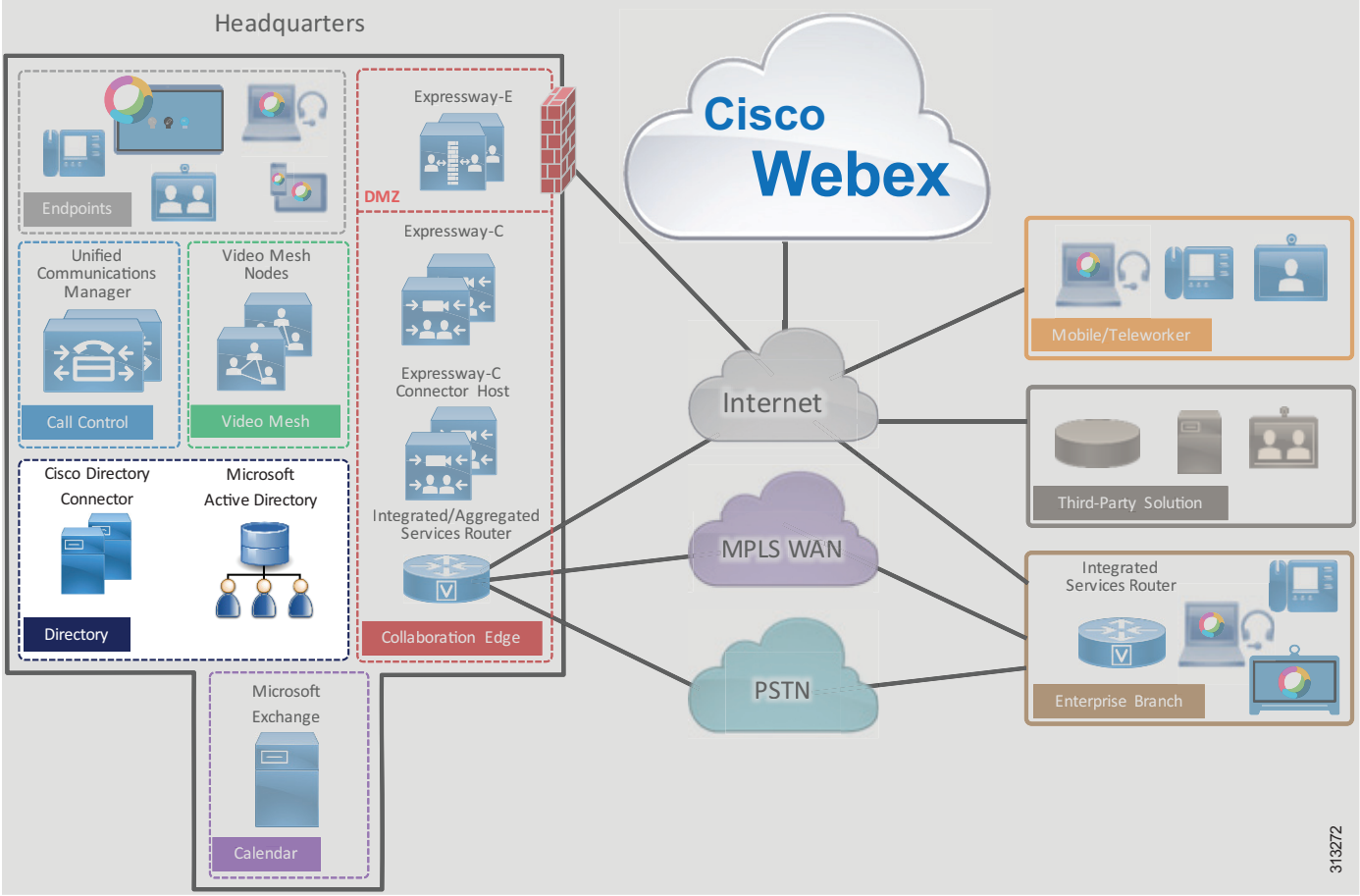
Revised: May 31, 2019

Cisco Webex Hybrid Services enable Webex Teams customers to connect on-premises collaboration services to Webex. Integrating directory services between the on-premises LDAP directory and the identity service within the customer's Webex Teams organization adds value by simplifying user on-boarding.

Overview

The Webex Hybrid Directory Service high-level architecture, depicted in Figure 2-1, allows the Webex Teams customer to synchronize their corporate Microsoft Active Directory with the identity store of their organization in Webex. This makes Webex Teams user on-boarding and service provisioning simple and consistent.

Figure 2-1 Cisco Webex Hybrid Directory Service High-Level Architecture



Prerequisites

Prior to implementing and deploying Webex Hybrid Directory Service, perform the following requirements:

- Deploy Microsoft Active Directory within the organization and populate it with user information.
- Make sure Cisco Unified Communications Manager (Unified CM) is fully integrated with Microsoft Active Directory (directory synchronization and authentication).
- If the on-premises network is behind a firewall, ensure that outbound access to the Internet through HTTPS on port 443 is available either directly or by way of an HTTP proxy.

Core Components

The core components for Cisco Webex Hybrid Directory Service include:

- Cisco Directory Connector
- Microsoft Active Directory

Recommended Deployment

To deploy Webex Hybrid Directory Service in the PA for Webex Hybrid Services, we recommend the following:

- Ensure that the end-user account mail ID field in the Unified CM End User database contains the user's email address. Webex Teams users correlate to Cisco Unified CM end users by means of email addresses. With LDAP directory integration, the mail ID field for Unified CM end users is typically mapped from the mail field of the LDAP directory during synchronization.
- Install Cisco Directory Connector on a separate Windows server from the Active Directory Domain Service or Active Directory Lightweight Directory Services.
- Run a first synchronization after the Directory Connector installation finishes. Then configure full synchronization and incremental synchronization schedules to keep the Directory Connector (and in turn Webex) updated when resource and user information changes (resource or user update, deletion, or addition) within Microsoft Active Directory.

Key Benefits

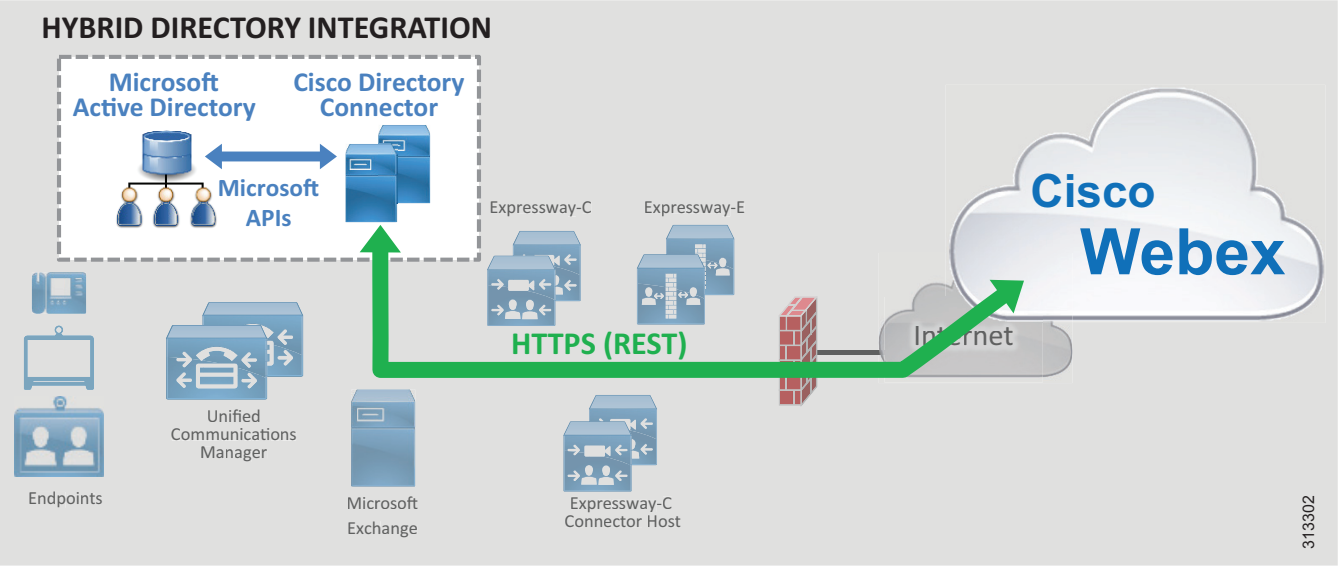
Webex Hybrid Directory Service provides the following benefits:

- Synchronization of identities, users, resources, and groups from the corporate Microsoft Active Directory to the cloud, and the creation of Webex Teams user accounts from this corporate directory source.
- HTTPS outbound connection from the enterprise to Webex on standard port 443, which is typically allowed by organizations and thus should not require additional configuration to open ports on the firewall. The organization's existing HTTP proxy may also be leveraged as required.
- Automatic, scheduled synchronization of users and resources from the enterprise Active Directory to Webex through the Cisco Directory Connector.
- Incremental synchronization and full synchronization to facilitate management of resource and user identity information.
- Custom attribute mappings between Microsoft Active Directory and Cisco Directory Connector for maximum flexibility.

Architecture

Figure 2-2 shows the Webex Hybrid Directory Service integration to the enterprise directory. This integration relies on the Cisco Directory Connectors, which are co-located in the central site with the Microsoft Active Directory. Cisco Directory Connector is deployed on two Microsoft Windows Servers for redundancy and high availability.

Figure 2-2 Architecture for Integration of Webex Hybrid Directory Service with the Enterprise Directory



Cisco Directory Connector relies on Microsoft Active Directory application programming interfaces (APIs) to pull user information from the Microsoft Active Directory. The APIs are based on the Microsoft .NET framework. Directory Connector uses HTTPS to push user information to the organization's Webex identity store.

Role of Cisco Directory Connector

Cisco Directory Connector plays the role of synchronization agent between the corporate Microsoft Active Directory and the organization's identity store in Webex. The Directory Connector initially populates Webex with user and resource information from the Active Directory and maintains this information with subsequent synchronizations to update the organization's Webex identity store with the latest moves, adds, changes, and deletions occurring on the enterprise Active Directory.

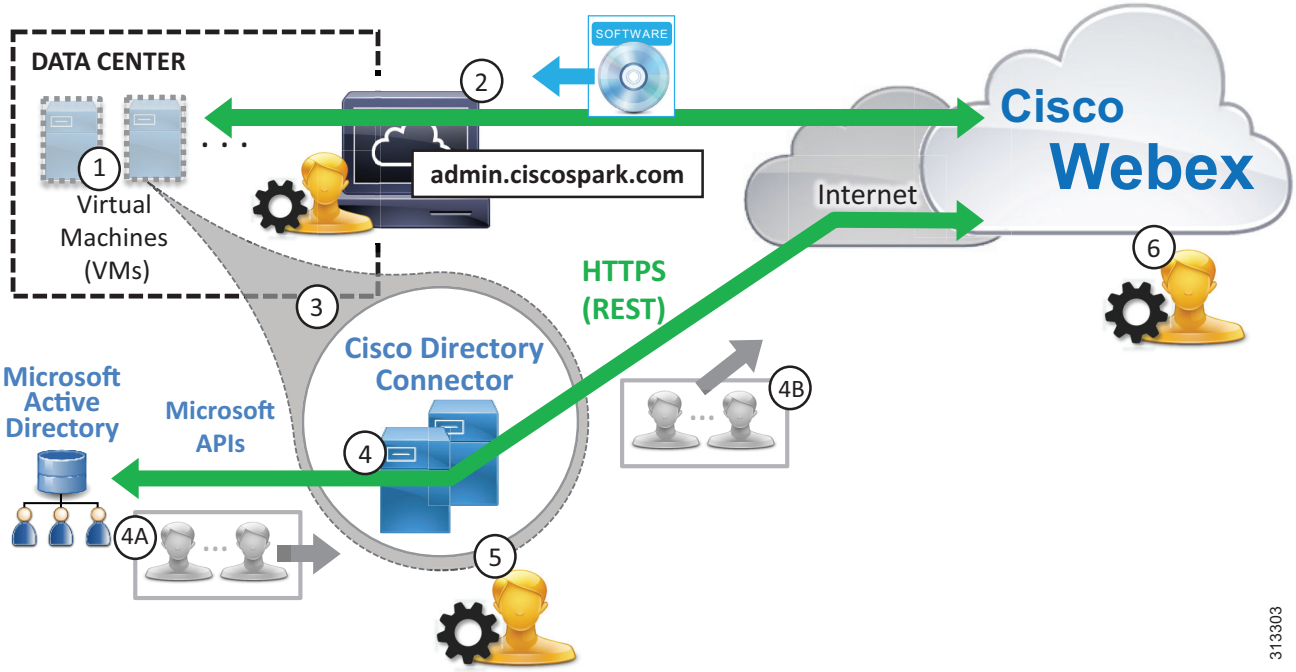
Role of Microsoft Active Directory

Microsoft Active Directory is the enterprise resource and user repository and the single source of validation for that information. The directory administrator maintains the enterprise resource and user information contained within the directory with moves, adds, changes, and deletions. Any updates to this information in Active Directory are propagated to the Cisco Directory Connector (and in turn to Webex) during synchronization.

Deployment Overview

Figure 2-3 shows the high-level steps required to deploy Webex Hybrid Directory Service. Virtual Microsoft Windows Servers are created and deployed in the enterprise data center (step 1). After the Windows servers are deployed, the administrator logs into the Webex Control Hub at https://admin.webex.com to enable directory synchronization and download the Cisco Directory Connector software installation package (step 2). Next, Directory Connector is installed on the Windows servers (step 3). After Directory Connector is installed, the administrator configures the connector (step 4), and an initial synchronization occurs between Microsoft Active Directory and the Directory Connector (step 4A) and between the Directory Connector and Webex (step 4B).

Figure 2-3 Webex Hybrid Directory Service Deployment Overview

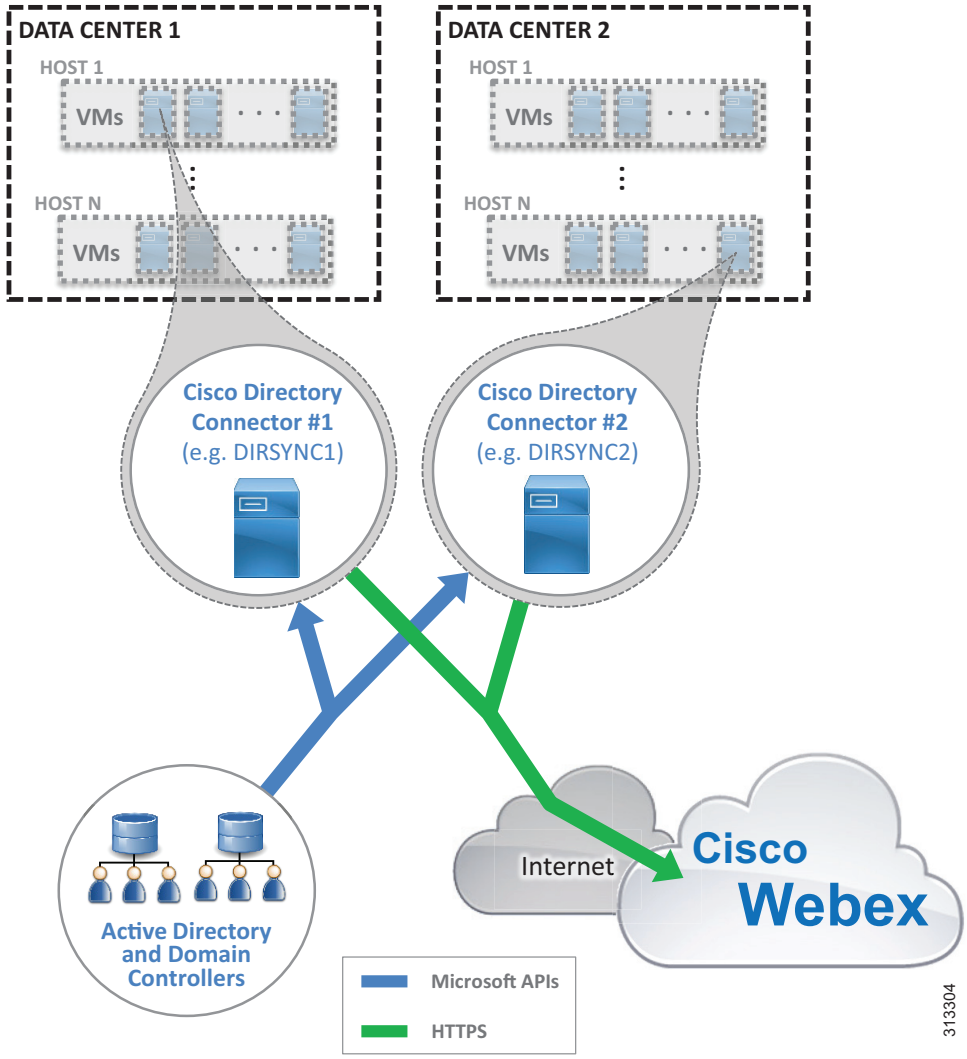


Once the initial synchronization completes, the administrator configures the schedule for periodic incremental and full synchronizations (step 5). After that, the administrator manages users and provisions them for cloud services as appropriate (step 6).

High Availability

As shown in Figure 2-4, two Cisco Directory Connectors are deployed. These Windows Servers virtual machines are deployed on separate hosts in separate buildings or data centers to provide high availability and redundancy. Directory Connectors are deployed as a pair, and both are capable of synchronizing directory information between the enterprise directory and the cloud. However, under normal operation, one Directory Connector (primary) handles directory synchronization while the other (backup) maintains connectivity to Webex but does not perform any synchronization. In the event that the primary Directory Connector fails, the backup Directory Connector will continue to handle synchronization operations based on the configured failover interval.

Figure 2-4 Webex Hybrid Directory Service High Availability



Note In cases where only a single Cisco Directory Connector is deployed (non-redundant deployments), if the Directory Connector fails, user information is no longer synchronized between Active Directory and the Webex identity store. The administrator is able to manage existing users and to provision them for services while the Directory Connector is down, but no users or resources can be added or removed from the Webex identity store until the Directory Connector is returned to service.

In addition to Cisco Directory Connector high availability considerations, also consider providing redundancy for other aspects of the integration such as the Active Directory services, connectivity to Webex (HTTPS), and availability of cloud services.

Microsoft components (Active Directory, Domain Controllers, and other Microsoft enterprise network services) should be deployed in a redundant fashion. Consult Microsoft product documentation for information on high availability.

Highly available network connectivity to the Internet is also required to ensure that Webex Teams and other Webex services are reachable from the enterprise. Redundant physical Internet connections, preferably from different providers, are recommended.

Webex services are highly available because those services and components are deployed across multiple physical data centers on elastic compute platforms.

Scalability

The primary sizing and scalability considerations for Webex Hybrid Directory Service is the size of the synchronization. The larger the enterprise directory and the search base in terms of number of resources and users, the longer a synchronization will take to complete. For this reason it is important to monitor synchronization operations initially to ensure that both incremental and full synchronizations are completing prior to the beginning of the next synchronization period. We recommend running the Directory Connector on a dedicated Windows server host. Additional load on the Windows server can reduce performance and increase overall system response and synchronization times.

For more information on Webex Hybrid Directory Service scaling, see the chapter on Sizing Cisco Webex Hybrid Services.

Webex Hybrid Directory Service Deployment Process

Webex Hybrid Directory Service requires the deployment of the Cisco Directory Connector and synchronization between the on-premises directory and the organizations Webex identity store.

Directory synchronization allows corporate users and resources to be imported into Webex. Directory synchronization is facilitated using the Webex Control Hub and Cisco Directory Connector. The Directory Connector allows for automatic synchronization of corporate directory information with Webex. Without Directory Connector, users and resources must be imported manually to Webex using a **.csv** file.

Note This section presents high-level guidance for deploying Webex Hybrid Directory Service. This guidance should be used in conjunction with the detailed instructions provided in the latest version of the *Deployment Guide for Cisco Directory Connector*, available at https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html.

The deployment of Webex Hybrid Directory Service starts with the Windows Server installation followed by the download, installation, and initial configuration of Cisco Directory Connector. To deploy Webex Hybrid Directory Service, perform the following tasks in the order listed here:

1. Deploy Microsoft Windows Server hosts for Cisco Directory Connector.
2. Enable directory synchronization and download Cisco Directory Connector software from the Webex Control Hub.
3. Install Cisco Directory Connector on the Windows Server host.
4. Configure Directory Connector and complete the initial synchronization.
5. Schedule periodic incremental and full synchronizations.
6. Manage imported users and provision them for Webex services.

1. Deploy Microsoft Windows Server hosts for Cisco Directory Connector.

The Cisco Directory Connector runs on a trusted Microsoft Windows domain server deployed in the corporate network. The server joins the Active Directory domain and needs an administrator read-only account to authenticate the Cisco Directory Connector server to the on-premises domain.

Deploy a new Microsoft Windows Server and join the corporate Microsoft Active Directory domain. To ensure a highly available deployment of Webex Hybrid Directory Service, install a second domain Microsoft Windows Server on a separate host.

For information about the specific Microsoft Windows Server and Microsoft Active Directory versions supported for Webex Hybrid Directory Service, refer to the latest version of the *Deployment Guide for Cisco Directory Connector*, available at

https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

Note Microsoft Windows Servers should be deployed and configured according to corporate standards and policies and should adhere to any requirements around virus and malware protection, device management, and security.

2. Enable directory synchronization and download Cisco Directory Connector software from the Webex Control Hub.

Log into the Webex Control Hub at https://admin.webex.com from the web browser on the Windows Server host you deployed in Step 1. Use your Webex Teams organization administrator credentials.

On the Webex Control Hub, enable directory synchronization by navigating to **Users** and clicking **Manage Users**. Next, click **Enable Directory Synchronization** and choose **Next** to continue. Then click the **Download and Install** link to save the Cisco Directory Connector installation **.zip** file (for example, DirectoryConnector.zip) to the local server.

3. Install Cisco Directory Connector on the Windows Server host.

Locate the **.zip** file saved to the host server in Step 2. Unzip the file, navigate to the setup folder, and run the **.msi** file (for example, CiscoDirectoryConnector.msi) in the setup folder to launch the Cisco Directory Connector Setup wizard.

Select **I accept the terms in the License Agreement** and click **Next** to accept the license agreement. Click **Next** to accept the default installation location.

Select the **Domain Account** option for the service account and enter the username and password for the domain account. In the **Username** field include the Active Directory domain and username with the format <*domain*>\<*user_name*> (for example, ENT-PA\administrator). Click **Next** to save the domain account information.

Then click **Install** to start the installation of Cisco Directory Connector.

When the installation completes, repeat this step on the second Windows Server host to install a redundant Directory Connector.

4. Configure Directory Connector and complete the initial synchronization.

Launch Cisco Directory Connector and sign into the Webex Teams organization by entering the email address and password of the administrator account for the organization. Note that this is the same email address and password used to log into the Webex Control Hub management portal. Click to confirm the Webex Teams organization and domain.

Next, perform initial configuration of Directory Connector. From the Directory Connector dashboard click the **Configuration** tab.

Note If a configuration tab or field value is not mentioned here, then the default setting and value should be assumed.

Navigate the tabs on the Configuration screen and configure the settings as shown in Table 2-1.

Table 2-1 Cisco Directory Connector Configuration Settings

Configuration Tab	Setting	Description and Values
General	Connector Name	Enter a name for the Directory Connector (for example, DIRSYNC1). This is the name that will be displayed on the dashboard and on the Webex Control Hub web portal.
	Preferred Domain Controllers	Add one or more Domain Controllers by using the drop-down menu. Select a Domain Controller on the network and click the **Add** button. Add at least two Domain Controllers to ensure directory services are highly available on the network.
Object Selection During synchronization, user information (based on the selected containers and configured LDAP filters) is pushed from the Directory Connector to Webex through an HTTPS connection. Because this is an outbound connection from the enterprise's perspective, it does not require any inbound ports to be opened on the internal or external firewall.	Object Type	**Users** box is selected.
	LDAP Filters	Enter any required LDAP filters in standard LDAP format to limit the number of searchable containers. Directory Connector pulls user information from the corporate Microsoft Active Directory. User information can be pulled from the entire domain or from specific containers and organizational units. Create multiple LDAP filters if more granularity is needed.
	On Premises Base DNs to Synchronize	Select one or more DNs from the window (for example, CN=Users,DC=ent-pa,DC=com) and click **Select** to choose appropriate synchronization containers and objects (for example, Users) to include in the directory synchronization agreement. The Webex Hybrid Directory Service integration with Microsoft Active Directory supports deployments with both single and multiple forests and either single or multiple domains.
User Attribute Mapping Cisco Directory Connector synchronizes a number of Microsoft Active Directory attributes to Webex (identity store of the customer organization).	Active Directory Attribute Name	Configure any required Active Directory to Webex attribute name mappings by selecting options from the Active Directory attribute drop-down lists. At a minimum, ensure that the Active Directory attribute name **mail** is mapped to the required Webex attribute name **uid**. The **mail** attribute plays a key role in Webex because it uniquely identifies the user. Other commonly synchronized Microsoft Active Directory attribute names include displayName, givenName, and telephoneNumber.

Click **Apply** to save and apply the configuration settings.

Once Directory Connector is installed and configured as above, perform an initial full synchronization to pull directory information from the corporate Microsoft Active Directory and push it to the organization's Webex identity store.

On the redundant Cisco Directory Connector, configure the same settings shown in Table 2-1, but use a unique name for the Connector Name setting (for example, DIRSYNC2).

5. Schedule periodic incremental and full synchronizations.

After the initial synchronization, it is important to keep the organization's Webex identity store updated with moves, adds, and changes that occur in the corporate Active Directory.

To keep Webex up to date with corporate directory changes, configure periodic incremental and full synchronizations on one of the Directory Connectors. Return to the Directory Connector Configuration tab and select **Schedule**. Then configure synchronization settings as shown in Table 2-2.

Table 2-2 Cisco Directory Connector Schedule Configuration Settings

Configuration Tab	Setting	Description and Values
Schedule	Incremental Sync Interval	Set the interval in minutes between incremental synchronizations (for example, 10 minutes is the default).
	Enable Full Sync Schedule	Select this option.
	Schedule	Select the time and day(s) of week to perform a periodic full synchronization (for example, 7:30 AM on S(unday)).
	Failover Interval	Set the amount of time in minutes before the secondary Directory Connector becomes primary and takes over incremental and full synchronization (for example, 60 minutes is the default). This setting applies for high availability deployments with more than one Directory Connector.

The settings in Table 2-2 are shared and apply to both Directory Connectors in the deployment.

6. Manage imported users and provision them for Webex services.

After the enterprise directory user information has been propagated to Webex, the administrator is able to provision users for cloud services and manage those service features and settings by using the Webex Control Hub.

Use your Webex organization administrator credentials to log into the Webex Control Hub at https://admin.webex.com from a web browser.

On the Webex Control Hub, begin managing and provisioning user services by navigating to **Users** and then clicking **Manage Users**. Once directory synchronization is enabled, there are multiple ways to modify users and the services they use. Users can be modified individually or in bulk.

To modify large numbers of users in bulk, choose either **Export and modify users with a CSV file** or **Modify all synchronized users**. The CSV file method is good for modifying groups of users in bulk (up to 1,100 users at a time); however, preparing the CSV file for bulk modification is a manual process.

To enable a feature or service for all users, click **Modify all synchronized users** and click **Next**. If prompted, acknowledge that users will automatically be sent an email by clicking **Next**. On the next screen, wait for the system to synchronize the list of users from the latest synchronization agreement, and then click **Next**.

On the subsequent screen, provision users for Message, Meeting, and other services including Hybrid Services. Once you have selected the services, click **Next** to start the update of user accounts. When the update is complete, users can begin to use the added services and features.

Note Valid licenses are required to add and enable licensed services and features.

Cisco Webex Hybrid Calendar Service

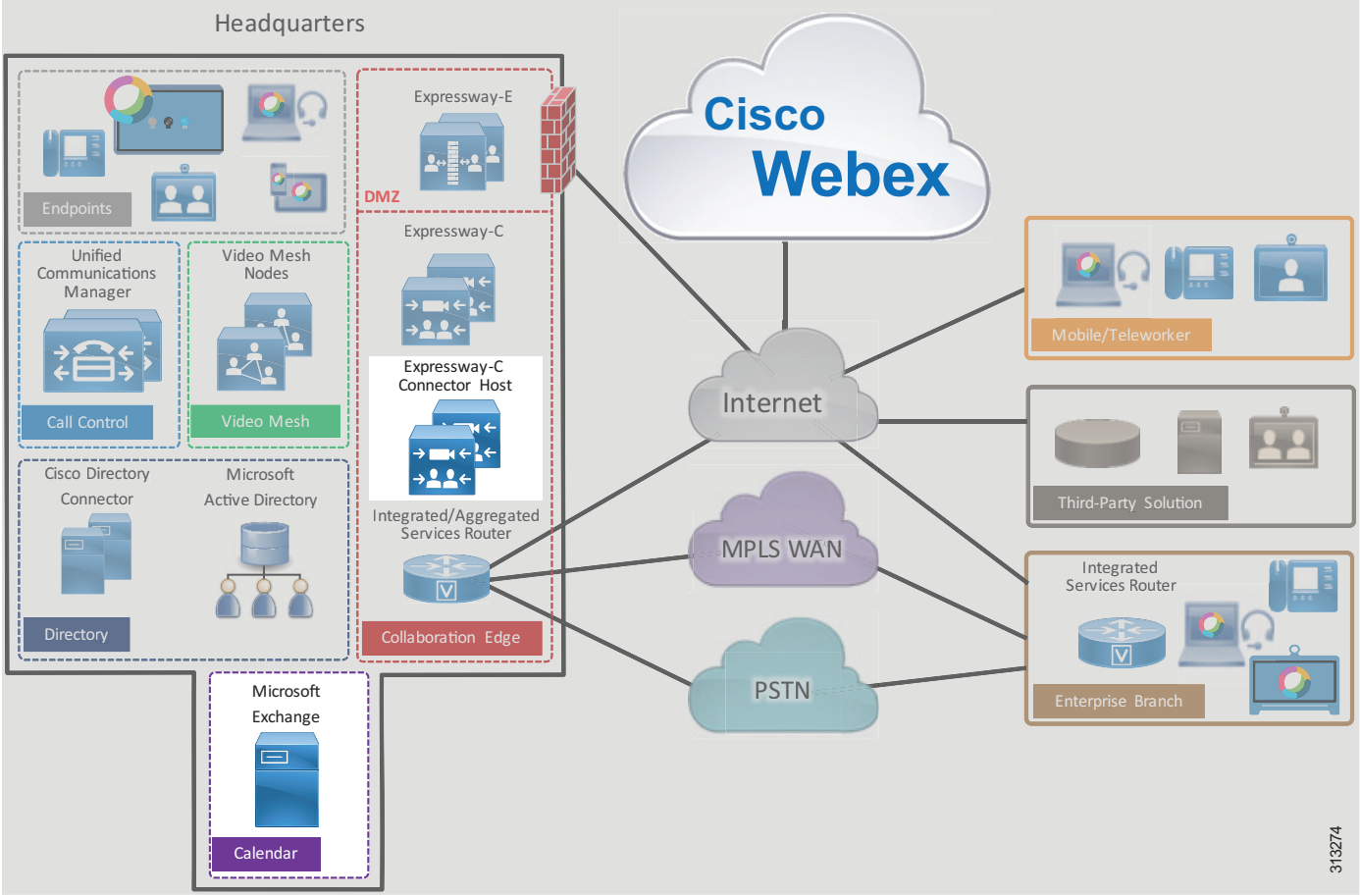
Revised: May 31, 2019

Cisco Webex Hybrid Services enable Webex Teams customers to connect on-premises collaboration services to Webex. Synchronizing enterprise calendar services with the Webex Hybrid Calendar Service for the customer's organization provides a seamless integration with improved end-user experience for managing meeting invitations, content, and communications with participants.

Overview

The Cisco Webex Hybrid Calendar Service high-level architecture, depicted in Figure 3-1, enables an organization to integrate their corporate Microsoft Exchange calendar services with Webex through the Expressway-C Connector Host. This integration enables pre-meeting and post-meeting communications and file sharing while providing an enhanced user experience with simplified scheduling and joining for meetings.

Figure 3-1 Cisco Webex Hybrid Calendar Service High-Level Architecture



Prerequisites

Prior to implementing and deploying Webex Hybrid Calendar Service, perform the following requirements:

- Deploy Microsoft Exchange within the organization with full email and calendaring functionality.
- Deploy Webex Hybrid Directory Service with corporate directory user information synchronized to Webex.
- If the on-premises network is behind a firewall, ensure that outbound HTTPS (port 443) access to the Internet is available.

Core Components

The core components for Webex Hybrid Calendar Service include:

- Cisco Calendar Connector
- Microsoft Exchange

Note Although Webex Hybrid Calendar Service also supports integration to Microsoft Office 365 or G Suite by Google Cloud, these integrations are not discussed or covered in this PA for Webex Hybrid Services. For information about these integrations, refer to the latest version of the *Deployment Guide for Cisco Webex Hybrid Calendar Service*, available at https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html.

Key Benefits

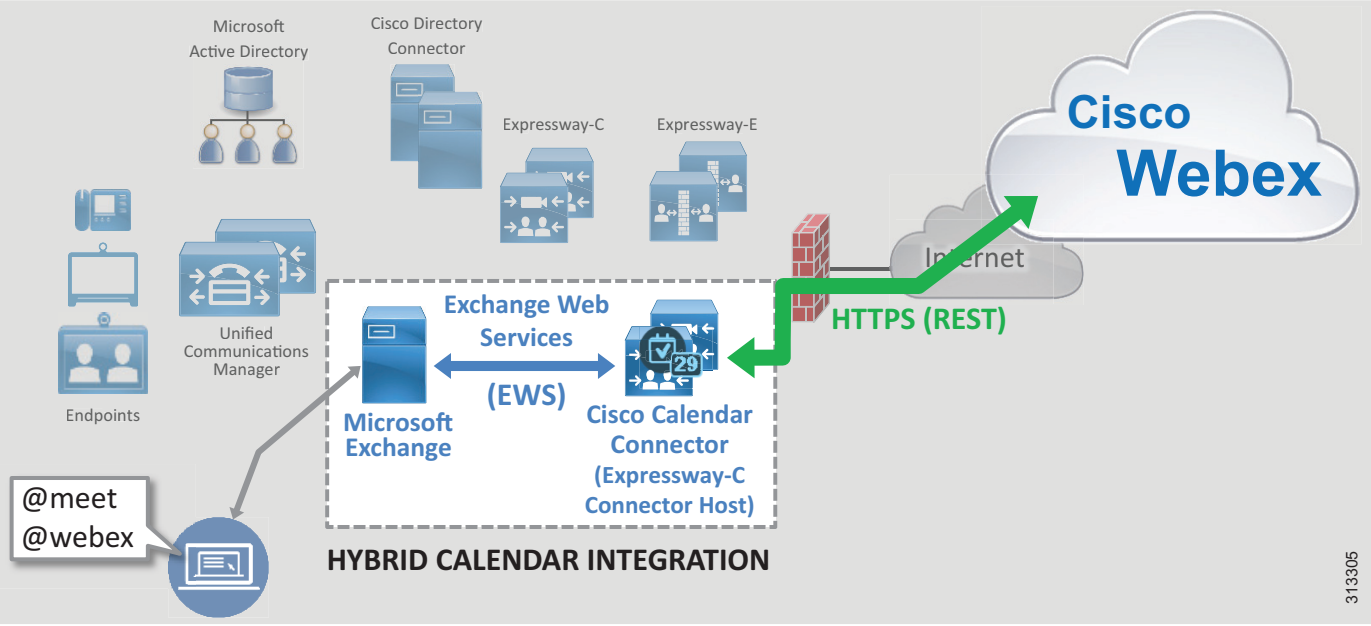
Webex Hybrid Calendar Service provides the following benefits:

- Automatic synchronization of users' Microsoft Exchange calendars, including meeting information, to Webex.
- Capability for users to automatically add, schedule, and invite others to Webex Teams meetings.
- Ability to run Cisco Calendar Connector co-resident with other connectors (Management and Call) on the Cisco Expressway-C Connector Host for maximum deployment flexibility.
- HTTPS outbound connection from the enterprise to Webex on standard port 443, which is typically allowed by organizations and thus should not require configuration to open ports on the firewall. The organization’s existing HTTP proxy may also be leveraged as required.

Architecture

Figure 3-2 shows the Webex Hybrid Calendar Service integration to the enterprise calendar. This integration relies on the Cisco Calendar Connectors (residing on the Expressway-C Connector Hosts), which are co-located in the central site with the Microsoft Exchange environment. Cisco Calendar Connector is deployed on two Expressway-C Connector Hosts for redundancy and high availability.

Figure 3-2 Architecture for the Integration of Webex Hybrid Calendar Service with the Enterprise Calendar



Cisco Calendar Connector relies on Microsoft Exchange Web Services (EWS) to pull calendar information from Microsoft Exchange based on the **@webex** and **@meet** notations in the calendar invitations. Calendar Connector uses HTTPS to push user information to the organization's calendar service in Webex.

The Calendar Connector service provides the following capabilities for creating calendar meeting invitations:

- **Webex Teams meeting and automatic space creation with @meet**

  With this capability a Webex Teams meeting is scheduled and a Webex Teams space is created when the user generates a meeting invitation from their Microsoft Outlook calendar with the @meet notation.

  When the @meet keyword is specified in the location field of the meeting invitation, Calendar Connector and the cloud calendar service create a Webex Teams meeting and a Webex Teams space with a name that matches the invitation subject. All users in the calendar invitation are not only invited to the meeting but they are also added to the Webex Teams space. The meeting information is also contained inside the Webex Teams space.

  This facilitates collaboration and allows the meeting organizer and attendees to communicate and share material prior to, during, and even after the meeting. If a calendar invitation includes a distribution list, users on the distribution list will not be added to the Webex Teams space automatically; however, they will receive the meeting invitation.

Note While the previous @spark keyword notation still works today, it will eventually be removed. Therefore, we recommend that organizations begin using the @meet keyword instead.

- **Webex Personal Room meeting scheduling with @webex**

  With this capability a Webex Personal Room meeting is added when the user generates a meeting invitation from their Microsoft Outlook calendar with the @webex notation.

  When the @webex keyword is specified in the location field of a Microsoft Outlook calendar invitation, Calendar Connector automatically populates the invitation with the user's Webex Personal Room meeting information.

For more information regarding the Calendar Connector @*keyword*, refer to the *Calendar Connector Release Notes*, available at https://collaborationhelp.cisco.com/.

Hybrid Calendar Service integration also enables synchronization of users' Microsoft Exchange enterprise calendar with their Webex Teams application calendar and meeting list and sharing of users' out-of-office status from Microsoft Outlook with Cisco Webex.

Role of Cisco Expressway-C Connector Host

The Cisco Expressway-C Connector Host registers to Webex and hosts various cloud connector micro-services, including the Cisco Calendar Connector. Expressway-C Connector Hosts are deployed within the enterprise boundary and communicate with Webex using HTTPS. Multiple cloud connectors may reside on the same Expressway-C Connector Host.

Role of Cisco Calendar Connector

Cloud connectors are small pieces of software that enable cloud service integrations. These connectors reside on the Expressway-C Connector Host and are downloaded, installed, and updated from Webex. Administrators manage cloud connectors from the Webex Control Hub web-portal.

The Cisco Calendar Connector serves as the intermediary between the enterprise Microsoft Exchange server or environment and Webex. The Calendar Connector communicates with the Exchange server using Exchange Web Services (EWS) and with Webex using HTTPS. Calendar Connector enables users to add meeting invitations to their Webex Teams application calendar and dynamically create Webex Teams spaces when scheduling meetings using Microsoft Outlook (application or web-based).

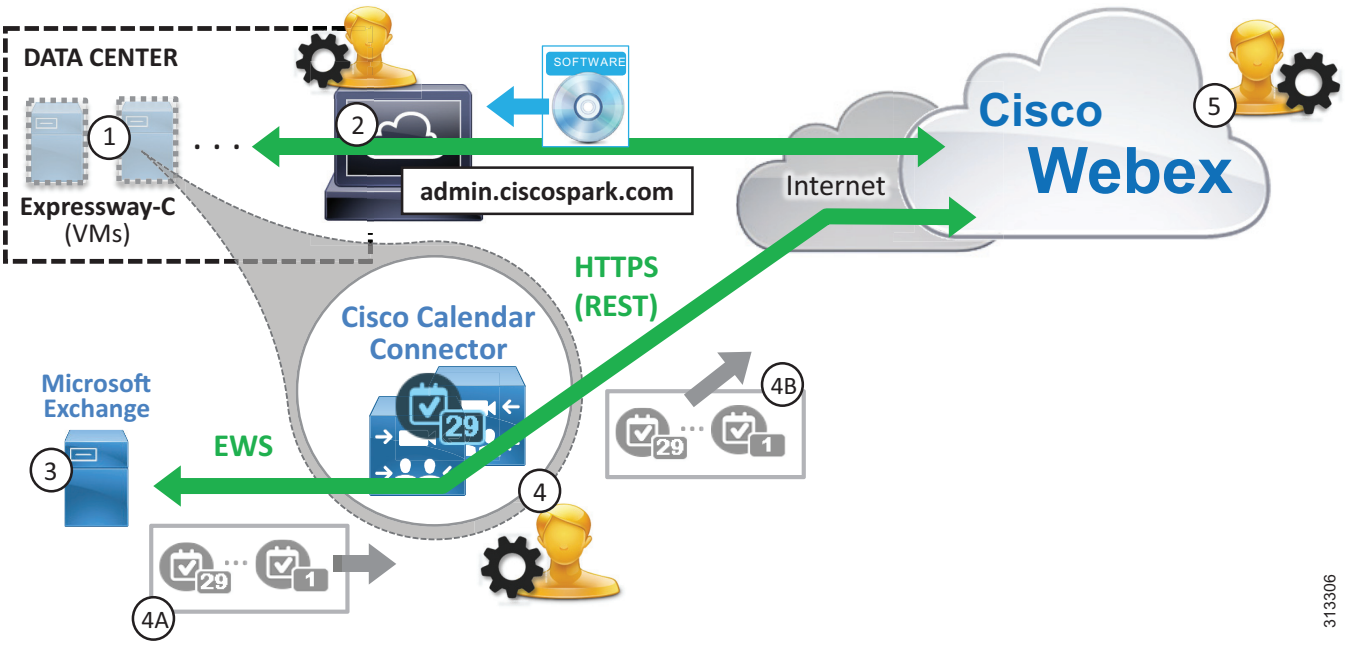
Role of Microsoft Exchange

Microsoft Exchange is the enterprise email and calendaring application. Users maintain and update their calendars as appropriate. Any updates to user calendars are propagated to the Cisco Calendar Connector using EWS and leveraging an impersonation service account to access and pull users' calendar information.

Deployment Overview

Figure 3-3 shows the high-level steps required for deploying Webex Hybrid Calendar Service. Virtual machines based on the Cisco Expressway-C open virtual appliance (OVA) template are created and deployed in the enterprise data center (step 1). (Alternatively, you can deploy a hardware appliance.) After deploy the virtual machines, from the Webex Control Hub (https://admin.webex.com) register the Expressway-C Connector Host to Webex to automatically download cloud connector software (step 2). Next, set up impersonation for the Calendar Connector service user account and a throttling policy on Microsoft Exchange (step 3). On the Expressway-C Connector Host configure the connection to Microsoft Exchange and the Webex integration details, and enable the Calendar Connector service on Expressway-C (step 4). Calendar invitations including the @meet or @webex notation are pushed from Microsoft Exchange using Exchange Web Services (step 4A) and in turn propagated by HTTPS to Webex Hybrid Calendar Service (step 4B). Then provision enterprise users for Webex Hybrid Calendar Service using the Webex Control Hub (step 5).

Figure 3-3 Webex Hybrid Calendar Service Deployment Overview

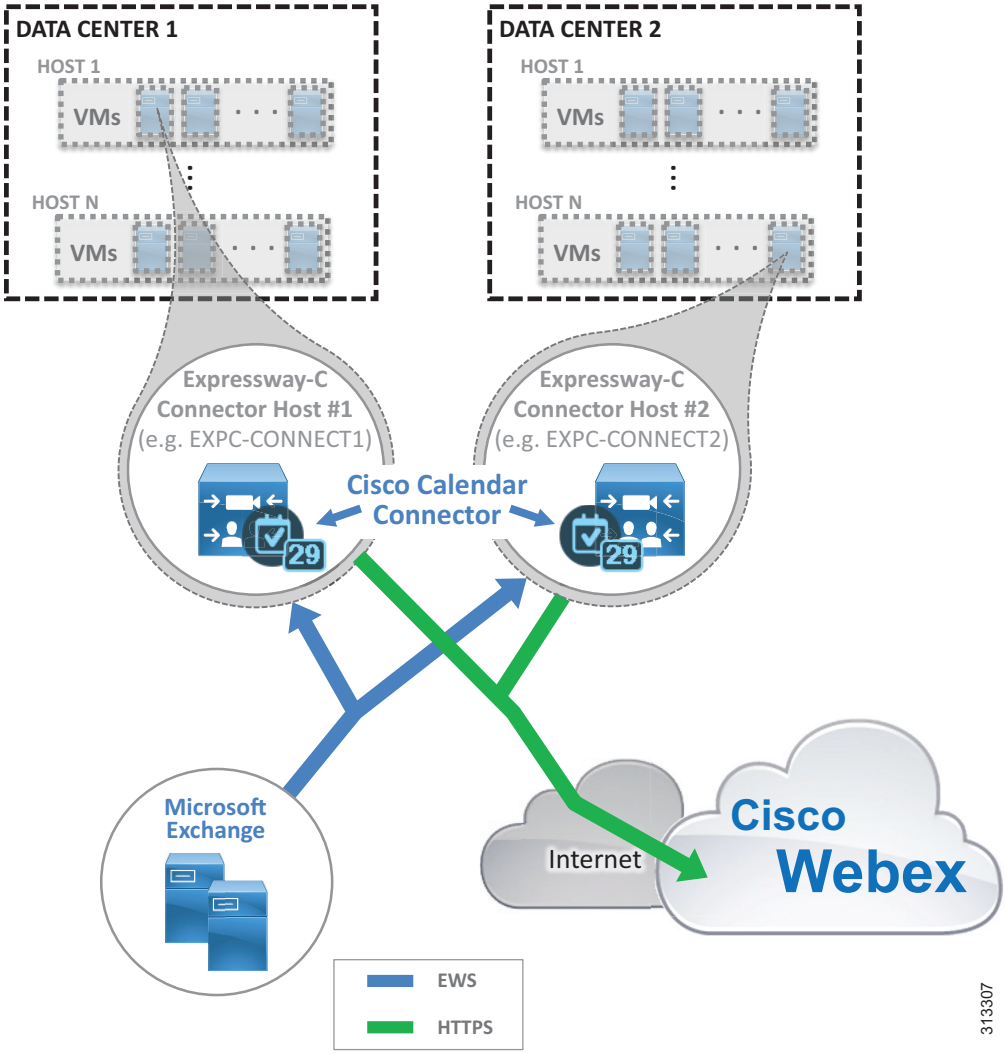


High Availability

As shown in Figure 3-4, two Cisco Expressway-C Connector Hosts are deployed. These connector hosts are Cisco Expressway-C virtual machines (VMs) and are deployed on separate hosts in separate buildings or data centers to provide high availability and redundancy.

Expressway-C Connector Hosts are clustered in an active/active pair, and each host runs the Calendar Connector micro-service. These Calendar Connectors are capable of synchronizing calendar meeting invitations and updates between the user's enterprise calendar and Webex.

Figure 3-4 Webex Hybrid Calendar Service High Availability



In addition to Cisco Calendar Connector and Expressway-C Connector Host high availability considerations, also consider providing redundancy for other aspects of the integration such as the Microsoft Exchange services (EWS), connectivity to Webex (HTTPS), and availability of cloud services.

Microsoft Exchange should be deployed in a redundant fashion and should leverage network load balancing as required. Consult Microsoft product documentation for information on Microsoft Exchange high availability.

Highly available network connectivity to the Internet is also required to ensure that Webex services are reachable from the enterprise. We recommend redundant physical Internet connections, preferably from different providers.

Webex services are highly available because those services and components are deployed across multiple physical data centers on elastic compute platforms.

Scalability

The primary sizing and scalability considerations for Webex Hybrid Calendar Service are the capacity of the Expressway-C Connector Host and of Microsoft Exchange.

User capacity of the Calendar Connector on the Expressway-C Connector Host depends on the following factors:

- Expressway-C Connector Host size — Small, medium, or large OVA or the Cisco Expressway CE appliance (for example, CE1200).
- Calendar Connector deployment type — Standalone on the connector host or co-resident with other connectors
- Non- connector operations and functions (for example, hybrid calling media and signaling firewall traversal or business-to-business calling) — Co-resident with the Calendar Connector or handled by other Expressway nodes

From the perspective of Microsoft Exchange, the Calendar Connector increases the CPU usage and load on the Exchange servers. The impact on the Exchange environment depends on:

- The size and type of Exchange deployment
- The expected number of @webex and @meet meetings per user per hour
- The number of configured Exchange users
- The size of each user's calendar

Knowing and understanding these aspects for your deployment is important for sizing Webex Hybrid Calendar Service appropriately.

For more information on Webex Hybrid Calendar Service scaling, see the chapter on Sizing Cisco Webex Hybrid Services.

Webex Hybrid Calendar Service Deployment Process

Webex Hybrid Calendar Service requires the deployment of the Cisco Expressway-C Connector Host, installation of the Calendar Connector, and configuration of Microsoft Exchange and the Cisco Expressway-C Connector Host for calendar integration between the on-premises enterprise calendar service and the organization's Webex calendar service.

Note This section presents high-level guidance for deploying Webex Hybrid Calendar Service. This guidance should be used in conjunction with the detailed instructions provided in the latest version of the *Deployment Guide for Cisco Webex Hybrid Calendar Service*, available at https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html.

The deployment of Webex Hybrid Calendar Service starts with installation of the Cisco Expressway-C Connector Host followed by deployment and initial configuration of Cisco Calendar Connector and the calendar integration. To deploy Webex Hybrid Calendar Service, perform the following tasks in the order listed here:

- 1. Download and deploy the Cisco Expressway-C Connector Host OVA template.
- 2. Register the Expressway-C Connector Hosts to Webex using the Webex Control Hub.
- 3. Prepare Microsoft Exchange for Webex Hybrid Calendar Service integration.
- 4. Configure the Expressway-C Connector Hosts for Webex Hybrid Calendar Service integration.
- 5. Provision enterprise users for Webex Hybrid Calendar Service by using the Webex Control Hub.

1. Download and deploy the Cisco Expressway-C Connector Host OVA template.

The Cisco Calendar Connectors run on Cisco Expressway-C Connector Hosts. The Cisco Expressway-C Connector Host is simply a regular Expressway-C server enabled for hybrid services. Download the Cisco Expressway OVA template from https://www.cisco.com/, then deploy the OVA template on two separate VMware hosts. Alternatively, use two Cisco Expressway hardware appliances (for example, the Cisco Expressway CE1200 appliance).

When deploying the OVA template, select the appropriate Expressway deployment configuration size (for example, Medium) based on the size of your deployment. For more information about Expressway-C Connector Host sizing, refer to the Scalability information earlier in this chapter and the chapter on Sizing Cisco Webex Hybrid Services.

Note The large deployment OVA configuration is not supported on Cisco Business Edition 7000.

For information about the specific Cisco Expressway-C and Microsoft Exchange versions supported for Webex Hybrid Calendar Service, refer to the latest version of the *Deployment Guide for Cisco Webex Hybrid Calendar Service*, available at

https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

Once the virtual machines (VMs) or appliances have been deployed, power on and complete the initial installation wizard to set system account passwords (for example, administrator password), network information (for example, IP address, default gateway, and so forth), and basic services (for example, SSH and web) at each server console.

Next, navigate to the web interface of each Expressway-C server (for example, *https://us-expc-connector1/* and *https://us-expc-connector2*), login, and on the subsequent Service Setup Wizard page ensure the series is set to **Expressway** and the type is set to **Expressway-C**. Click the box beside **Cisco Webex Hybrid Services** to enable hybrid services and service connectors, and click **Continue** to save the service selection and bring up the system Overview page.

Next, create an Expressway cluster of the Expressway-C Connector Hosts. Select one of the Expressway-C servers as the master Expressway-C Connector Host cluster node. Navigate to **System** > **Clustering** to assign the Expressway-C Connector Host cluster fully qualified domain name (FQDN) (for example, us-expc-connector1.ent-pa.com), and specify the IP address of this host as the peer 1 or cluster master peer address. This FQDN is used to register the master peer to Webex, and additional cluster peers automatically register once the master registers.

To add the second Expressway -C Connector Host to the cluster, configure the second host's IP address as the peer 2 address on the **System > Clustering** page of the primary Expressway-C Connector Host. Then replicate the same **System > Clustering** page configuration on the second Expressway-C Connector Host.

The Expressway-C Connector Hosts do not require release or feature keys to use Webex Hybrid Services. If you see an alarm regarding a system release key, you can safely acknowledge to remove it from the web interface.

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

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

2. Register the Expressway-C Connector Hosts to Webex using the Webex Control Hub.

To register the Expressway-C Connector Hosts to Webex and begin to use hybrid connectors, log into the Webex Control Hub at https://admin.webex.com using your Webex organization's administrator credentials. Then perform the configuration tasks and settings shown in Table 3-1.

Table 3-1 Cisco Expressway-C Connector Host Cloud Registration

Expressway-C Connector Host Cloud Registration Tasks and Descriptions	Navigation	Configuration Settings and Steps
Create Expressway Resource Groups. Expressway-C Connector Hosts may be assigned to resource groups in Webex to simplify management of multiple Expressway-C Connector hosts and/or clusters, particularly in global and multi-regional deployments.	Navigate to **Services > On-Premises Resources** (under the Hybrid Services area) and select **All Resources**. Click the settings gear icon next to Expressway and select **Create new resource group**. (Refer to the *Configuration Settings and Steps* column for the configuration value.) Click **Done** to save.	Enter the name of the resource group: **US Hybrid Services**
Add the Expressway-C Connector Host master peer as an Expressway resource. The Expressway-C Connector Host primary server must be defined in Webex in order to register and access connector software and services.	Navigate to **Services > On-Premises Resources** (under the Hybrid Services area) and select **All Resources**. Click **Add Resource**. On the following screens, make selections as shown in the *Configuration Settings and Steps* column, and click **Next** to save and move to the next screen.	1. Click **Expressway** to add a resource for Hybrid Calendar and/or Call service. 2. Click **Hybrid Calendar Service**.[1] 3. Enter the FQDN of the master Expressway-C Connector Host cluster node: **us-expc-connector1.ent-pa.com** 4. Enter the display name for this Expressway-C Connector Host cluster: **us-expc-connectors** 5. Click **Yes, assign now**, and select: **US Hybrid Services**

Table 3-1 Cisco Expressway-C Connector Host Cloud Registration (continued)

Expressway-C Connector Host Cloud Registration Tasks and Descriptions	Navigation	Configuration Settings and Steps
Register the Expressway-C Connector Host to Webex. The final step of adding the Expressway-C Connector Host resource is to complete the cloud registration.	On the final screen of the add resource wizard, click **Go to Expressway** to launch the web interface of the Expressway-C Connector Host cluster master peer (for example, https://us-expc-connector1.ent-pa.com/). (Refer to the *Configuration Settings and Steps* column for the configuration values.)	1. Login with Expressway administrator credentials. 2. Click **I want Cisco to manage the Expressway CA certificates required for this trust** in order to automatically add the Webex CA certificates to the Expressway-C trust list. 3. Click **Register** to initiate cloud registration. 4. On redirect to the Webex Control Hub, click **Allow** to complete the registration.

1. If you plan to deploy Webex Hybrid Call Service, then you may also click **Hybrid Call Service** to use this connector host resource for Webex Hybrid Call Service as well.

Once registration of the Expressway-C Connector Host to Webex completes, the Management Connector software offers to automatically upgrade itself if required, and then it begins downloading and installing the Calendar Connector software from the cloud onto the Expressway-C Connector Host.

You do not need to register the second Expressway-C Connector Host to Webex; it will automatically register when the master peer registers, and it will automatically upgrade and/or install the same connectors.

3. Prepare Microsoft Exchange for Webex Hybrid Calendar Service integration.

After the Expressway-C Connector Host nodes are registered to Webex, the next step is to prepare Microsoft Exchange for the Webex Hybrid Calendar Service integration. Perform the following tasks on Microsoft Exchange in order to set up Webex Hybrid Calendar Service integration:

Add the impersonation role to the service account for the Calendar Connector Service.

Calendar Connector integrates with Microsoft Exchange through an impersonation account. The application impersonation management role in Microsoft Exchange enables applications to impersonate users in an organization in order to perform tasks on behalf of the user. The application impersonation role is configured in Microsoft Exchange.

Navigate to the Microsoft Exchange server and enter the following command in the Exchange Management Shell:

```
new-ManagementRoleAssignment -Name:<RoleName>
-Role:ApplicationImpersonation -User '<UserName>'
```

Where <*RoleName*> is the name of the new role (for example, CalendarConnector) and <*UserName*> is the name of the service account the impersonation role is being assigned to in the format *domain\name* (for example, ENT-PA\CalendarConnectorAcct).

Note The impersonation account does not require administrator permissions, but it must have a mailbox.

Configure a throttling policy and apply it to the impersonation account.

As with any service or application entity that accesses Microsoft Exchange, it is a good idea to configure a throttling policy to ensure that Microsoft Exchange is able to handle the added load of the service account and can continue to operate and respond as normal.

Return to the Exchange Management Shell and enter the following command:

```
New-ThrottlingPolicy -Name "<ThrottlePolicy>" -EWSMaxConcurrency unlimited
-EWSMaxBurst unlimited -EWSRechargeRate unlimited -EWSCutOffBalance unlimited
-EWSMaxSubscriptions 5000
```

Where <*ThrottlePolicy*> is the name of the new role (for example, CalendarConnectorPolicy).

Next assign the new throttling policy to the impersonation account with the following command:

```
Set-ThrottlingPolicyAssociation -Identity "<ImpersonationAcct>" -ThrottlingPolicy
"<ThrottlePolicy>"
```

Where <*ImpersonationAcct*> is the name of the service account (for example, CalendarConnectorAcct), and <*ThrottlePolicy* > is the name of the throttle policy (for example, CalendarConnectorPolicy) created in the previous step.

4. Configure the Expressway-C Connector Hosts for Webex Hybrid Calendar Service integration.

With the Expressway-C Connector Hosts registered to Webex and with the Microsoft Exchange environment prepared, the next step is to complete the Webex Hybrid Calendar Service integration configuration.

Return to the Expressway-C Connector Host master peer web interface (for example, https://us-expc-connector1/) and log in with the administrator credentials. Then perform the configuration tasks and settings shown in Table 3-2.

Note In order to enable TLS verification for the link to Microsoft Exchange (TLS Verfiy Mode = **On**), the Expressway-C server host must be able to validate the certificate received from Microsoft Exchange. Prior to proceeding, ensure that the root certificate of the Certificate Authority (CA) that signed the Microsoft Exchange server certificate has been appended to the Expressway-C server trust list. Failure to import the CA root certificate will result in TLS verification failure and prevent connection between Expressway-C and the Microsoft Exchange server. The CA root certificate must be appended to the server trust list for each Expressway-C node in the cluster.

Table 3-2 Cisco Expressway-C Connector Host Configuration Tasks

Configuration Tasks	Settings	Example Values
Configure the Microsoft Exchange Connection. Create the connection between Expressway-C Connector Host and Microsoft Exchange. Navigate to **Applications > Hybrid Services > Calendar Service > Microsoft Exchange Configuration**. Click **New** to begin adding Microsoft Exchange configuration information. (Refer to the *Settings* and *Example Values* columns for configuration values.) Click **Add** to create the connection.	Service Account Credentials	**CalendarConnectorAcct@ent-pa.com** (Format: *username@domain*)
	Display Name	**us-exchange-1**
	Type	**Exchange On-Premises**
	Need Proxy for Configuration	**No** (Enter **Yes** if web proxy is required to reach Microsoft Exchange.)
	Enable this Exchange Server	**Yes**
	Authentication Type	**NTLM**
	TLS Verify Mode	**On**
	Autodiscovery	**Use Active Directory** Configure additional Active Directory information as required: • Active Directory Domain (for example, **ent-pa.com**) • Query Mode (for example, **ldaps**) • LDAP TLS Verify Mode (for example, **On**)
Configure Webex Site Settings. Add Webex information to facilitate use of Webex personal meeting rooms (PMRs) when using @webex in meeting invitations. Navigate to **Applications > Hybrid Services > Calendar Service > Cisco Webex Configuration**. Click **New** to begin adding Webex configuration information. (Refer to the *Settings* and *Example Values* columns for configuration values.) Click **Save** to complete the configuration.	WebEx Fully Qualified Site Name	**ent-pa.webex.com**
	WebEx account credentials	*<account username@domain / password>*
	Default Site	**Yes**

After completing the configuration tasks in Table 3-2, start the Calendar Connector service to complete the Calendar Connector integration. Navigate to **Applications > Hybrid Services > Connector Management** and select the Calendar Connector node. Select **Enable** from the drop-down list, and then click **Save** to save the configuration. Make sure the Calendar Connector comes up and begins to run (status says **Running**).

5. Provision enterprise users for Webex Hybrid Calendar Service by using the Webex Control Hub.

After you have enabled and configured Webex Hybrid Calendar Service, you can provision users for the Webex Hybrid Calendar Service. From a web browser, use your Webex organization's administrator credentials to log into the Webex Control Hub at https://admin.webex.com.

Provision users individually or in bulk for Webex Hybrid Calendar Service by navigating to **Users** and selecting individual users or by clicking **Manage Users** to provision groups of users.

To enable large numbers of users in bulk for Webex Hybrid Calendar Service, choose either **Export and modify users with a CSV file** or **Modify all synchronized users**. To enable Webex Hybrid Calendar Service for all users, select **Modify all synchronized users** and click **Next**. If prompted, acknowledge that users will automatically be sent an email by clicking **Next**. On the next screen, wait for the system to synchronize the list of users from the latest directory synchronization agreement, and then click **Next**.

On the subsequent screen, provision all users for Webex Hybrid Calendar Service by selecting **Calendar Service** and clicking **Next** to start the update of user accounts. Once the update is complete, users can begin to use Webex Hybrid Calendar Service.

Note Valid licenses are required to add and enable licensed services and features.

Cisco Webex Video Mesh

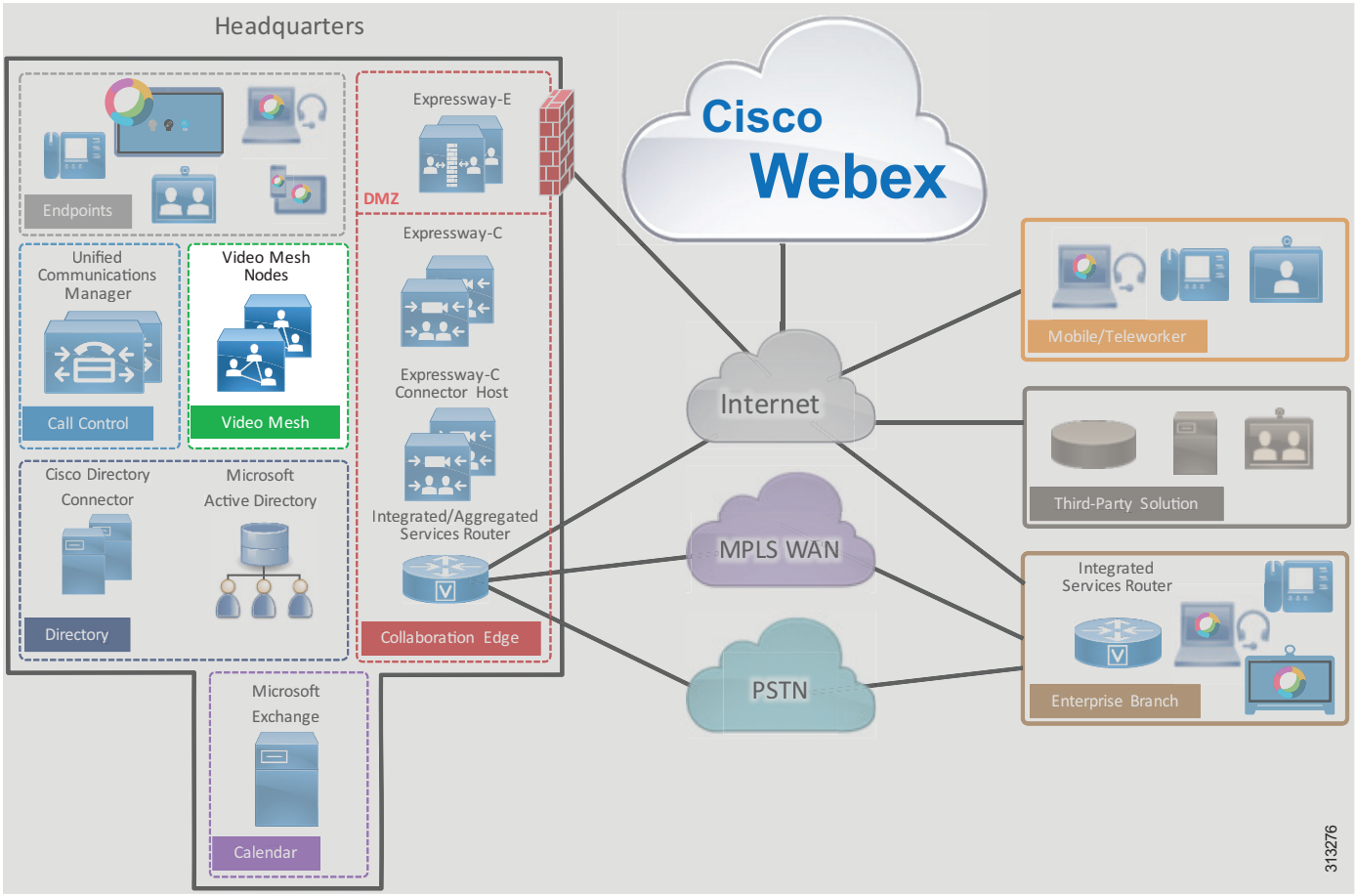
Revised: May 31, 2019

Cisco Webex Video Mesh is a component of Webex Hybrid Services that allows organizations to deploy an instance of Webex media processing on-premises. This means that Webex Teams devices and applications can terminate media on-premises instead of sending all media to the cloud. SIP endpoints registered to Cisco Unified Communications Manager (Unified CM) can also use Video Mesh services when dialing into Webex Meetings.

Overview

The central component of Cisco Webex Video Mesh is the Video Mesh Node, which can be deployed in clusters (see Figure 4-1). The Video Mesh Node is packaged as an OVA file and is installed on a Cisco Unified Computing System (UCS) or specification-based server in the organization's data center(s). The Video Mesh Node registers to Webex, and all management tasks are performed in the Webex Control Hub. Webex Teams devices and applications can send audio, video, and shared screen content to a Video Mesh Node. Cisco Webex Board traffic is sent to the Webex cloud media services. SIP endpoints registered to Cisco Unified CM can send audio, video, and shared screen content to a Video Mesh Node when joining Webex Meetings. Unified CM SIP endpoints include SIP desktop phones, SIP video endpoints, SIP room systems, and Cisco Jabber running in softphone mode.

Figure 4-1 Cisco Webex Video Mesh High-Level Architecture



Core Components

The core components for Webex Video Mesh include:

- Cisco Webex Video Mesh Node
- Cisco Webex Control Hub
- Cisco Webex

Key Benefits

The benefits of Webex Video Mesh include:

- Improved call quality as media stays local, which reduces latency and packet loss
- Reduced consumption of Internet bandwidth
- On-premises deployment simplicity via Webex

Hardware Requirements

Webex Video Mesh Node software can be downloaded from the Webex Control Hub (https://admin.webex.com). The software is packaged as an OVA file that can be installed on VMware ESXi 6 (or later) with VMware vSphere 6 (or later). Table 4-1 lists the supported hardware options.

Table 4-1 Hardware Requirements for Webex Video Mesh Nodes[1]

Platform	Specifications
Cisco Meeting Server 1000	72 vCPUs 60 GB main memory 250 GB local hard disk space
Specification-based configuration	46 vCPUs 60 GB main memory 250 GB local hard disk space 2.6 GHz Intel Xeon E5-2600v3 or later processor

1. For additional hardware requirements, refer to the *Cisco Webex Video Mesh Data Sheet*, available at https://www.cisco.com/c/en/us/solutions/collateral/unified-communications/spark-hybrid-services/datasheet-c78-738153.html.

Webex Video Mesh Ports and Protocols

The Webex Video Mesh Nodes must be accessible from the corporate network. The nodes also need access to Webex for some services such as signaling and media cascading. Table 4-2, Table 4-3, Table 4-4, and Table 4-5 list the ports that must be open for successful deployment of Webex Video Mesh.

Table 4-2 lists the ports required for management of the Video Mesh Nodes.

Table 4-2 Traffic Signatures for Management of Video Mesh Nodes

Source	Destination	Source Address	Source Port	Protocol	Destination Address	Destination Port
Administrator computer	Video Mesh Node	Management device IP address	ANY	TCP HTTPS	Video Mesh Node	443
Video Mesh Node	Webex cloud media services	Video Mesh Node IP address	ANY	TCP HTTPS	ANY	443
Video Mesh Node	Webex cloud media services	Video Mesh Node IP address	ANY	UDP NTP	ANY	123[1]
Video Mesh Node	Webex cloud media services	Video Mesh Node IP address	ANY	UDP DNS	ANY	53[1]

Table 4-2 Traffic Signatures for Management of Video Mesh Nodes (continued)

Source	Destination	Source Address	Source Port	Protocol	Destination Address	Destination Port
Video Mesh Node	Webex cloud media services	Video Mesh Node IP address	ANY	TCP HTTPS	*.docker.io *.wbx2.com *.webex.com	443
Video Mesh Node #1	Video Mesh Node #2	Video Mesh Node #1 IP address	ANY	TCP HTTPS	Video Mesh Node #2 address	5000 5001

1. UDP ports 53 and 123 are not required if you are using local DNS and NTP resources.

Table 4-3 details the port requirements for cascade signaling from the Video Mesh Nodes to the Webex cloud media services.

Table 4-3 Traffic Signatures for Cascade Signaling to the Webex Cloud Media Services

Source	Destination	Source Address	Source Port	Protocol	Destination Address	Destination Port
Video Mesh Node	Webex cloud media services	ANY	ANY	TCP	ANY	444

Table 4-4 details the port requirements for Webex Meetings media traffic.

Table 4-4 Traffic Signatures for Webex Real-Time Media (Egress Direction[1])

Source IP Address	Destination IP Address	Source UDP Ports	Destination UDP Ports	Protocol	Media Type[2]
Webex Teams application or endpoint	Webex cloud media services	52000 to 52099	5004	UDP TCP[3]	Audio
Webex Teams application or endpoint	Webex cloud media services	52100 to 52299	5004	UDP TCP[3]	Video
Webex Teams application or endpoint	Video Mesh Node	52000 to 52099	5004	UDP[3]	Audio
Webex Teams application or endpoint	Video Mesh Node	52100 to 52299	5004	UDP[3]	Video
Video Mesh Node	Webex cloud media services	52500 to 62999	5004	UDP/SRTP[4]	Audio
Video Mesh Node	Webex cloud media services	63000 to 65500	5004	UDP/SRTP[4]	Video
Video Mesh Node	Video Mesh Node	52500 to 62999	5004	UDP/SRTP[4]	Audio
Video Mesh Node	Video Mesh Node	63000 to 65500	5004	UDP/SRTP[4]	Video

1. Egress direction is from the endpoint to Webex.
2. As elsewhere in this document, Audio in this table refers to audio streams of voice-only calls, audio streams of video calls, and related RTCP packets; while Video refers to video streams (main video and presentations or content) and related RTCP packets.
3. UDP is preferred for media traffic. However, if the UDP connection fails, Webex Teams applications can fail-over to TCP for media traffic.
4. TCP can also be used for media cascades from Video Mesh Node to Video Mesh Node, and from Video Mesh Node to the Webex cloud media services. However, UDP is preferred, and TCP can affect media quality.

Table 4-5 lists the port range requirements to allow SIP endpoints to use Webex Video Mesh services.

Table 4-5 Port Range Requirements to Allow SIP Endpoints to Use Webex Video Mesh Services

Description	Source IP Address	Destination IP Address	Source Ports	Destination Ports	Protocol
Unified CM SIP signaling to Video Mesh cluster	Unified CM	Video Mesh Node	5060	5060	TCP
SIP endpoint signaling to Video Mesh cluster	SIP Endpoint	Video Mesh Node	5060 to 5062	5060 to 5062	TCP
SIP endpoint media to Video Mesh cluster	SIP Endpoint	Video Mesh Node	ANY	52500 to 62999 for audio 63000 to 65500 for video	UDP

For more information on the ports and protocols required for Webex, refer to the latest version of the following documents:

- *Cisco Webex Teams Firewall Traversal* whitepaper, available at

  https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/whitepapers/cisco-wbxt-firewall-traversal-whitepaper.pdf

- *Deployment Guide for Cisco Webex Video Mesh*, available at

  https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

Architecture

Before deploying Webex Video Mesh Nodes, consider the following factors:

- Number of Webex Teams endpoints per site
- Number of SIP endpoints registered to Cisco Unified CM per site
- Available Internet edge bandwidth per site
- Corporate network architecture
- Number of local participants (located on the corporate network) and number of remote participants (located on the Internet) in Webex Meetings
- Webex Video Mesh Node hardware requirements

After you have evaluated the above factors for your deployment, identify the locations for installing the Video Mesh clusters. The next step is deployment of the Video Mesh Nodes. The Video Mesh Node software can be downloaded from the Webex Control Hub. Once installed and powered on, the Video Mesh Nodes should be configured with relevant network details such as IP, DNS, and NTP addresses.

After installing the Video Mesh Nodes, the next step is to register them to Webex. Video Mesh Node registration is performed via the Webex Control Hub. Video Mesh Nodes must be assigned to a cluster. A cluster can represent a geographical region for Webex Teams endpoints to use for media termination. The IP address of the installed Video Mesh Node is entered into the Webex Control Hub, which registers the node to Webex. More nodes can be added to the cluster at any time.

Video Mesh Cluster Discovery for Webex Teams Endpoints

When a Webex Teams endpoint starts up, it registers to Webex. Webex then returns the addresses of cloud media services as well as Video Mesh Node clusters provisioned for that Webex Teams organization. Next the Webex Teams endpoint performs a number of tests to determine where it should send media when in a meeting.

The first test that the Webex Teams endpoint performs is a reachability test to see if it can connect to the cluster(s). If a Video Mesh Node is not reachable, the Webex Teams endpoint will not use it to terminate media when in a meeting. When Webex Teams endpoints are roaming outside of the corporate network, if they are not connected to a VPN, reachability tests to Video Mesh Nodes will fail unless the Video Mesh Nodes are exposed to the Internet (not recommended). In this situation, Webex Teams endpoints will send media to the Webex cloud media services when in a meeting.

The second test that the Webex Teams endpoint performs is a STUN test to determine the round-trip delay time (RTD) between the endpoint and the media node (cloud and hybrid). In most cases, for an on-premises Webex Teams endpoint, a Video Mesh cluster should have a shorter RTD than cloud media services. The Webex Teams endpoint reports the results of the STUN test to Webex. Webex then assigns the Webex Teams endpoint to send media to a node in the cluster with the lowest round-trip delay time.

Webex Teams endpoints perform these tests in the background when one of the following events occurs:

- Webex Teams endpoint startup
- A network change event
- Media service cache expiry

The cache expiry time for media node discovery is 2 hours. When new Video Mesh Nodes are added to a deployment, it may take Webex Teams endpoints up to 2 hours to recognize this event. Restarting a Webex Teams endpoint will force the endpoint to perform connectivity and STUN tests again and to recognize the new Video Mesh Node.

Deploying Video Mesh Nodes on the Corporate Network

The Video Mesh cluster can be deployed on the corporate network or in the demilitarized zone (DMZ). We recommend deploying the Video Mesh cluster in the corporate network to allow corporate network-based Webex Teams endpoints to discover the cluster and thus save bandwidth at the Internet edge. Roaming Webex Teams endpoints will not discover internally deployed Video Mesh Nodes and will connect to Webex for media services. Deploying Video Mesh Nodes on the corporate network also allows Unified CM to connect over SIP without having to open TCP port 5060 on the DMZ internal firewall.

Deploying the Video Mesh cluster in the DMZ allows roaming Webex Teams endpoints (Webex Teams endpoints that are not connected to the corporate network directly or via VPN) to discover and send media to the Video Mesh cluster instead of sending media directly to the Webex cloud media services. However, a DMZ-based deployment of the Video Mesh cluster is not recommended due to the following reasons:

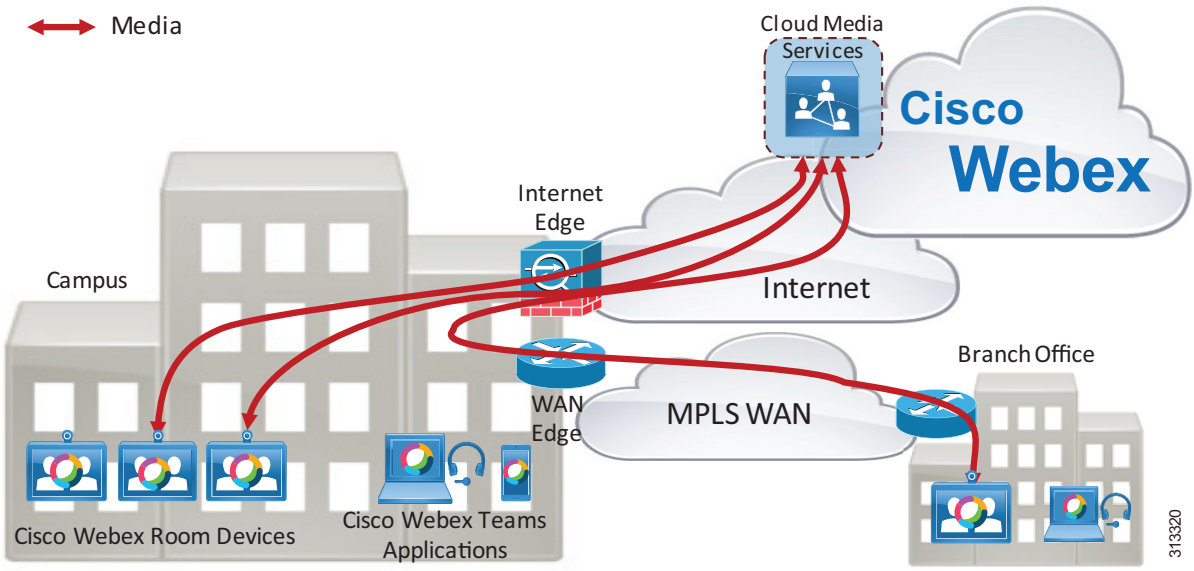
- The external firewall will need to allow UDP traffic from ANY port to the address of the Video Mesh Nodes via port 5004, so that roaming Webex Teams endpoints can send media to the nodes. This is not a preferred approach.
- DMZ-based deployment can lead to cases where media is sent from the corporate network to a Video Mesh cluster in the DMZ and back to the corporate network. This can happen when two internal Webex Teams endpoints are in a meeting. Both endpoints will send media from the corporate network to the Video Mesh cluster in the DMZ.

Deploying Video Mesh Clusters in Large Population Centers

Video Mesh clusters should be deployed in sites with large numbers of Webex Teams endpoints. Deploying the Video Mesh Nodes in such sites provides the biggest bandwidth savings, as endpoints will discover and send media to the local Video Mesh cluster instead of media being routed over the WAN to a remote Video Mesh cluster or media being routed to Webex. As a best practice, deploy a small Video Mesh cluster initially. Clusters can be increased in size and number, based on traffic patterns monitored via the Webex Control Hub.

The example scenario in Figure 4-2 shows a large campus site with a large number of Webex Teams devices. The large campus site has direct Internet access (DIA) as well as MPLS WAN connectivity to a branch office. The branch office has a small number of Webex Teams endpoints and has MPLS WAN connectivity to the campus site. The branch office in this case must route traffic destined for the Internet via the MPLS WAN to the campus site's Internet edge router.

Figure 4-2 Media Paths from Webex Teams Endpoints to Webex



When Webex Teams endpoints in the campus and branch office start up, they register to Webex. This organization does not have any Video Mesh Nodes deployed, so the Webex Teams endpoints will send media directly to Webex when in a meeting. The Webex Teams endpoints in the campus site will route media to Webex via the Internet edge router, while the Webex Teams endpoints in the branch office will route media via the MPLS WAN to the campus site and to Webex via the Internet edge, as illustrated in Figure 4-2.

As the number Webex Teams endpoints at the campus site increases, bandwidth usage at the Internet edge increases. As the number of Webex Teams endpoints at the branch site increases, bandwidth usage at the WAN edge between the campus and branch site increases, and so does the bandwidth usage at the Internet edge.

If we consider that the average media bandwidth required for a Webex Teams endpoint while in a meeting is 2 Mbps, we can determine the bandwidth required for Webex Meetings in this organization as the sum of the bandwidth usage for all endpoints actively in a meeting:

- Internet edge bandwidth required (Mbps) = (campus(n) + branch(n)) * 2
- WAN edge bandwidth required (Mbps) = branch(n) * 2

Where campus(n) is the number of Webex Teams endpoints actively in a meeting at the campus site, and branch(n) is the number of Webex Teams endpoints actively in a meeting at the branch site.

Typically busy hour call attempts (BHCA) are used to determine the number of concurrent calls required in this type of calculation (that is, the number of campus and branch endpoints actively in a meeting). Without knowledge of the BHCA of the deployed Webex Teams endpoints or the number of maximum concurrent calls during the busy hour, a good starting point is 1 concurrent call for every 4 users. So if there are 100 users, then 25 concurrent calls could be assumed. This number would change based on the type of business and user groups, but 25% is a reasonable initial estimate when the number of concurrent calls is unknown.

Note that Webex Teams endpoints can use more than 2 Mbps of bandwidth when in a meeting. Webex Teams endpoints consistently use 80 kbps to send and receive audio. Video rates can vary greatly depending on a number of factors, including endpoint type, multi-stream capabilities, and negotiated bit rate.

Deploying a Video Mesh cluster in the campus site reduces Internet edge bandwidth requirements for Webex Meetings by keeping the media local.

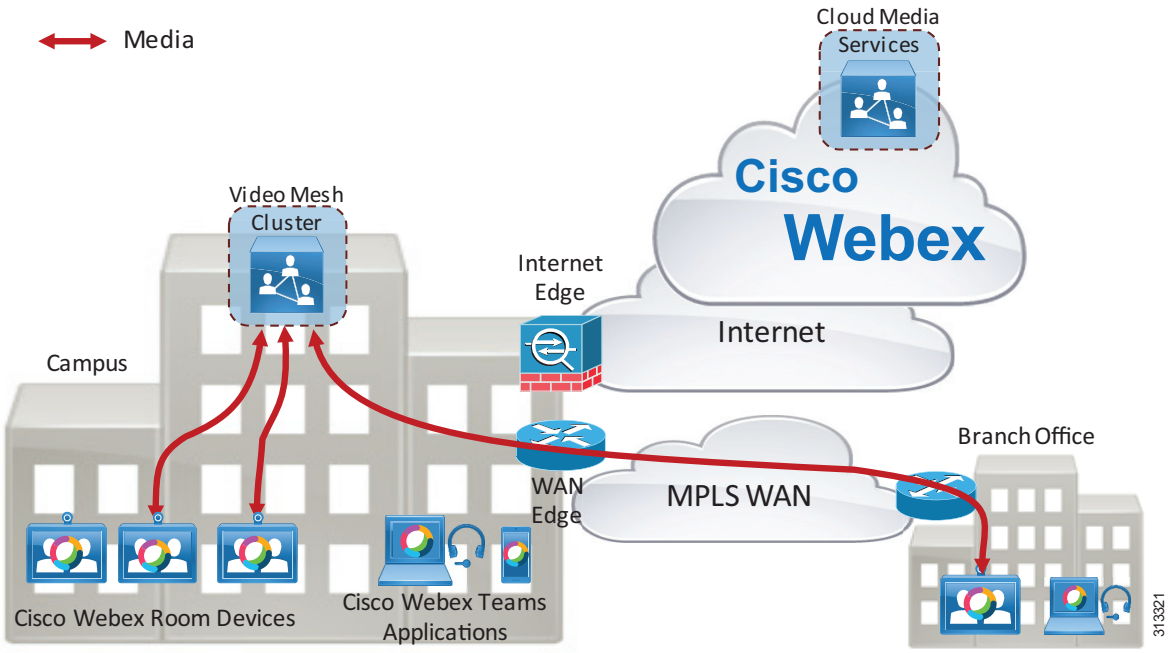
When Webex Teams endpoints in the campus and branch office start up, they register to Webex. If a Video Mesh cluster is deployed, Webex will provide the Webex Teams endpoints with the addresses of the Webex cloud media services and the Video Mesh cluster.

The Webex Teams endpoints perform a connectivity test to the Video Mesh cluster and the Webex cloud media services. The Video Mesh cluster connectivity test should be successful because the Video Mesh cluster is reachable from anywhere on the corporate network. The connectivity test to the Webex cloud media services should also be successful.

The Webex Teams endpoints then perform a STUN test to calculate round-trip delay (RTD) time to available media node clusters (cloud and Video Mesh). The Webex Teams endpoints at the campus site are located at the same site as the Video Mesh cluster, so the RTD to the Video Mesh cluster should be lower than the RTD to the Webex cloud media services. The Webex Teams endpoints at the branch site route STUN tests via the WAN to the Video Mesh cluster and out the Internet edge to the Webex cloud media services. The RTD to the Video Mesh cluster should be shorter than the RTD to the Webex cloud media services. Based on the results of the STUN tests, the Webex Teams endpoints will send media to the Video Mesh cluster when in a meeting, as illustrated in Figure 4-3.

Note that the Webex Teams endpoints will perform this action of testing the connectivity and RTD to the clusters each time the endpoint starts up, at a network change, or after the 2-hour cache has expired.

Figure 4-3 Media Paths from Webex Teams Endpoints to the Video Mesh Cluster



Webex Teams endpoints at the campus site will route media to the Video Mesh cluster, while Webex Teams endpoints at the branch site will route media over the WAN to the Video Mesh cluster. Since there are no Webex Teams endpoints roaming outside of the corporate network (Webex Teams endpoints that are not connected to the corporate network directly or via VPN) in this scenario, and there is sufficient meeting capacity in the Video Mesh cluster, Webex media will not traverse the Internet edge, thus saving bandwidth usage to the Internet. WAN edge bandwidth usage will still be based on the number of Webex Teams endpoints in the branch site connected to a Webex meeting. Therefore, as the number of Webex Teams endpoints on the corporate network increases, so does the bandwidth savings to the Internet by deploying Video Mesh Nodes.

Cascading

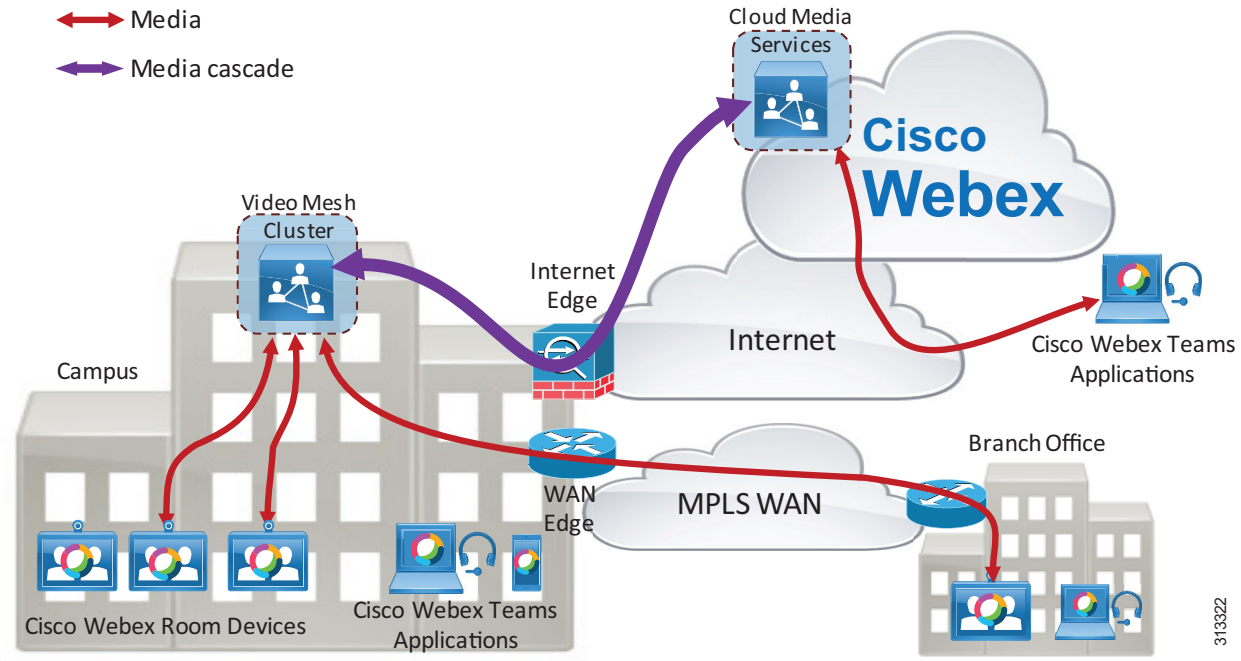
The Video Mesh cluster creates a media cascade to the Webex cloud media services if the Webex meeting includes an endpoint that is not using that specific Video Mesh cluster for media termination. This can happen when:

- A Webex Teams endpoint is roaming outside of the corporate network
- The Video Mesh cluster is full
- An endpoint that is not a Webex Teams endpoint is in the meeting (for example, a Webex Meetings application sending media directly to the Webex cloud media services)

When a roaming Webex endpoint starts up, it performs connectivity tests to Video Mesh clusters provisioned in the organization. If the Webex Teams endpoint is outside of the corporate network, connectivity tests will fail and the Webex Teams endpoint will register to the Webex cloud media services for media termination. This scenario assumes that the Webex Teams endpoint is not connected to the corporate network via VPN and that the Video Mesh cluster is deployed on the corporate network and not in the DMZ.

Figure 4-4 depicts an example deployment with four participants attending a Webex meeting. There are three Webex Teams devices on the corporate network, and they have registered with a Video Mesh cluster for media termination. This included one Webex Teams endpoint in the branch office connected via a WAN. There is also one roaming Webex Teams application that has registered to the Webex cloud media services for media termination. When the meeting starts, the Video Mesh cluster creates a media cascade link to the Webex cloud media services.

Figure 4-4 Cisco Video Mesh Cluster Cascading to the Webex Cloud Media Services

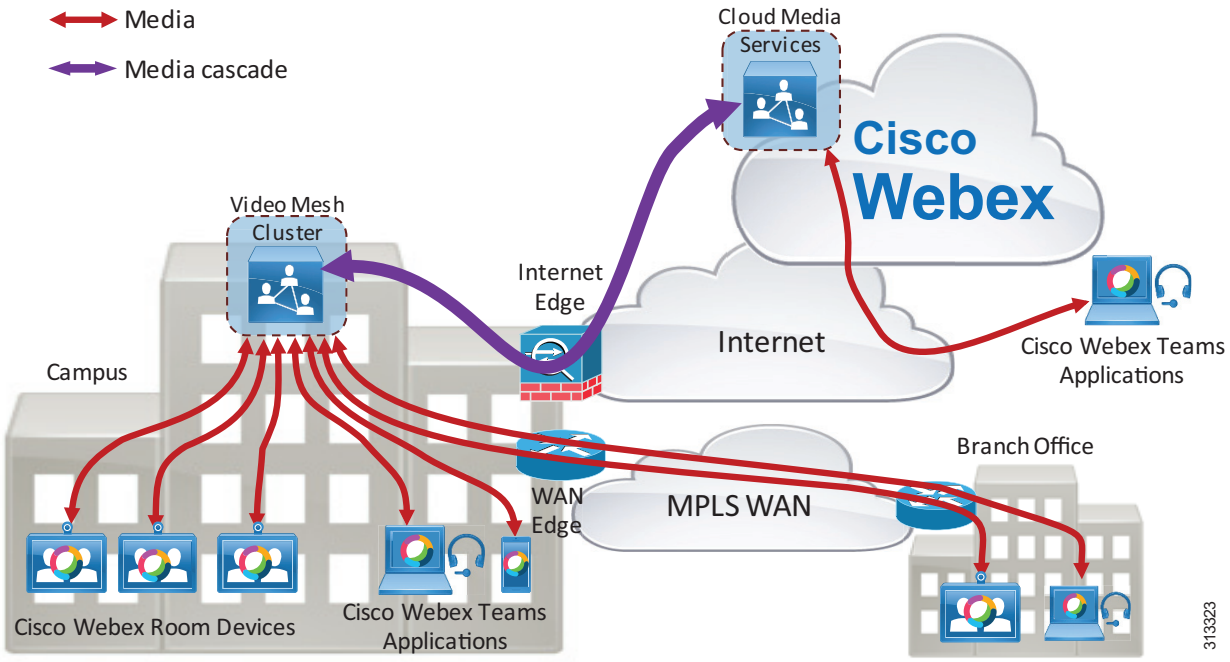


The media cascade link created in this scenario carries multiple video streams sent by the three corporate network-based Webex Teams endpoints from the Video Mesh cluster to the Webex cloud media services. Each endpoint can also send multiple streams. The purpose of the multiple streams being sent in the cascade link is to allow the roaming endpoint to receive multiple streams (if capable) and to control the video layout (for example, setting the video layout to show the active speaker main video and up to five picture-in-picture frames, or to show the video layout in equal segments regardless of who is the active speaker).

The Video Mesh cluster can send the video of up to six endpoints per meeting to Webex in the cascade link. Each endpoint may send more than one stream and/or resolution (multistream capabilities).

The example deployment in Figure 4-5 shows a Webex meeting with eight participants. Seven participants are using Webex Teams endpoints that are connected to the corporate network, and one participant is roaming.

Figure 4-5 Webex Video Mesh Cluster Cascading Example



The seven Webex Teams endpoints on the corporate network in Figure 4-5 have registered to the Video Mesh cluster, and the roaming Webex Teams endpoint has registered to the Webex cloud media services. Because there is a roaming participant, the Video Mesh cluster will create a media cascade link to Webex. The cascade link can carry a maximum of six participant's audio/video streams to Webex. In this scenario there are seven meeting participants sending media to the Video Mesh cluster. The cascade link will carry the last six active speakers' video streams from the Video Mesh cluster to Webex, and it will carry one participant's video from Webex to the Video Mesh cluster (because there is only one roaming Webex Teams endpoint in this scenario). Note that the cascade link from Webex to the Video Mesh cluster can also carry a maximum of six participant's video.

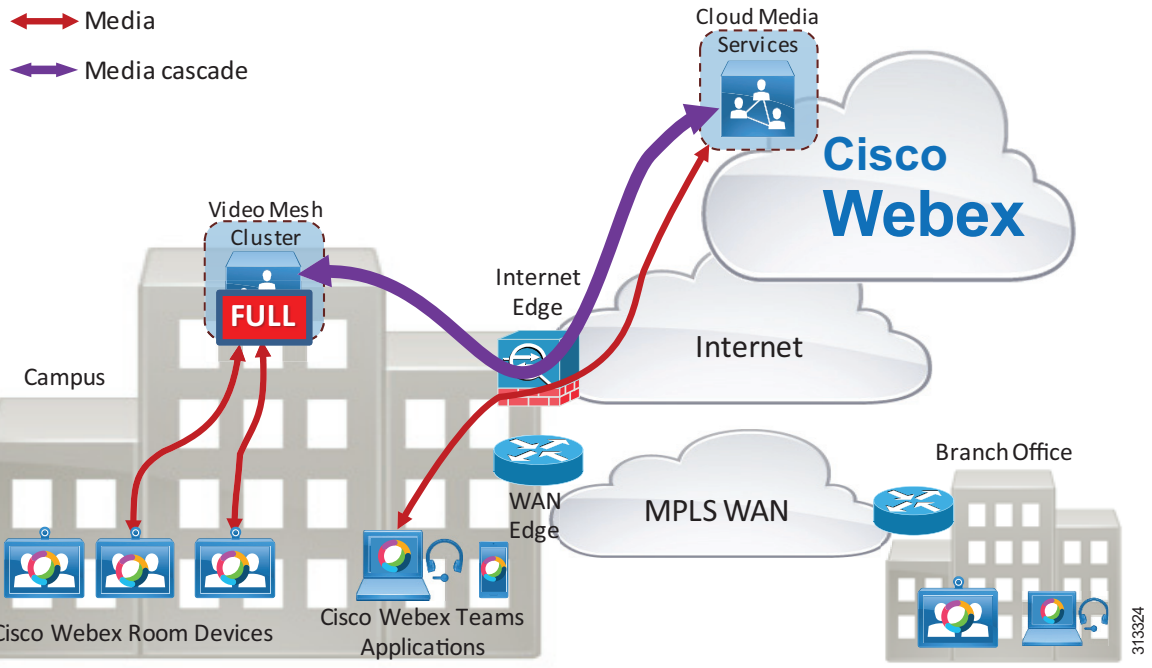
The following considerations apply to Video Mesh clusters and cascade links:

- The Video Mesh cluster provides more bandwidth savings at the Internet edge as the number of on-premises participants in a single meeting increases above six.
- Each participant's device can send multiple streams, depending on the video layout requested by the devices.
- The bandwidth requirement at the WAN edge is not affected by the placement of a Video Mesh cluster in the campus site. Media is still sent and received over the WAN to/from the Video Mesh cluster. In general, WAN bandwidth is more expensive than direct Internet access bandwidth, therefore direct Internet access from the remote sites is preferred for Webex Teams endpoints.
- As the number of concurrent meetings increases, the likelihood is that there will be more cascade links created due to roaming or remote participants. Cascade links can use a large amount of bandwidth in both directions. You should plan for and continuously monitor these bandwidth usage requirements in your organization. Use the Webex Control Hub reporting feature to monitor how Webex Video Mesh services are being used.

If the available Video Mesh clusters in an organization are at full capacity, Webex Teams endpoints will be directed to use Webex cloud media services for media termination. In Figure 4-6, the Video Mesh cluster is serving a large number of Webex Teams endpoints attending meetings, and it reaches its full

capacity. There are two Webex Teams devices on the corporate network in a meeting with each other. Both devices are registered to the Video Mesh cluster for media. A third Webex Teams endpoint on the corporate network joins the meeting. Webex is aware that the available Video Mesh cluster is full, so it directs the third Webex Teams endpoint to register with the Webex cloud media services. The Video Mesh Node creates a cascade link to the Webex cloud media services, and all three participants are now in the meeting.

Figure 4-6 Webex Video Mesh Cluster Cascading Due to Capacity Limit



Webex provides overflow for Webex Teams endpoints that cannot send media to a Video Mesh cluster when it has reached full capacity. The cascade link bridges the Video Mesh cluster to Webex.

Multistream Cascading

The multistream technology applied to Webex Teams endpoints also applies to the cascade link. For example, a Video Mesh Node can send multiple video streams per endpoint inside the cascade link to Webex. For details, see the Multistream Cascading section in the Bandwidth Management chapter.

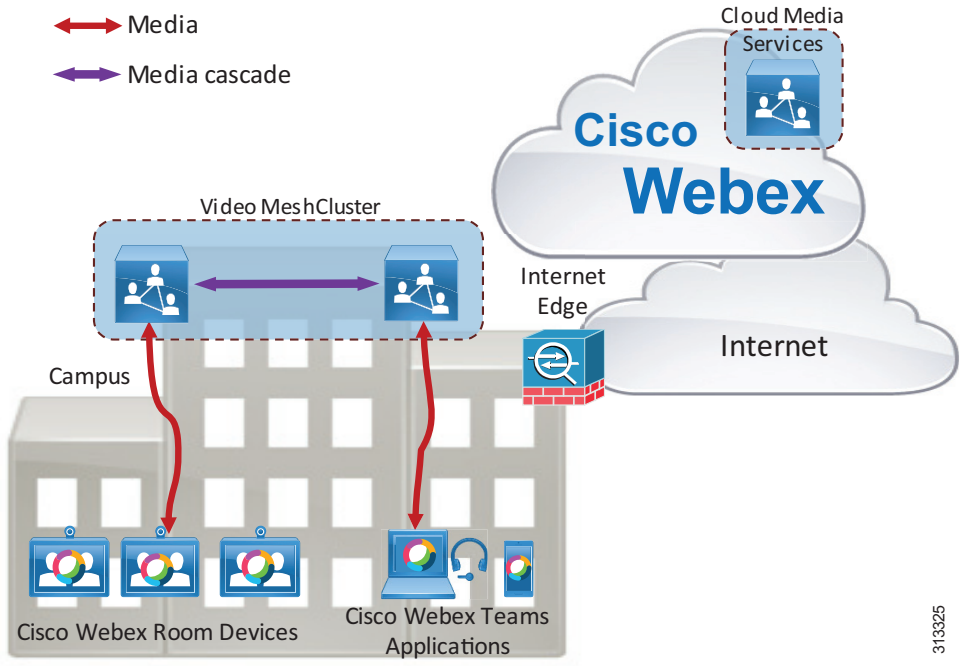
Clustering

Video Mesh Nodes should be deployed in clusters. A cluster of nodes provides larger capacity than a single Video Mesh Node. It also provides redundancy in case a single node becomes unavailable for any reason. The Video Mesh Nodes are in an active/active state in a cluster.

When a Webex Teams endpoint discovers a Video Mesh cluster, Webex assigns the endpoint to use a particular node in that cluster. Two Webex Teams endpoints in the same site, attending the same meeting, will typically be assigned to the same Video Mesh Node by Webex. However, Webex Teams endpoints attending the same meeting may be assigned to different nodes in the cluster if one of the nodes becomes

full. In that case the meeting will be cascaded across the nodes in the cluster, as illustrated in Figure 4-7.

Figure 4-7 Webex Video Mesh Cluster Cascading

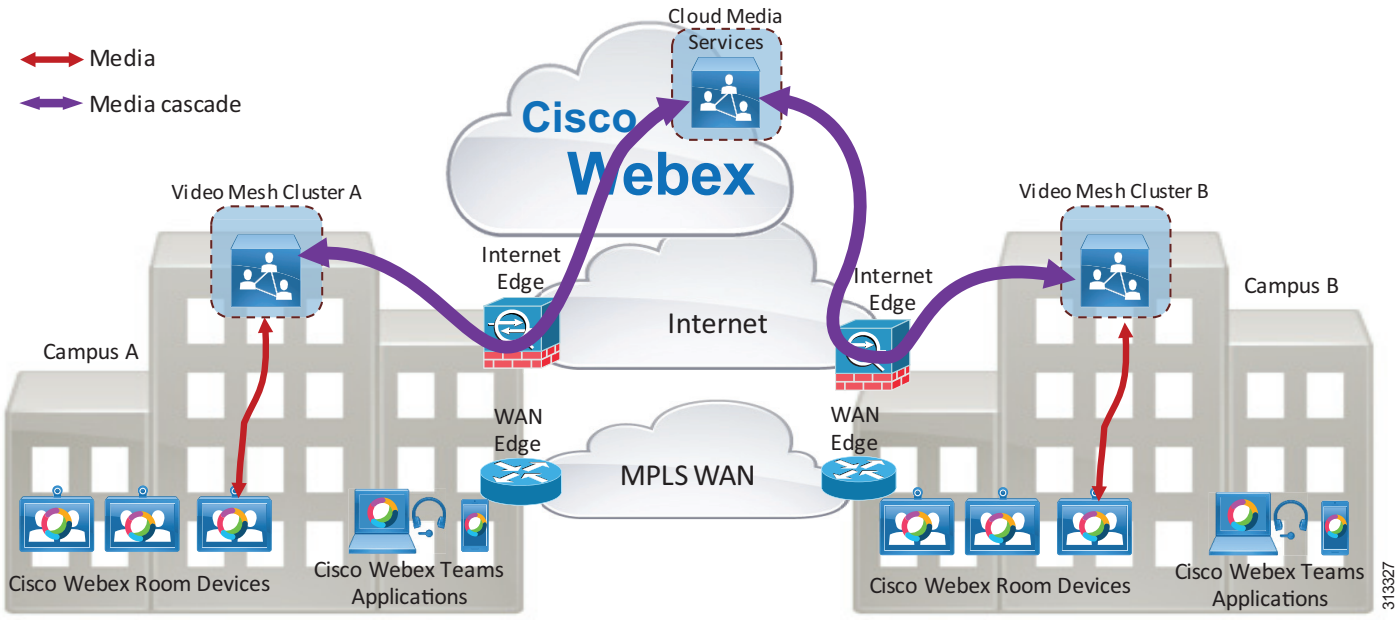


We recommend deploying the Video Mesh cluster in a single site and *not* clustered over a WAN. Clustering Video Mesh Nodes over a WAN can lead to inefficient media paths, such as hairpinning of media between data centers, which causes increased bandwidth consumption. Having media cascade to Webex is a more efficient use of bandwidth than having media cascade between nodes located over a WAN, for the following reasons:

- Media hairpinning can be avoided
- WAN edge bandwidth is generally much more expensive than Internet edge bandwidth

Deploying a cluster in a single site avoids the scenario of Video Mesh Nodes cascading over the WAN. For example, Figure 4-8 shows a deployment with two Video Mesh clusters. Cluster A is deployed in Campus A, and Cluster B is deployed in Campus B. A Webex Teams endpoint in Campus A and a Webex Teams endpoint in Campus B join a meeting. The Webex Teams endpoint in Campus A is assigned to a Video Mesh Node in Cluster A (lowest RTD time), and the Webex Teams endpoint in Campus B is assigned to a Video Mesh Node in Cluster B (lowest RTD time). Each Webex Teams endpoint sends media to its assigned node. Because the two assigned Video Mesh Nodes being sent media from the endpoints in the meeting are in different clusters, they each cascade media to Webex. There is no hairpinning of media in this case, and the WAN edge bandwidth is not impacted.

Figure 4-8 Webex Video Mesh Cluster per Site



There is no maximum limit to the number of nodes you can deploy in a Video Mesh cluster. As busy hour calling rates increase, the bandwidth requirements at the Internet edge will increase; and depending on the network architecture, the WAN edge bandwidth requirements might also increase. Adding more nodes to a Video Mesh cluster will increase the cluster capacity.

We do not recommend deploying a Video Mesh cluster in every location. Due to the distributed nature of most meetings, deploying a Video Mesh cluster in every location will not lead to bandwidth savings. Instead, we recommend deploying Video Mesh clusters in locations that host regular localized meetings.

Also, we recommend starting with a small number of Video Mesh Nodes in each cluster, and then growing the clusters over time based on usage monitored and reported in the Webex Control Hub.

The following considerations apply to Video Mesh clusters:

- Extra capacity can be added to the Video Mesh cluster by adding more nodes.
- Adding more nodes to the Video Mesh cluster increases hardware requirements. Hardware costs should be weighed against bandwidth costs when considering whether to add more nodes to the cluster to avoid cascade links due to capacity limitations.
- Cascade links are created for meetings with roaming or remote participants, regardless of cluster capacity.

Direct Internet Access and Centralized Internet Access

Some organizations deploy their network in such a way that only certain sites have direct Internet access (DIA). In this type of deployment, DIA is usually available at large campus sites only, and the organization's branch sites are provisioned with connectivity to an MPLS WAN network. Branch site applications that access services on the public Internet will route traffic via the WAN to the closest site with DIA. This can lead to inefficient traffic routes, especially for real-time traffic such as audio and video.

MPLS WAN bandwidth is typically much more expensive than direct Internet bandwidth. Providing direct Internet access to branch offices can help provide the most efficient media paths for Webex Teams endpoints.

For branch sites that do not have a Video Mesh cluster deployed but that do have direct Internet access and WAN connectivity to a campus site, we recommend connecting the branch sites' Webex Teams endpoints to the Webex cloud media services instead of to a Video Mesh cluster located at the campus site. This means that the branch sites' Webex Teams devices and applications will route their media traffic via the Internet edge to the Webex cloud media services instead of routing media over the WAN. This can be configured by blocking access to the IP addresses of all Video Mesh Nodes at the WAN edge firewall (but only at branch offices with direct Internet access). When Webex Teams endpoints in the branch office perform connectivity tests to the Video Mesh cluster, connectivity will fail and the endpoints will connect to the Webex cloud media services.

Deploying Video Mesh Nodes in Sites with Direct Internet Access

Deploy Video Mesh clusters only in sites that have direct Internet access. Video Mesh clusters will often have to cascade media streams to Webex. Cascading media over the MPLS WAN can use large amounts of WAN bandwidth and lead to inefficient media paths.

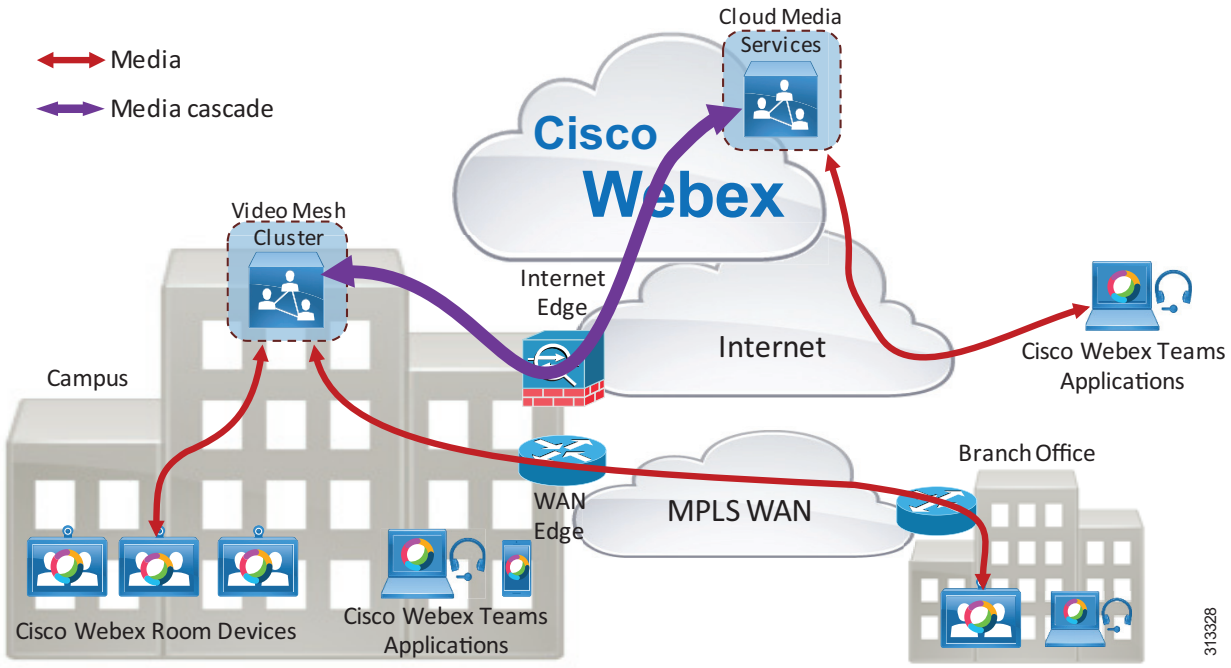
Deploying a Video Mesh cluster in a branch office that does not have direct Internet access can sometimes provide bandwidth savings if that branch has regular Webex meetings with local Webex Teams endpoints only. However, with this deployment model, WAN bandwidth consumption increases if the Webex meetings include roaming participants. Because most meetings have participants distributed in a number of locations, both on the corporate network and on the public network, we recommend that you do not deploy Video Mesh clusters in sites that do not have direct Internet access.

Deploying Video Mesh clusters in sites with no direct Internet access can lead to various issues such as:

- Cascaded media might be routed over the WAN to a site with direct Internet access.
- Webex Teams endpoints might send media to a remote Video Mesh Node over the WAN instead of using their direct Internet access (not ideal and can use WAN resources inefficiently).

Deploying Video Mesh clusters only in sites that have direct Internet access will ensure that media cascaded links are not sent over the MPLS WAN, as illustrated in Figure 4-9.

Figure 4-9 Webex Video Mesh Cluster Deployed in a Site with Direct Internet Access



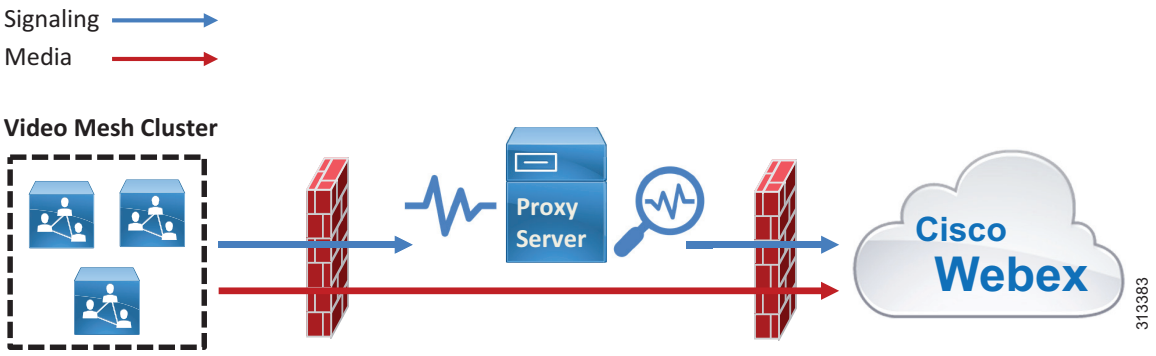
Deploying Video Mesh Nodes in Sites with HTTP(S) Proxy Servers

Cisco Webex Video Mesh supports transparent inspecting and non-inspecting proxies (see Figure 4-10). You can tie these proxies to your Webex Video Mesh deployment so that you can secure and monitor traffic from the enterprise out to the cloud. You can use the Webex Video Mesh administration interface for certificate management and overall connectivity status after you implement the proxy with the nodes.

The following proxy types are supported by Video Mesh:

- Transparent Proxy (non-inspecting) — Video Mesh nodes are not aware that they are going through a proxy and should not require any changes to work with a non-inspecting proxy.
- Transparent Proxy (tunneling or inspecting) — Video Mesh nodes are not aware that they are going through a proxy. No http(s) configuration changes are necessary on Video Mesh; however, the Video Mesh nodes need a root certificate so that they trust the proxy. Inspecting proxies are typically used by IT to enforce policies regarding which websites can be visited and which types of content are not permitted. This type of proxy decrypts all of your http and https traffic.

Figure 4-10 Proxy Support for Video Mesh Nodes



Deploying Webex Video Mesh for SIP Endpoints

SIP endpoints registered to Cisco Unified CM can send audio, video, and screen share content to a Webex Video Mesh cluster when joining Webex Meetings, provided that the Webex Meetings site is configured to allow Webex Video Mesh.

The following statements describe how Unified CM SIP endpoints can use Webex Video Mesh for Webex Meetings (see Figure 4-11).

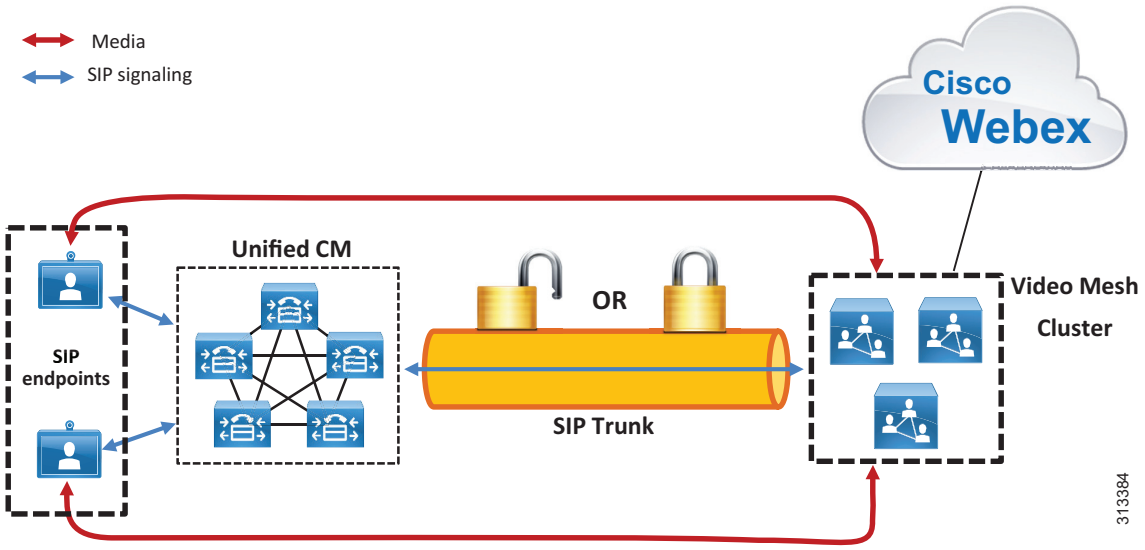
- A Unified CM SIP trunk can be pointed to nodes in a Video Mesh Cluster.
- A Unified CM SIP trunk to a Video Mesh cluster may be secured with TLS, and SIP endpoint media through the Video Mesh cluster may be encrypted.
- A Unified CM SIP route pattern can route calls based on a specific domain (for example, sitename.webex.com) via the SIP trunk to a node in the Video Mesh cluster.
- The Video Mesh Node will signal to Webex to set up a meeting, and Webex will determine the cluster node where the meeting will be hosted.
- The Video Mesh Node will then signal to Unified CM to indicate which node in the cluster should be used for media.
- The SIP endpoint will send media to the selected node.

The Video Mesh cluster will cascade media to Webex if:

- There is a participant in the meeting using the Webex Meetings App
- There is a participant in the meeting hosted on a different Video Mesh cluster
- There is a participant in the meeting sending media directly to Webex

If there are no nodes available, (for example, the cluster is at capacity), Unified CM can route the call to Webex via Cisco Expressway by using the route list logic of Unified CM in response to a failure message sent by the Video Mesh cluster.

Figure 4-11 SIP Endpoints Sending Media via a Video Mesh Cluster



Deploying Video Mesh Clusters in Large Population Centers

The best practices for where to deploy Video Mesh clusters for Webex Teams endpoints also apply for Unified CM SIP endpoints. Video Mesh Clusters should be:

- Deployed on the corporate network
- Deployed in high population centers
- *Not* clustered over a WAN
- Deployed in sites with direct Internet access (DIA)

Analytics should also be monitored continuously to determine if more nodes are required in a particular location. For more details, see the section on Monitoring Analytics.

SIP Trunk Design

Configure a SIP trunk on Unified CM to point to a Webex Video Mesh cluster to route SIP calls to a Video Mesh Node. The SIP trunk can be pointed to a maximum of 16 Video Mesh Nodes.

The trunk should point to a Video Mesh cluster that will host meetings for endpoints that register to that Unified CM cluster. The closer the endpoints are to the Video Mesh cluster, the more efficient the call flows and bandwidth usage become. For example, endpoints on the same LAN as the Video Mesh cluster will send media directly to the cluster, and thus the media will not traverse a WAN.

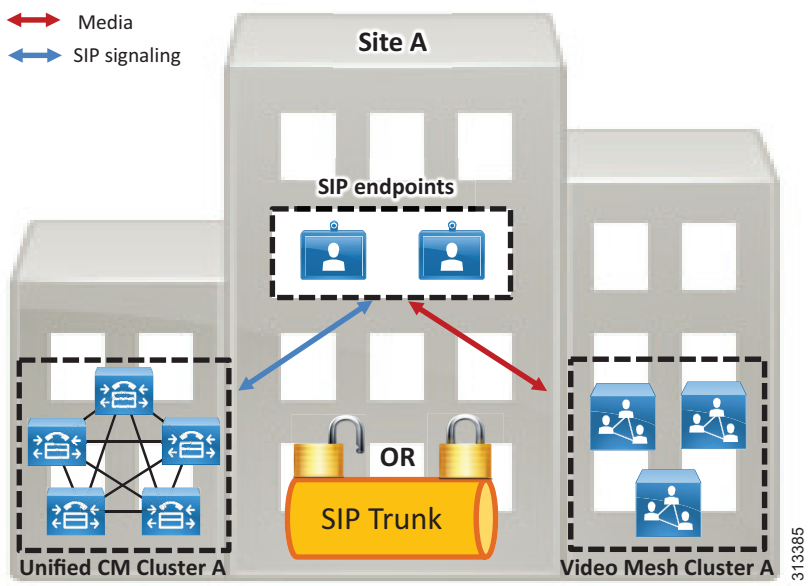
We recommend pointing the trunk to Video Mesh Nodes from a single Video Mesh cluster, and pointing the trunk to all nodes within the cluster (16 maximum). **Run on all Active Unified CM Nodes** should also be enabled on the SIP trunk to ensure efficient traffic signaling in Unified CM. Pointing a SIP trunk to a single cluster will ensure that meetings are hosted on that cluster (unless the cluster reaches capacity). This provides more control and predictability of where meetings will occur and how much bandwidth will be needed. It also allows the administrator to expand the Video Mesh cluster by adding more nodes if more SIP endpoints are configured on the Unified CM cluster.

The Unified CM SIP trunk will determine which node in the Video Mesh cluster is used for call setup. Webex determines which node within that Video Mesh cluster hosts the meeting (that is, the node to which endpoints send media).

The trunk should be configured with the FQDN of all Video Mesh Nodes in the cluster (up to 16 nodes). This will allow for high availability so that if a node becomes unavailable, the call will be set up using a different available node configured in the SIP trunk. The destination port for each Video Mesh Node FQDN should be set to port 5060 (SIP over TCP) or 5061 (SIP over TLS).

For example, Figure 4-12 shows Site A with a Unified CM cluster and a Video Mesh cluster containing 3 nodes. The nodes have FQDNs vmn-1-siteA.ent-pa.com, vmn-2-siteA.ent-pa.com, and vmn-3-siteA.ent-pa.com.

Figure 4-12 SIP Trunk Configured to Point to a Video Mesh Cluster



The SIP trunk in Figure 4-12 should be configured as shown in Table 4-6 to point to the Video Mesh Nodes.

Table 4-6 SIP Trunk Configuration Settings

Destination (Node) #	Destination Address	Destination Port
1	vmn-1-siteA.ent-pa.com	5060 or 5061
2	vmn-2-siteA.ent-pa.com	5060 or 5061
3	vmn-3-siteA.ent-pa.com	5060 or 5061

As more nodes are added to the cluster to provide more capacity, the new nodes should be added to the SIP trunk.

This configuration for Site A ensures that all SIP endpoints registered to the Site A Unified CM cluster will use the Site A Video Mesh cluster for Webex Meetings. Assuming endpoints registering to the Site A Unified CM are geographically nearby, this will provide the best use of bandwidth.

The SIP trunk must have an associated SIP Profile. Most SIP Profile defaults apply; however, ensure that the following items are set:

- Set **Early Offer support for voice and video calls** to **Best Effort (no MTP inserted)**.
- Set **SIP OPTIONS Ping** to **enabled**.
- Set **Allow Presentation Sharing using BFCP** to **enabled**

Secured SIP Trunk and Media Encryption to Video Mesh Cluster

Video Mesh nodes support SIP trunk TLS and media encryption for SIP endpoints registered to Unified CM. There are a few requirements for this support as well as a few benefits.

Benefits:

- Secured signaling and media encryption end-to-end
- Roster List with Video Mesh cascade links — This feature requires the entire media flow to be encrypted end-to-end.

Requirements:

- Unified CM must be in mixed mode.
- All Video Mesh nodes must be enabled with secured trunks within the organization, and the feature must be enabled on the Control Hub at the organization level.
- If encryption is enabled, it will be required between SIP endpoints and the Video Mesh nodes. This means that SIP endpoints must have a certificate [locally significant certificate (LSC) recommended] and a device security profile with encryption enabled. Endpoints without a certificate and an encryption-enabled security profile will not be able to connect to the Video Mesh nodes.

Additional trunk configuration settings when using SIP over TLS:

- Enable sRTP Allowed
- Calling and Connecting Party Info Format: Deliver URI and DN in connected party, if available.
- Destination Port: 5061
- Video Mesh Trunk Security Profile

Trunk security profile configuration settings when using SIP over TLS:

- Device Security mode: Encrypted
- Incoming and outgoing: TLS
- X.509 Subject Name: Enter the common name of the Video Mesh node certificate
- SIP V.150 Outbound SDP offering filter: Use Default Filter

For more information about SIP Profile and SIP trunking best practices as well as security best practices, refer to the latest version of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*, available at https://www.cisco.com/go/pa.

Dial Plan Updates

Unified CM SIP endpoints can use Video Mesh clusters for terminating media for Webex Meetings only. SIP point-to-point calls or SIP calls that are not dialing into a Webex meeting do not use Video Mesh.

SIP endpoints typically dial into a Webex meeting via a SIP URI. The Unified CM dial plan must be modified to route calls as required for Webex Meetings.

Create a SIP route pattern in Unified CM to route calls based on a specific domain pattern via a specific route list and route group configuration. The route group should contain configured SIP trunks and can also be used to provide redundancy.

The SIP route pattern should be configured with the domain name for the Webex site. The domain name is usually in the format of *sitename*.webex.com. For example, if organization ent-pa.com has been configured with a Webex site of ent-pa.webex.com, then SIP endpoints in this organization will dial host-details@ent-pa.webex.com to join a Webex meeting. For this example, the SIP route pattern should be configured as shown in Table 4-7.

Table 4-7 SIP Route Pattern Example

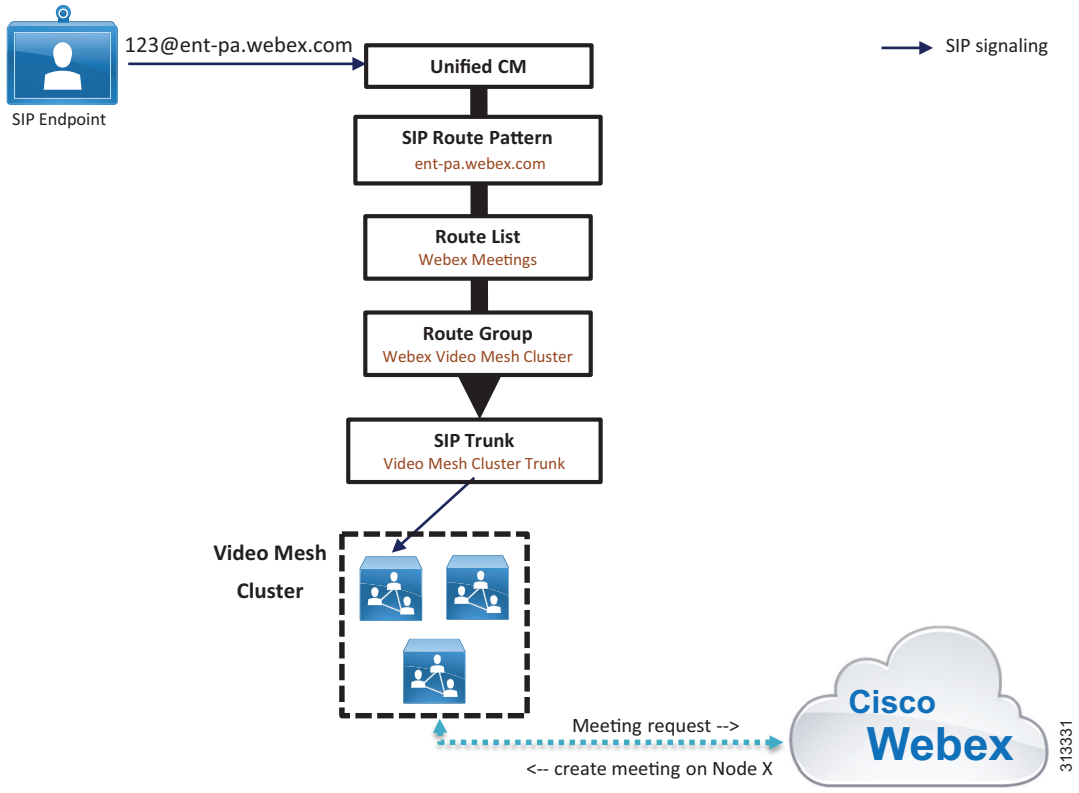
Configuration Field	Setting
IPv4 Pattern	ent-pa.webex.com
SIP Trunk/Route List	*Route list for Webex Meetings*

Create a route group is created for the Video Mesh cluster. The SIP trunk pointing to the Video Mesh cluster should be added to the Route Group Selected Devices.

Create a route list and add the route group to the top of the list in Selected Groups. This is the route list for Webex Meetings for Webex site ent-pa.webex.com on Unified CM. Specify the route list in the SIP Trunk/Route List field when you configure the SIP route pattern.

In the scenario shown in Figure 4-13, the SIP endpoint dials 123@ent-pa.webex.com.

Figure 4-13 Routing a Call from a SIP Endpoint



For the example in Figure 4-13, Unified CM routes the call via the Webex Meetings route list and route group to the Video Mesh cluster SIP trunk, according to how the SIP route pattern interprets the domain pattern ent-pa.webex.com. Unified CM routes the call invite to the node specified by the SIP trunk. (If multiple destinations are specified in the SIP trunk, a single destination is chosen randomly.) The Video Mesh Node then signals to Webex to set up a meeting. Webex then creates the meeting on one of the nodes in the Video Mesh cluster. Note that the node hosting the meeting might not be the same node that initially set up the meeting via the SIP trunk. If the node hosting the meeting reaches full capacity, another node in the cluster will be used and an intra-cluster cascade will be formed. (The intra-cluster cascade routes from node to node, not via Webex.)

If the cluster becomes full, the meeting will have to cascade to Webex to handle the overflow. This will occur automatically if a Webex Teams endpoint or application joins the meeting. The Unified CM dial plan must be modified to allow SIP endpoints to fail over to Webex (via Expressway) if the cluster becomes full.

Create a SIP trunk to an Expressway that can route to the Internet. The same Expressway that is being used for the Webex Hybrid Call Service may be used for this purpose, subject to capacity limits.

Create a route group for Expressway and add it to the route list previously created for Webex Meetings. Ensure that the Webex Video Mesh cluster route group is at the top of the list of Selected Groups in the route list configuration (see Figure 4-14). The Expressway route group should be second in the list. This will ensure that the Webex Video Mesh cluster route group will be used as priority. As the cluster reaches full capacity, it will return a SIP 4*xx* failure response to Unified CM. Unified CM will then fail over to the Expressway route group and send calls via the Expressway SIP trunk to Expressway and on to Webex.

Figure 4-14 Webex Meetings Route List Configuration

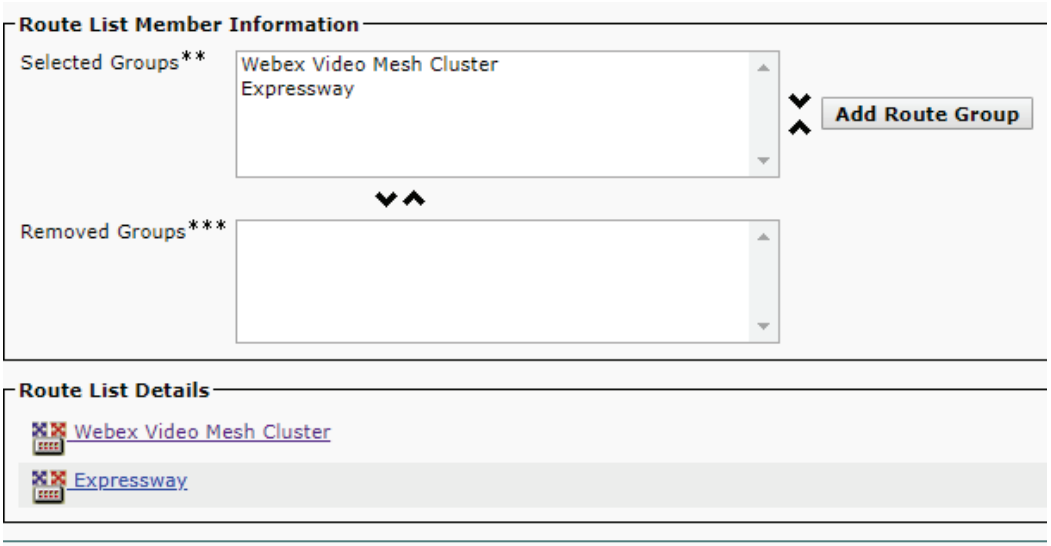
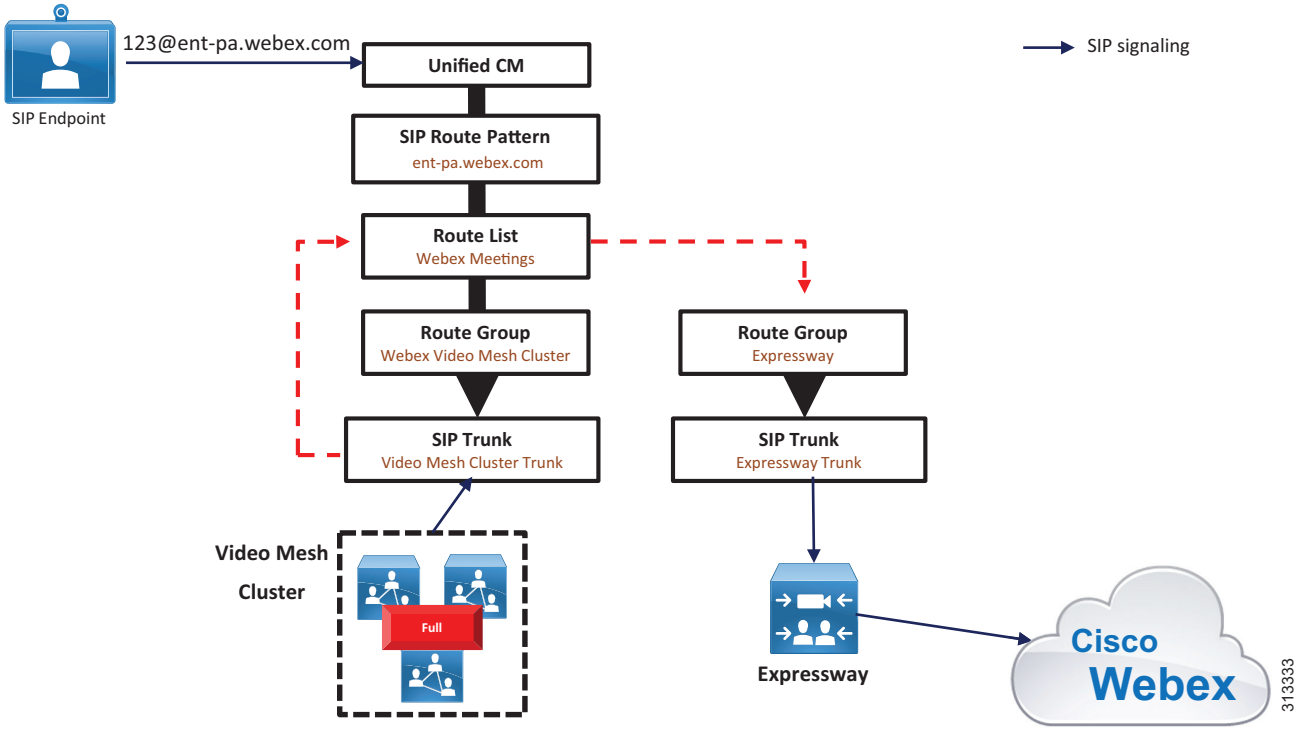


Figure 4-15 shows that a call dialed to 123@ent-pa.webex.com is rejected by the Video Mesh cluster due to the cluster being at full capacity. Based on the second route group in the list, the route list then routes the call to the Expressway SIP trunk, then to Expressway, and on to Webex.

Figure 4-15 Call Being Rerouted Due to Video Mesh Cluster Being at Full Capacity



If many calls are failing over to the Webex cloud media services via Expressway, you should add more nodes to the Video Mesh cluster to handle the load requirements.

Deploying Video Mesh Services for Multiple Unified CM Clusters

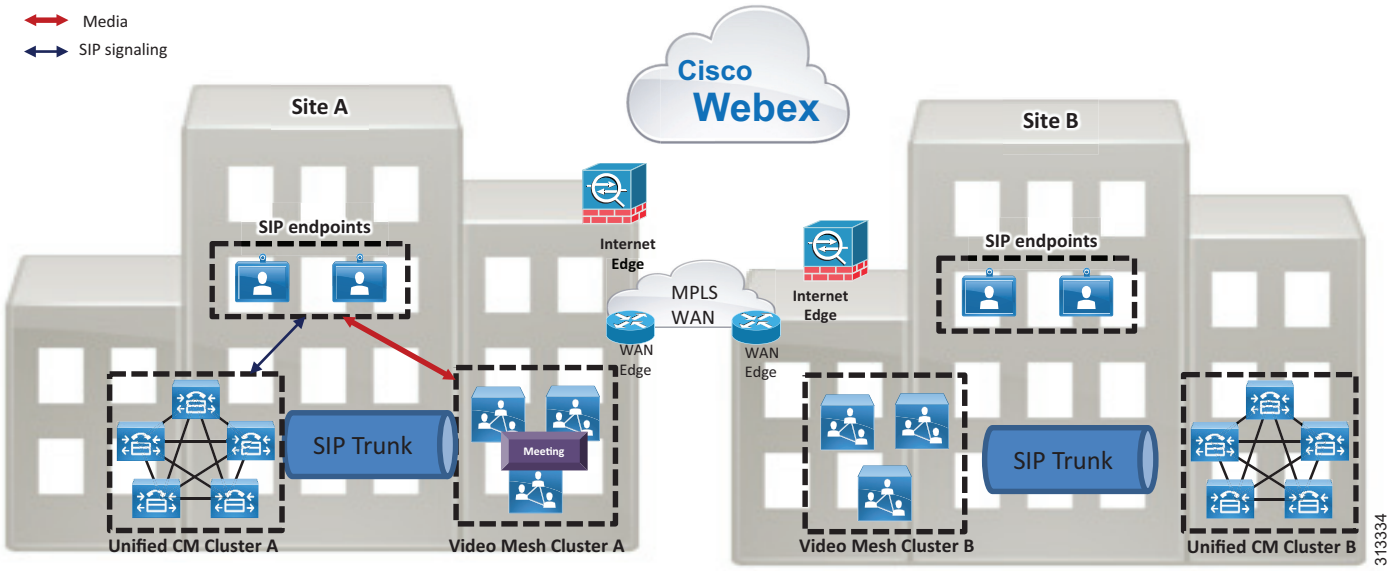
Each Cisco Unified CM cluster should point to a single Video Mesh cluster. We do not recommend pointing a Unified CM cluster to multiple Video Mesh clusters because doing so can result in endpoints that are part of the same meeting sending media to different clusters, resulting in unnecessary cascades to the cloud.

Deploy Video Mesh clusters in sites with large user populations. For the most efficient use of bandwidth, deploy Video Mesh clusters in sites with direct Internet access (DIA), and near to the endpoints. This may result in the need for multiple Video Mesh clusters for geographically dispersed deployments. Consider the example in Figure 4-16, where there are two sites, A and B. Both sites have:

- Large user populations
- Direct Internet access

Each site in Figure 4-16 has a Unified CM cluster, and a Video Mesh cluster has been deployed in each site. The endpoints in each site are registered to the local Unified CM cluster. Unified CM Cluster A has a SIP trunk pointing to Video Mesh Cluster A, and Unified CM Cluster B has a SIP trunk pointing to Video Mesh Cluster B.

Figure 4-16 Multiple Video Mesh Clusters for Multiple Large Sites

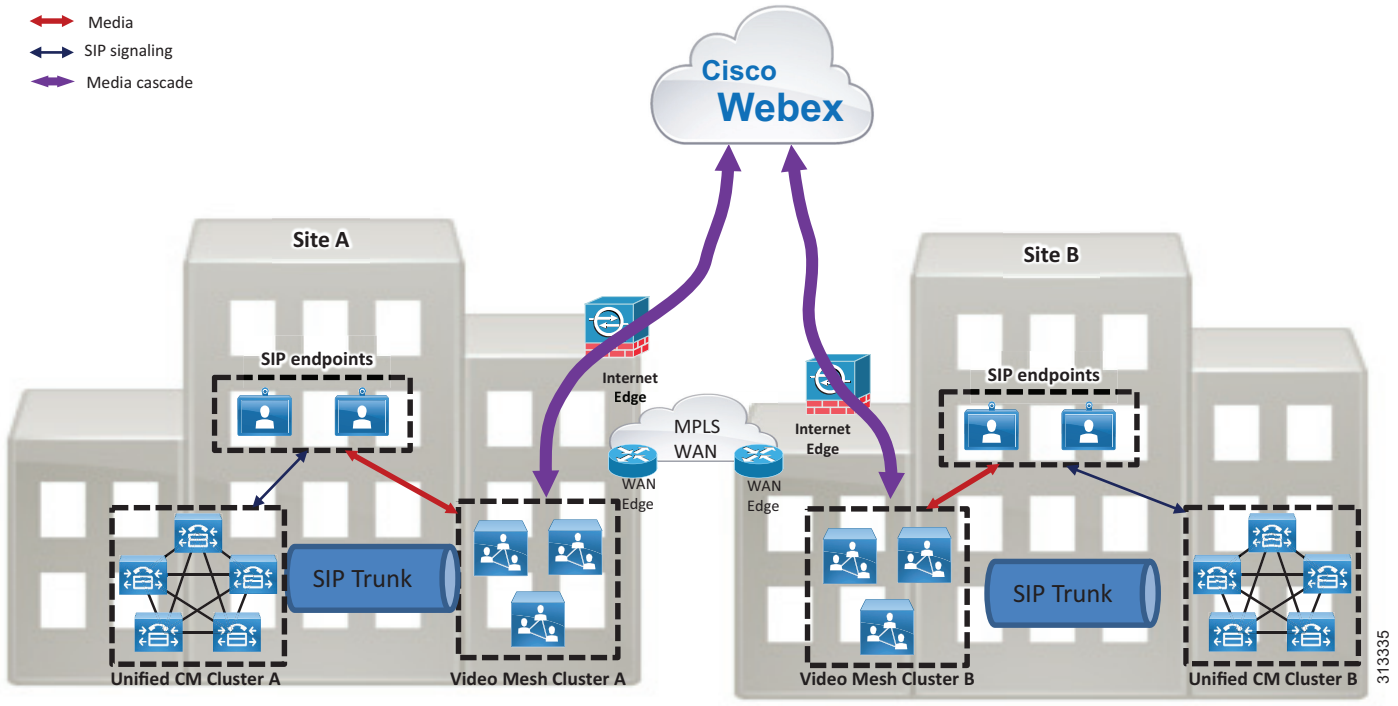


When SIP endpoints in Site A dial into a Webex meeting, they will send media to Video Mesh Cluster A. If all of the endpoints in the meeting are endpoints registered to the Site A Unified CM cluster, all media will remain on-premises, and there will not be overflow to the cloud (assuming the Video Mesh cluster has enough capacity).

If an endpoint registered to the Site B Unified CM cluster dials into the same Webex meeting, the endpoint will route media to Video Mesh Cluster B, as defined by the SIP route pattern on Unified CM Cluster B. Webex will signal to Video Mesh Cluster A and Video Mesh Cluster B to cascade media

(cascade is internally initiated) to Webex, so that all endpoints can participate in the same Webex meeting. The media cascade will be sent direct to Webex via the Internet Edge router, as shown in Figure 4-17.

Figure 4-17 Media Cascaded to Webex if Meeting Participants Are in Different Clusters



Endpoint Experience

Any of the following types of endpoints can join a Webex meeting:

- Webex Teams application
- Webex Teams device
- SIP endpoint registered to Unified CM
- Webex Meetings application

Depending on the endpoint type used to join a meeting, there may be a difference in the user experience. Webex Teams applications and devices have the same approach for Video Mesh cluster discovery and connectivity as well as a similar mid-call experience, including:

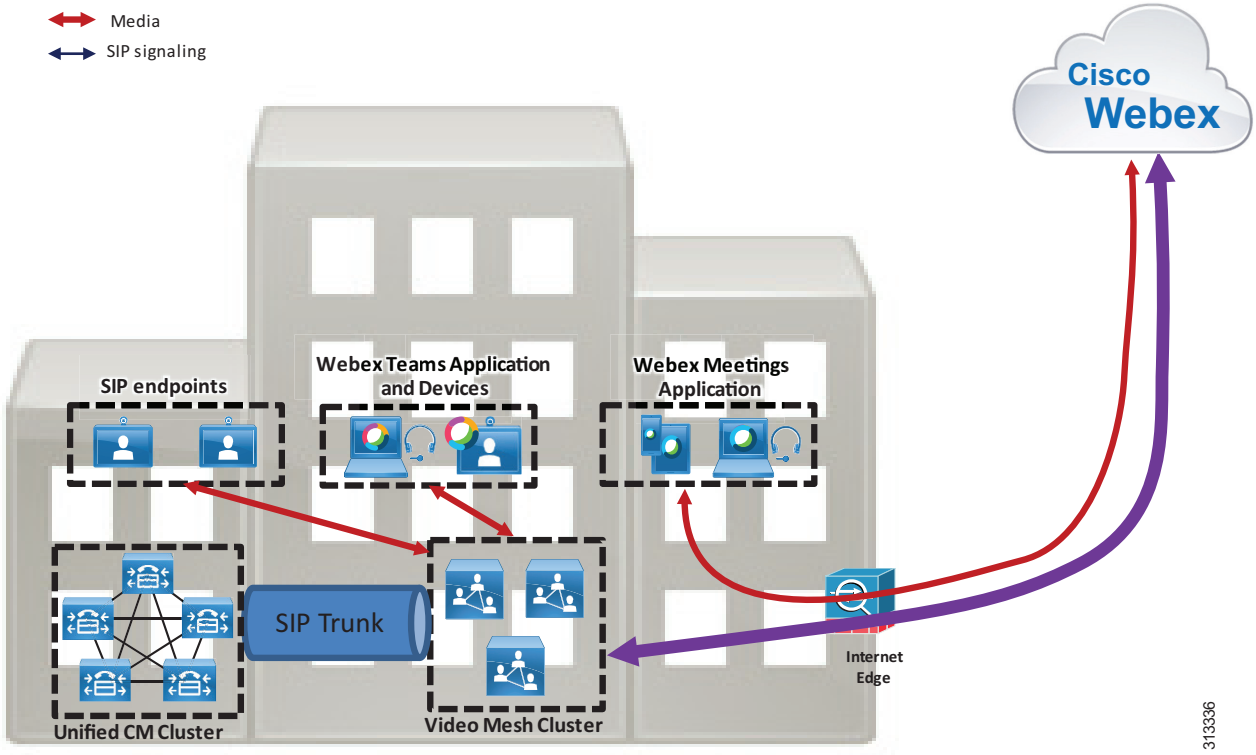
- Video multi-streaming
- Roster support

SIP endpoints discover and connect to a Video Mesh cluster based on the Unified CM configuration. SIP endpoints currently do not offer video multi-streaming or roster support.

The Webex Meetings application does not use Video Mesh for meetings; instead, it connects directly to Webex. The Webex Meeting application does offer roster support.

Figure 4-18 shows an example of the media flows when there are different types of endpoint in the same Webex Meeting.

Figure 4-18 Media Flows for Different Types of Endpoints in the Same Webex Meeting



The Webex Meeting in Figure 4-18 has participants joining via SIP endpoints, Webex Teams applications, Webex Teams devices, and Webex Meetings applications. The SIP endpoints send media to the Video Mesh cluster; the Webex Teams applications and devices also send media to the Video Mesh cluster; and the Webex Meetings Apps send media directly to Webex. The Video Mesh cluster then cascades the media to Webex to allow all endpoints to participate in the same meeting.

Monitoring Analytics

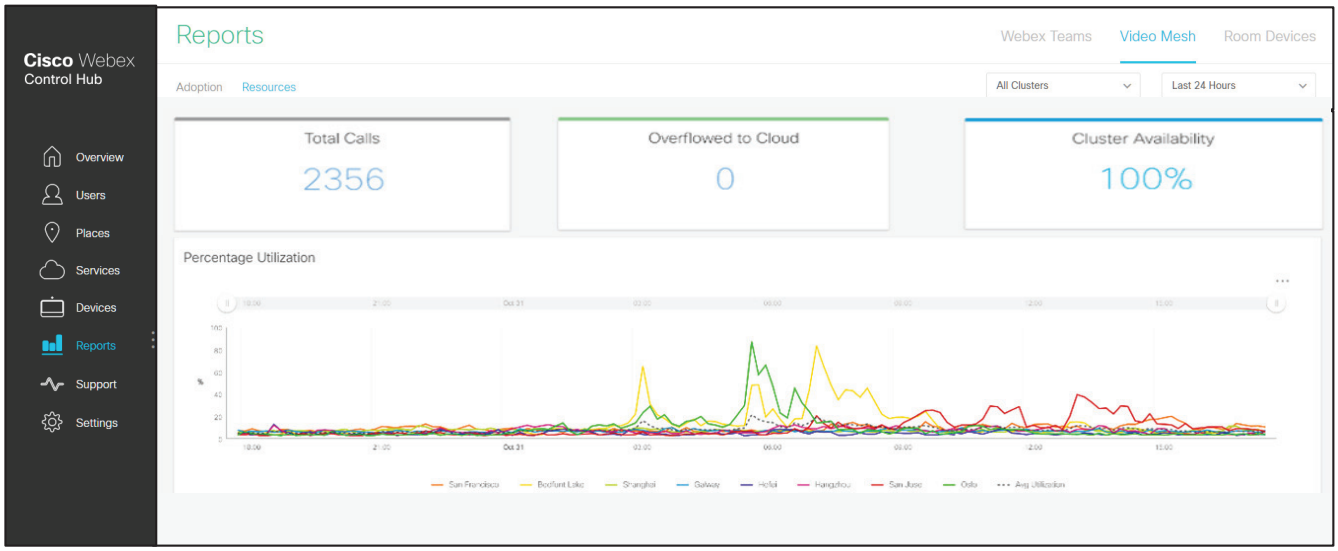
Use the Webex Control Hub to generate various reports that detail usage analytics. Calling reports are very useful when planning a Webex Video Mesh deployment. We recommend monitoring the reports regularly so that you can grow and modify the Webex Video Mesh deployment architecture over time, depending on how your organization utilizes the service.

Reports are available at https://admin.webex.com via the **Video Mesh** tab in the **Reports** section. Reports can be generated for specific Video Mesh clusters or for the entire organization, and data can be displayed based on a specific time period. Utilization reports display graphs based on a selected time

range, and they show (see Figure 4-19):

- Total Calls — Total call legs handled by the organization (cloud and hybrid)
- Overflowed to Cloud — Number of call legs that overflowed to Webex due to the capacity of the Video Mesh clusters being exceeded
- Cluster Availability — Video Mesh cluster uptime based on the specified time range

Figure 4-19 Example Media Utilization Report



Note A call leg represents a single participant attending a Webex meeting. For example, a Webex meeting with five participants contains five call legs.

Planning for the deployment location and sizing of Webex Video Mesh is complex due to the number of variables that make up a meeting, including:

- Number of meetings in a busy hour
- Number of participants per meeting
- Location of participants in a meeting
- Type of endpoints in a meeting
- Time zone overlap

Other variables that should be taken into account include:

- Internet bandwidth availability at a particular site
- WAN bandwidth availability at a particular site

One size or deployment model does not fit all organizations. Regular monitoring of reports can assist with planning and modifying the initial deployment to better serve the needs of the organization.

The report in Figure 4-19 shows 2356 call legs created for Webex meetings by this organization over a 24 hour period, for a specific Video Mesh cluster. All 2356 call legs were hosted on-premises, with zero call legs overflowed to Webex, which indicates that this Video Mesh cluster has enough capacity. As the

Webex deployment grows for this organization, more users and endpoints will likely lead to more meetings and the possibility that the capacity of the Video Mesh cluster will be exceeded. Monitoring the reports regularly will provide feedback to the administrator that can be used to plan for that growth.

We also recommend comparing Webex Media Reports to actual bandwidth usage based on the organization's existing monitoring tools. This will provide an overall view of how the organization's network capacity is affected by Webex meetings. As the Webex deployment grows and overflow to the Webex cloud media services increases, more nodes can be added to the Video Mesh cluster to provide more capacity. Factors such as cost of bandwidth and cost of hardware should be considered when making the decision to add more nodes.

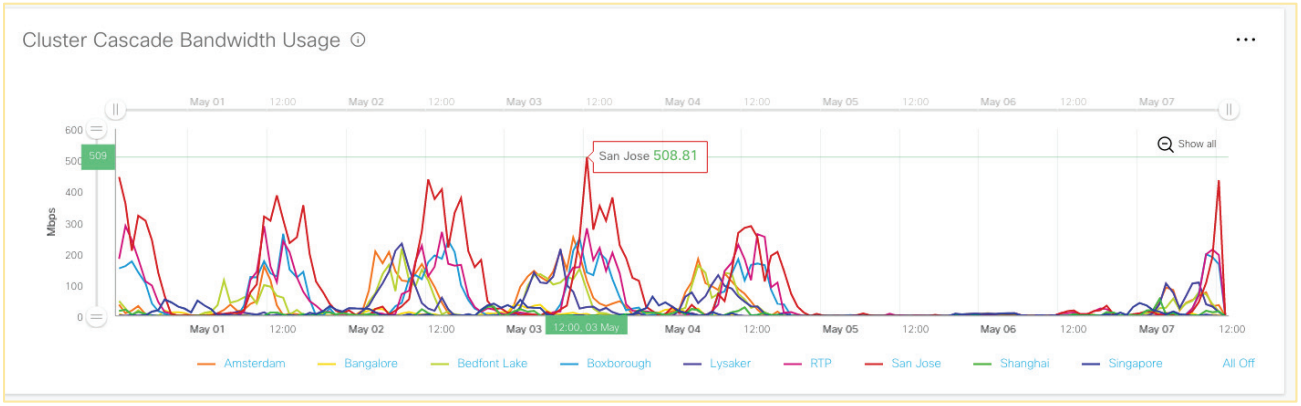
In summary, follow these general guidelines for Webex Video Mesh deployments:

- Begin with a small deployment. Deploy a few Video Mesh Nodes in small clusters.
- Continuously monitor Webex Control Hub reports to understand meeting patterns for the organization.
- Add Video Mesh Nodes to clusters as needed.

Cascade Bandwidth Reports

It is very complex to predict the bandwidth usage of the Video Mesh cascade link due to the number of variables involved. Webex Control Hub provides detailed reporting to monitor cascade link bandwidth usage, as illustrated in Figure 4-20.

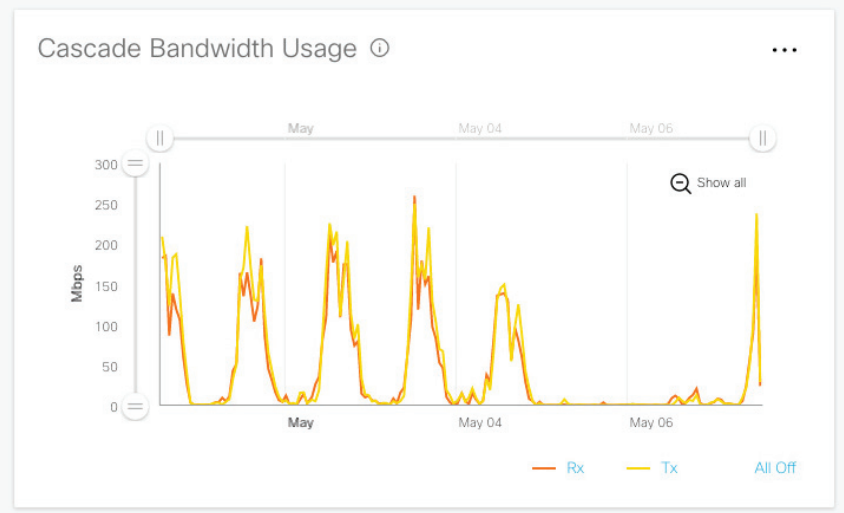
Figure 4-20 Cluster Cascade Link Bandwidth Utilization Report



The report in Figure 4-20 details the bandwidth usage for an organization's Webex Video Mesh cluster cascade link. The organization has 10 clusters configured, with names based on geographical locations. The illustration indicates that the San Jose cluster peaked at 508.81 Mbps of bandwidth for cascading on May 03. This value is cascade transmit (Tx) and receive (Rx) bandwidth. We recommend monitoring this report regularly. Based on the report, decisions can be made regarding whether to add more Video Mesh Node capacity to a cluster, or whether to provision more bandwidth to a site.

The reports can be further refined to detail Tx and Rx bandwidth for a specific cluster, as shown in Figure 4-21.

Figure 4-21 Tx and Rx Bandwidth Detail Report



If the Tx bandwidth is much higher than the Rx bandwidth, it generally means that meetings are localized with fewer remote participants. If the Rx bandwidth is much higher than the Tx bandwidth, it generally means that there are more remote participants attending meetings using that Video Mesh cluster.

Webex Video Mesh Deployment Process

Follow these high-level steps to deploy Webex Video Mesh Nodes:

1. Identify sites where Video Mesh clusters will be deployed.
2. Download and install the Video Mesh Node software.
3. Configure the network settings on each Video Mesh Node.
4. Register the Video Mesh Nodes to the Webex organization.

Once you have identified the sites where the Video Mesh clusters will be deployed, you can begin installation of nodes. Download the Video Mesh Node from the Webex Control Hub, then perform the following steps to deploy the Video Mesh Nodes:

1. Deploy the Video Mesh Node OVA file.
2. Power on the Video Mesh Node and set a new password.
   a. Power on the Video Mesh Node by right-clicking on the virtual machine in the host list, and choose **Power > Power On**.
   b. Open the **Console** to the Video Mesh Node.
   c. Login to the Video Mesh Node.

      Username: **admin**

      Password: **cisco**
   d. On initial login, you will be prompted to change the password. For the current password, type the default password listed above and press **Enter**. Type the new password, then press **Enter** and confirm the new password.
   e. Press **Enter** to proceed past the Unauthorized Access screen.
3. Set the network configuration on the Video Mesh Node.
   a. From the main menu of the Video Mesh Node console, type **2** and press **Enter** to choose **Edit Configuration**.
   b. From the screen that describes the effect of changes to the Video Mesh Node, press **Enter**.
   c. Select **Static** for IP addressing.
   d. On the **Configure Video Mesh Node** screen, configure the network details. The settings that have a * next to their name are mandatory.

      Ensure that the IP address is reachable on the internal network.

      Ensure that the DNS address is resolvable on the internal network.
   e. After completing the network configurations, tab to **Save** and press **Enter**.
   f. At the prompt to reboot, press **Enter**.

4. Register the Video Mesh Node to Webex.
   a. Once this process has begun, it must be completed within 60 minutes. Ensure that any browser popup blockers are disabled or that an exception is applied for **admin.webex.com**.
   b. From the browser, open **admin.webex.com** and login with an administrator account.
   c. Select **Services**.
   d. From the **Video Mesh** card, select **Set up**.
   e. Select **Yes, I'm ready to register my Video Mesh Node** and click **Next**.
   f. Because this is the initial setup of Webex Video Mesh for your organization, there are no clusters configured. Create a cluster by typing a name. We recommend naming clusters based on their geographical location or the name of a data center. In the second field, enter the **IP address** of the installed Video Mesh Node. Click **Next**.
   g. On the next screen, click **Go To Node**. A new browser opens, connecting to the Video Mesh Node. You can accept the certificate warnings.
   h. Select **Allow Access to the Video Mesh Node** and click **Continue**. The Video Mesh Node will perform a number of connectivity tests for Webex services.
   i. If tests are successful, go to the browser tab for **Cisco Webex Control Hub**. The Video Mesh card should show a status of Operational, indicating that node registration is now complete.

      More nodes can be added to the configured cluster by clicking **Resources** from the Video Mesh card and selecting the existing cluster from the **Register Video Mesh Node** window.

      More clusters can be added to the deployment by specifying a new cluster name from the **Register Video Mesh Node** window.

Cisco Webex Hybrid Call Service

Revised: May 31, 2019

Cisco Webex Hybrid Call Service provides seamlessly connection between Cisco Webex and Cisco Unified Communications Manager (Unified CM) as the on-premises enterprise call control or Cisco Hosted Collaboration Solution (HCS) as the hosted enterprise call control.

Note Please be aware that the Webex Hybrid Call Service architecture discussed in this document is currently going through a transitional phase. To better understand the future changes and how they will impact your deployment of the Webex Hybrid Services architecture, we recommend that you contact your Cisco account team before deploying the architecture described in this document.

Overview

Webex Hybrid Call Service is based on Call Connector. This service enables Webex Teams users to make and receive calls on their Webex Room Device or Webex Teams application using the same dialing procedures as with endpoints registered with Cisco Unified CM or Hosted Collaboration Solution (HCS).

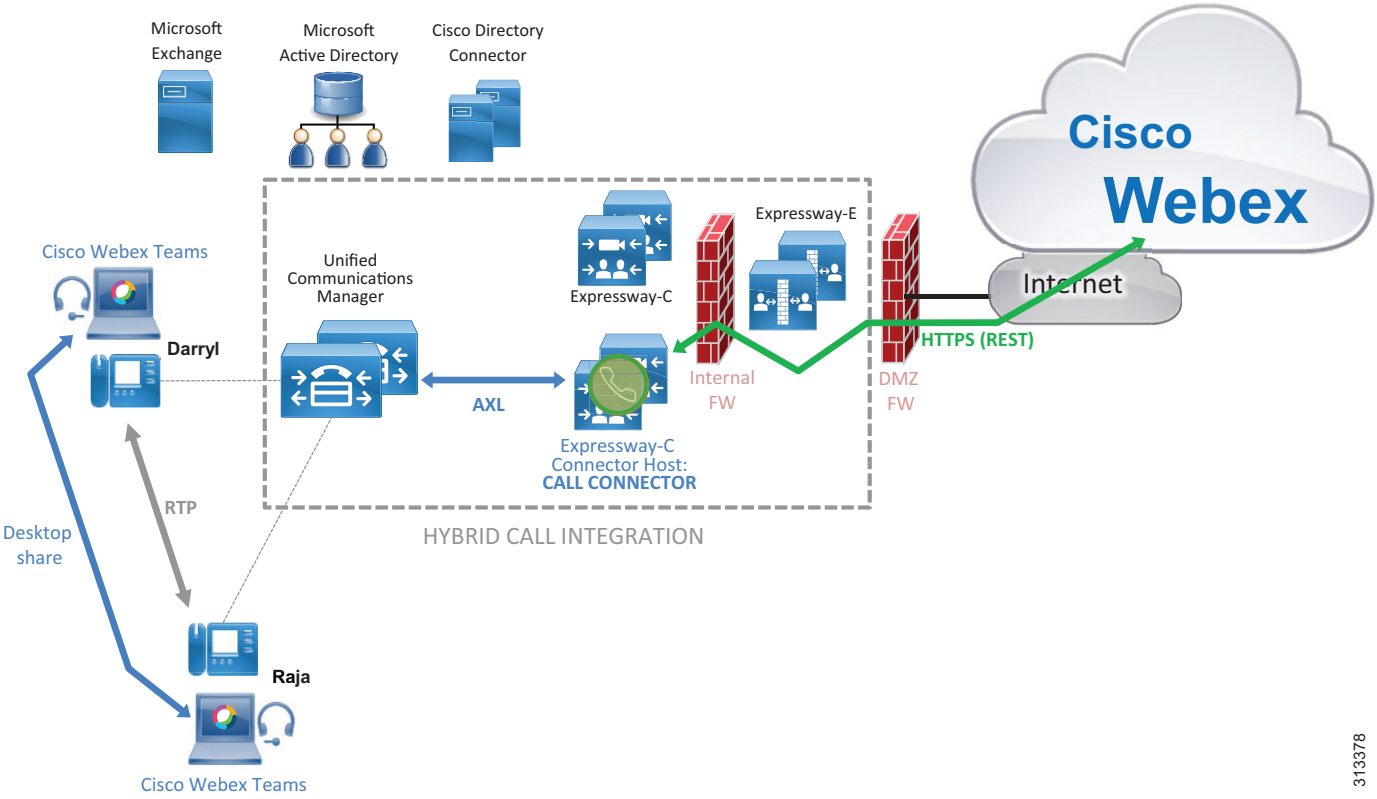
Core Components

- Cisco Expressway-C runs the Call Connector.
- Cisco Expressway-C and Expressway-E provide firewall traversal for SIP signaling and media.
- Cisco Unified Communications Manager (Unified CM) or Hosted Collaboration Solution (HCS) provides call control.

Recommended Deployment

The Hybrid Call Connector runs on the Cisco Expressway-C host and connects on one side to Unified CM via Administrative XML (AXL). This provides Call Connector with access to Unified CM provisioning. On the other side, the Call Connector uses HTTPS to communicate with Webex. (See Figure 5-1.) This connection traverses through the customer's Internet edge firewall and does not use the Expressway-E and Expressway-C firewall traversal setup.

Figure 5-1 Call Connector Provides Communication Between Cisco Unified CM and Cisco Webex for User and Device Provisioning



When a user in Webex is enabled for Hybrid Call Service, the Call Connector uses the AXL interface to find devices associated with that user on Unified CM and adds specific configuration, such as a Spark Remote Device (if configured for automatic Spark Remote Device provisioning) and the associated remote destination, called the *Associated Identity*. Call Connector does not participate in call setup or tear-down.

If a user has an endpoint registered to Cisco Unified CM and also has a Webex Teams application, both the endpoint and the Webex Teams application will receive calls regardless of whether the call is initiated by another Webex Teams application, by a Unified CM registered device, or by a Unified CM associated IP or PSTN gateway. Call Service Connect not only enables dual ringing on Webex Teams applications, including Webex Room Devices and Cisco Unified CM endpoints, but also allows Webex Teams users to place calls using enterprise dialing habits from their Webex Teams applications.

In order to achieve this, a SIP connection must be set up between Webex and Expressway-E using standard business-to-business technologies and Transport Layer Security (TLS) with mutual authentication. For this reason, Expressway-E must use a certificate signed by a Certification Authority trusted by Webex. For a list of trusted Certification Authorities, refer to the latest version of the *Deployment Guide for Cisco Webex Hybrid Call Service*, available at

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

Key Benefits

Webex Hybrid Call Service provides the following key benefits:

- Automatic provisioning of meetings
- Firewall traversal architecture for signaling and media, which increases security by minimizing the need to open outbound ports in the internal firewall
- Secure signaling and media encryption based on public certificates with mutual authentication

Architecture

Call Service Connect enables dual ringing for Webex Teams and Cisco Unified CM devices associated with the same user. In addition, it keeps the user experience consistent so that the user of Webex Teams has the same dialing habits, calling ID, and unified call history as any other user on Cisco Unified CM.

In order to achieve all of this, the Cisco Unified CM administrator must configure a Cisco Spark Remote Device for every user's primary extension. The administrator can configure the Call Connector to create the Spark Remote Device automatically, with the limitation that parameters such as device pool, calling search space, location, and reroute calling search space will be shared between all the Spark Remote Devices.

Webex Teams SIP Address and Enterprise URI

Once the Cisco Spark Remote Device is configured, Call Connector will automatically configure associated identities (formerly called remote destinations) associated with the Spark Remote Device on Cisco Unified Communications Manager in order to allow simultaneous ring functionality between Webex Teams applications and Unified CM devices.

As an example, if the user bob@ent-pa.com is provisioned for Call Service Connect, the Call Connector will add an associated identity to the Spark Remote Device of this user via the Unified CM AXL API. The associated identity will be in the form:

<userID>@*<subdomain>***.call.webex.com**

For example: bob@ent-pa.call.webex.com (see Figure 5-2)

Where *<userID>* is the attribute uniquely identifying the user in the corporate directory domain, and *<subdomain>* is the unique subdomain configured for the organization in the Webex Control Hub. In this example, the corporate domain is **ent-pa.com** and the subdomain configured by the administrator is **ent-pa.** Webex asserts that the subdomain is unique or else prompts the administrator to create a new one if the subdomain is already in use.

When a user is provisioned for Call Service Connect, Webex via the Call Connector learns the user's enterprise URI from the Directory URI defined for the user in Unified CM. This information is pushed to Webex.

Each user has two addresses:

- Enterprise URI — It matches the Directory URI on Cisco Unified CM (bob@ent-pa.com in our example). This address uniquely identifies the user in Unified CM.
- Webex Teams SIP address — This address (set to bob@ent-pa.call.webex.com in our example) identifies the user on Webex. The subdomain ent-pa.call.webex.com is a publicly reachable subdomain of the domain call.webex.com managed by Webex.

When Alice calls Bob using her Cisco Unified CM device (step 1 in Figure 5-2), Unified CM forks the call to the Spark Remote Device that shares Bob's directory number with Bob's device, as shown by step 2 in Figure 5-2. The associated identity is triggered, and the call is sent to bob@ent-pa.call.webex.com through a SIP route pattern to Expressway-C. Expressway-C is configured to send any URI of the form *<user>*@ent-pa.call.webex.com to Expressway-E, and Expressway-E in turn sends it to the DNS zone (step 3 in Figure 5-2).

Expressway-E queries the public DNS for SRV resolution for the record _sips._tcp.callservice.webex.com even if the domain portion of the SIP URI is ent-pa.call.webex.com, because the DNS Zone on Expressway is configured to use callservice.webex.com instead of ent-pa.call.webex.com. This is done through the **Modify DNS Request** and the **Domain to search for** settings in the DNS Zone, and the call is sent to Webex. As a consequence, both Bob's Unified CM endpoint and his Webex Teams application receive the call, and Bob can decide which of the two clients he will use.

Figure 5-2 shows the call signaling flow for this example.

Figure 5-2 Call Signaling Flow for Call Service Connect

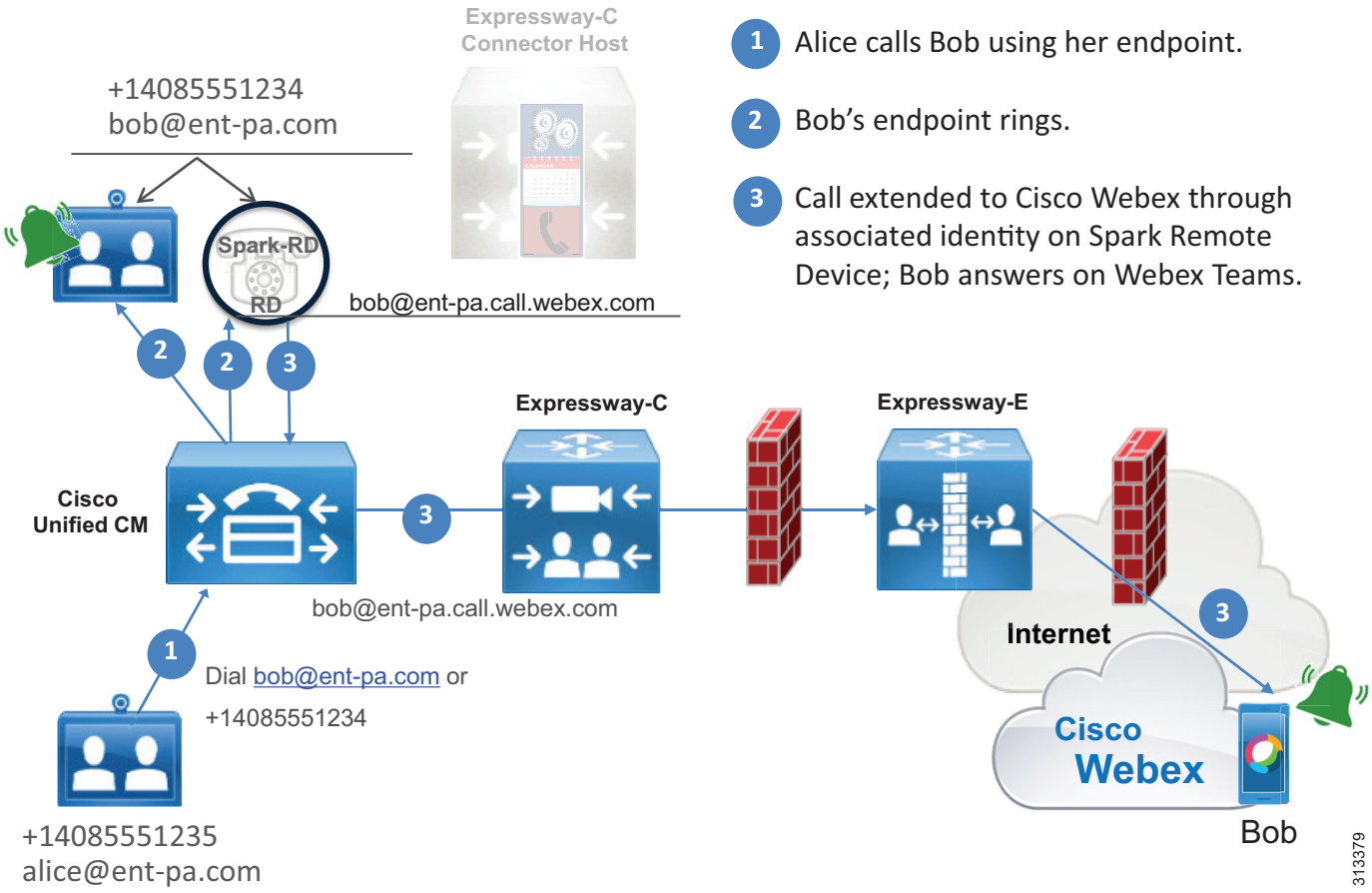


Figure 5-2 shows the following actions:

1. Alice calls Bob using her Unified CM registered device.
2. The call is sent to Bob's directory number, shared between Bob's Unified CM registered device and his Cisco Spark Remote Device. Bob's Unified CM device starts ringing.
3. The call is extended to Webex through the associated identity included in the Cisco Spark Remote Device.
4. Bob's Webex Teams application starts ringing. Bob can answer the call using the Webex Teams application or his Unified CM device.

When Alice on her Webex Teams application calls Bob, Webex detects that Bob is enabled for Call Service Connect with an enterprise URI set to bob@ent-pa.com, and it sends the call to both Bob's Webex Teams application and the Expressway-E cluster located through the SRV record _sips._tcp.ent-pa.com.

If this record is already used for business-to-business communications, we recommend specifying a subdomain of the corporate domain as the SIP destination in the Webex Control Hub, and consequently a public DNS SRV record, as follows:

```
Service and protocol: _sips._tcp.mtls.ent-pa.com
Priority: 1
Weight: 10
Port number: 5062
Target: us-expe1.ent-pa.com
```

The SIP destination configured by the corporate administrator in the Webex Control Hub determines where Webex sends Call Service Connect call legs for this organization.

Expressway-E and Expressway-C are configured to route the call internally, as they would with any business-to-business call.

Note Webex populates the SIP request with a Route Header, which takes precedence over the Request URI. In all cases, routing on Expressway-C and Expressway-E is not performed according to the Request URI (bob@ent-pa.com) but according to the Route Header instead. You must consider this when creating the search rules on Cisco Expressway. Because this is especially important in deployments of multiple Cisco Unified CM clusters, this information is covered in the section on Deployment Considerations for Multiple Unified CM Clusters, although it applies to a single cluster scenario as well.

The call reaches Cisco Unified CM and is anchored on Alice's Cisco Spark Remote Device based on the caller ID of the incoming SIP call leg, which matches the associated identity provisioned on Alice's Cisco Spark Remote Device. Call anchoring is a mobility feature that is used to preserve the calling ID and also to apply a user-based class of service based on the calling search space (CSS) configured on the Cisco Spark Remote Device where the call is anchored. For more details, see the section on Caller ID and Class of Service.

After anchoring, the call is sent to Bob's DN on which Bob's directory URI is configured as an alias. This is shared between Bob's Unified CM devices and his Cisco Spark Remote Device. As a consequence, the incoming call is presented on Bob's Unified CM devices and at the same time a forked call leg is created to Bob's cloud SIP URI, which is configured as an associated identity on Bob's Cisco Spark Remote Device, as shown in step 4 of Figure 5-3.

Figure 5-3 Call Flow to Bob's Cisco Spark Remote Device

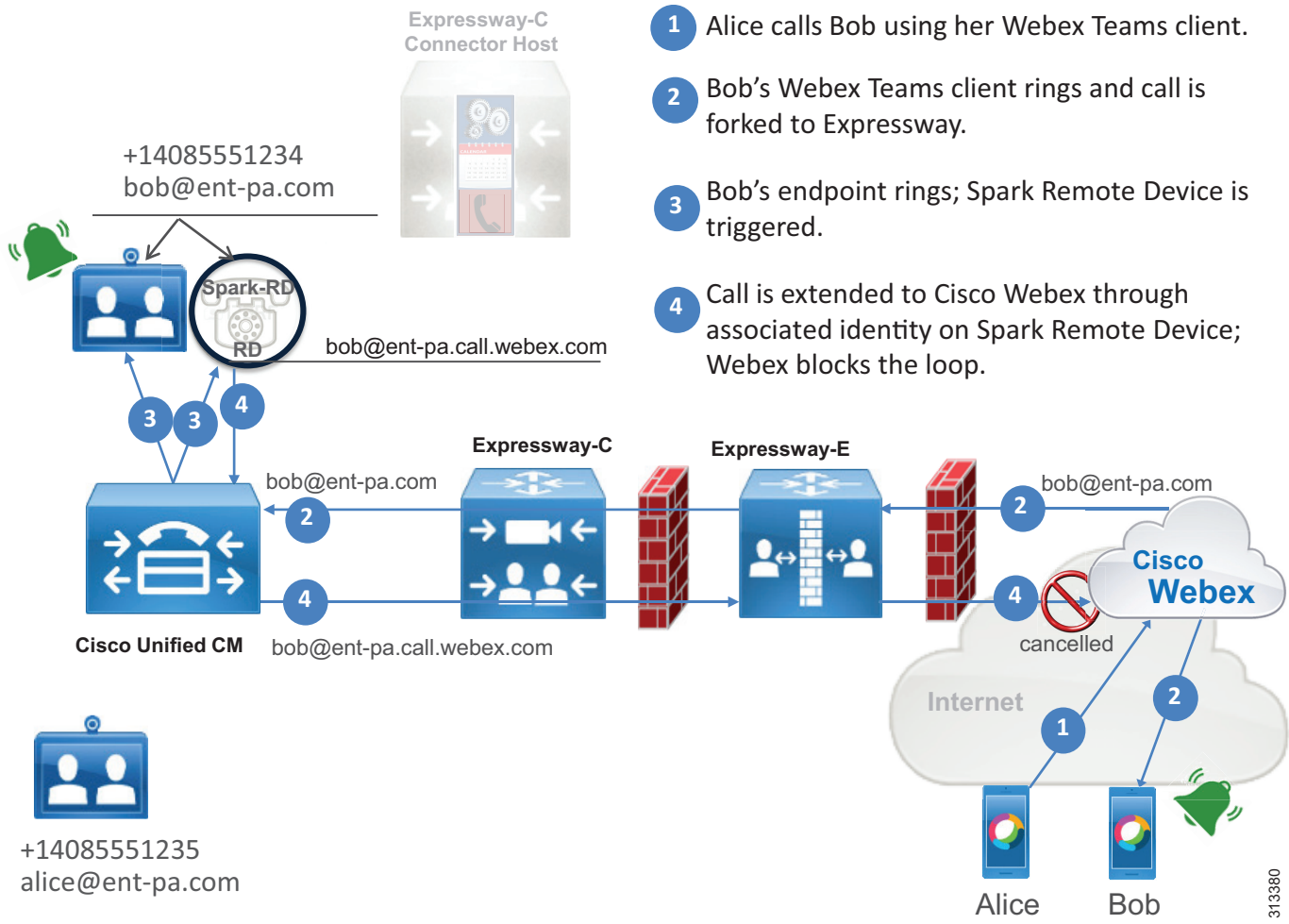


Figure 5-3 shows the following actions:

1. Alice calls Bob using her Webex Teams application.
2. Bob is notified of an incoming call from Alice on his Webex Teams application. The call is extended to Expressway-E, Expressway-C, and Unified CM.
3. The call is sent to Bob's shared line, appearing on both his Unified CM registered device and his Cisco Spark Remote Device. Bob has the option to answer the call from either his Unified CM device or his Webex Teams application.
4. The associated identity on the Cisco Spark Remote Device extends the call to Webex through Expressway-C and Expressway-E. Webex detects that it is a looped call and disconnects it through the mechanism explained in the section on Loop Detection and Avoidance.

Loop Detection and Avoidance

Before forking the call to the calling user's enterprise (step 2 in Figure 5-3), Webex populates the SIP request with a Contact Header parameter **call-type=squared**. When Webex receives a call from the corporate network (step 4 in Figure 5-3) that contains the Contact Header set to **call-type=squared**, Webex detects that this is a looped call and does not send it back to the Webex Teams application. Therefore, Cisco Expressway must be configured to allow Contact Header pass-through on Expressway-C and Expressway-E.

TLS with Mutual Authentication

SIP signaling between Webex and the enterprise network uses TLS with Mutual Authentication (MTLS). MTLS is part of the TLS specification, and like any TLS architecture it is client-server based, with the client as the initiator of the request. In the case of the SIP connection from Webex to the enterprise, Webex acts as the client for this connection and Expressway-E is the server side. With MTLS, both Webex and Expressway-E authenticate each other based on certificates. Specifically, on the DNS zone on Expressway-E to be used for calls from Webex, a **TLS verify subject name** is configured, and this needs to match the Common Name (CN) or one Subject Alternative Names (SANs) of the certificate presented by Webex to Expressway-E during TLS handshake.

When a Webex Teams call is received by Expressway-E (server-side in TLS handshake), Expressway-E requests the TLS client certificate that is the Webex certificate. If the certificate is valid and one of its SANs matches what has been configured in the **TLS verify subject name**, the call is treated as authenticated. Successful authentication also requires that trust is established with the certificate authority (CA) that signed this certificate.

If authentication is not successful, this means that the certificate validation has failed. The call will thus enter into the Default Zone and will be routed according to the search rules provided for business-to-business scenarios, if business-to-business is configured on Expressway-E.

Media Encryption

Media is encrypted with Secure Real-time Transport Protocol (SRTP) between Cisco Webex and Cisco Expressway. Depending on the configuration, different scenarios can be achieved:

- End-to-end encryption

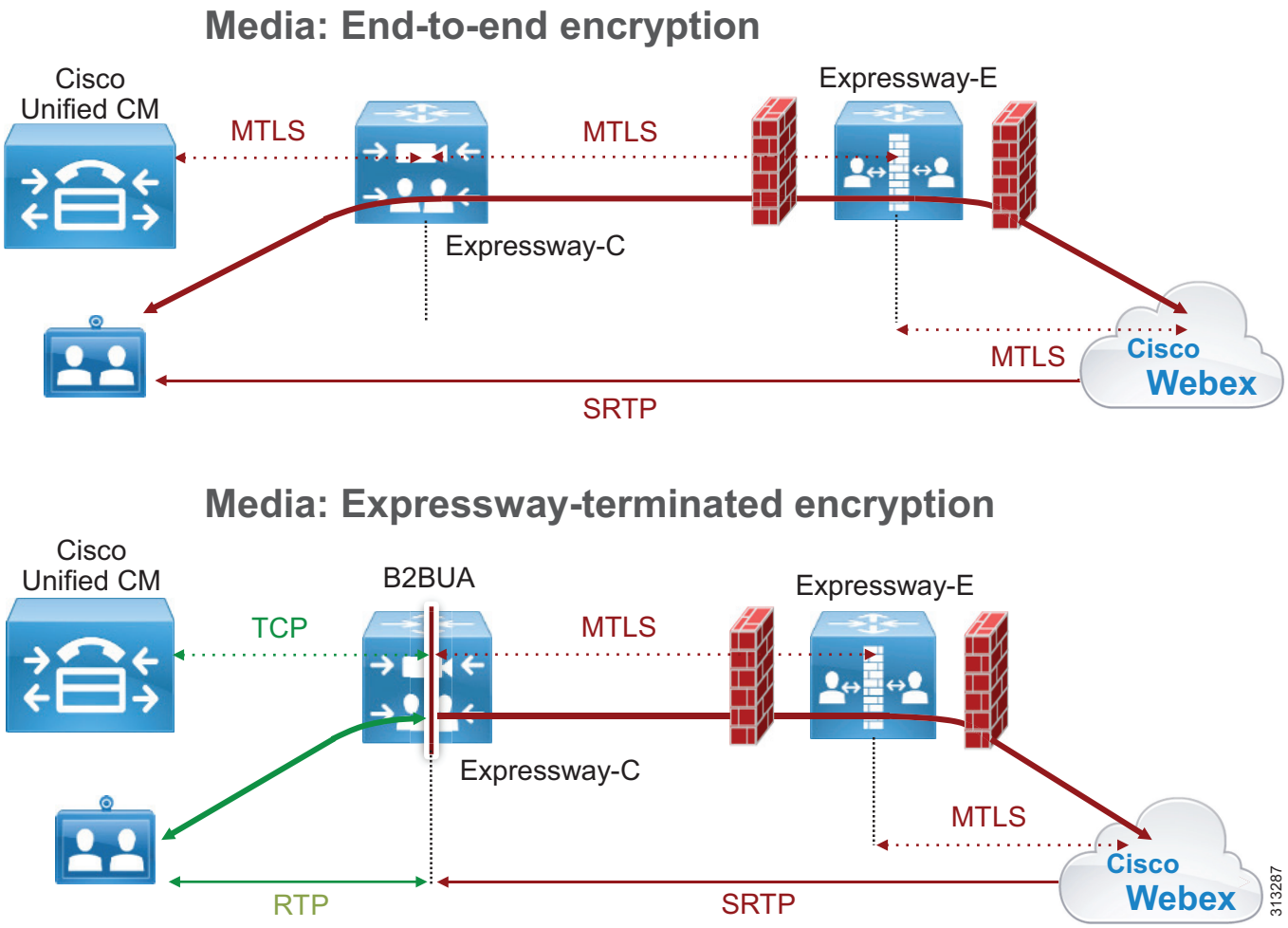
  This requires Cisco Unified CM to be in mixed mode and the endpoints to be provisioned for encryption.

- Expressway-terminated encryption

  If Cisco Unified CM is not in mixed mode and uses non-encrypted RTP media traffic to Expressway-C, then Expressway-C terminates the RTP connection with the Unified CM endpoint and creates another call leg using SRTP to Webex. Any time Expressway performs RTP-to-SRTP conversion, it engages a back-to-back user agent (B2BUA). If Expressway performs RTP-to-SRTP conversion, we recommend enabling it on Expressway-C instead of Expressway-E so that the traffic in the DMZ will be encrypted.

Figure 5-4 illustrates these two encryption options.

Figure 5-4 Media Encryption Options



Call Service Connect for Webex Room Devices

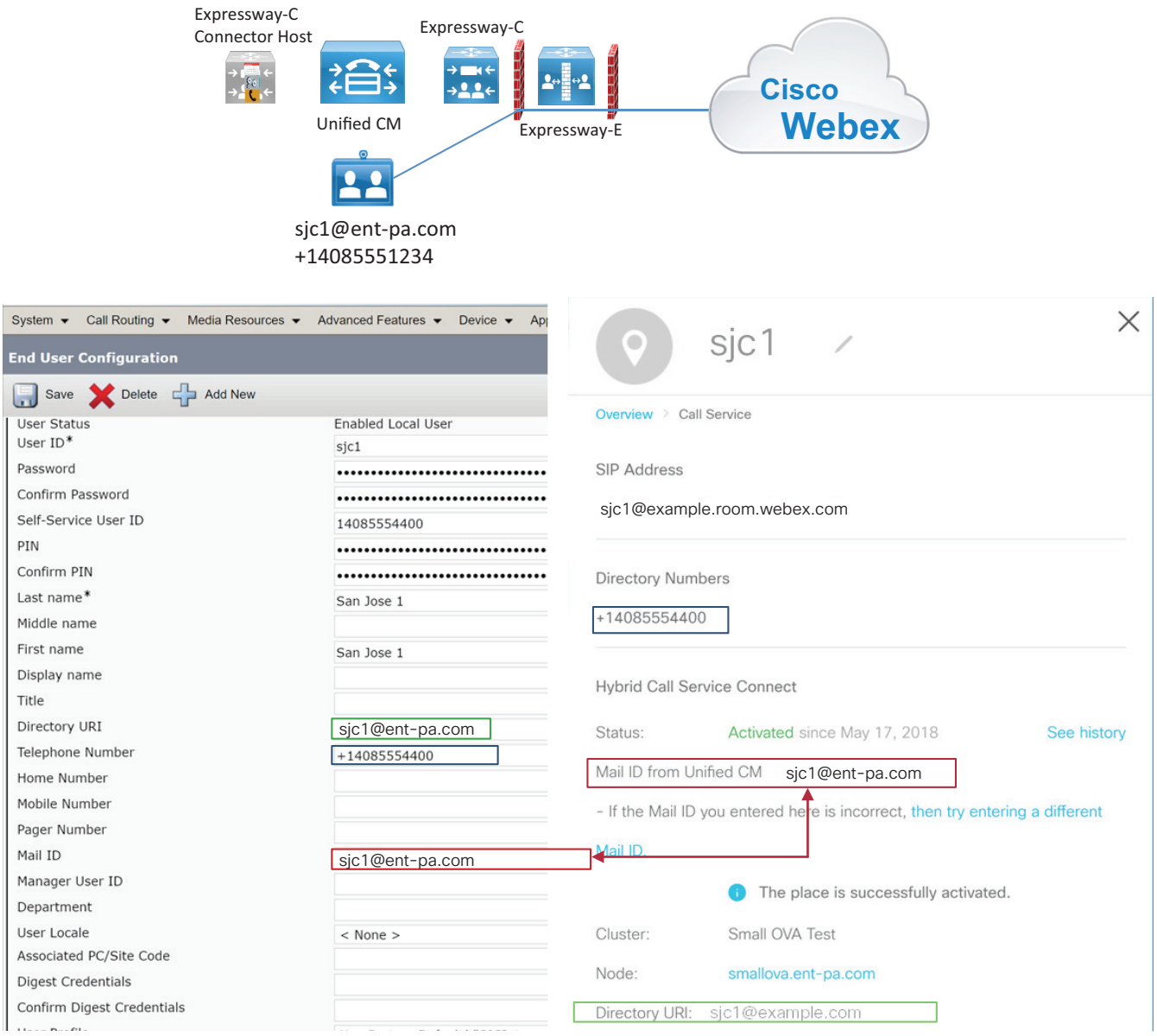
Cisco Webex Room Devices can be enabled for Call Service Connect. The result is similar to Webex Teams users enabled for Call Service Connect. The room device will have a directory number on Cisco Unified CM and a +E.164 number associated with the PSTN, and it will be able to dial out to the PSTN and to receive calls from the PSTN. In addition it will have all associated benefits of Call Service Connect, including the same dialing habits and same calling restrictions that are configured on Cisco Unified CM.

The room devices are provisioned in Webex Control Hub as "Places," and as such they do not require any user association in Webex Control Hub. However, a local user must be created on Cisco Unified CM for every Place configured on Webex Control Hub. That local user does not have to be provisioned on the LDAP directory Cisco Unified CM is synchronized with, but it must have a unique mail ID, a +E.164 telephone number, and a directory URI. Webex associates every identity to a unique email address, be it a user or a place, but the email address is not required to have an associated Exchange inbox because Webex sends emails (if configured) to Users, not to Places.

The associated Spark Remote Device will be configured by Expressway-C Connector Host if it has been configured for automatic provisioning, or it must be configured manually if automatic provisioning is disabled. In this case, only the associated identity will be configured by the Connector Host.

Figure 5-5 shows the fields that must be configured on Cisco Unified CM and on the Webex Control Hub.

Figure 5-5 Required Configuration Fields for Webex Room Devices



Deployment Overview

This section describes the high-level steps required for deploying Webex Hybrid Call Service.

Expressway-C and Expressway-E on a Shared Deployment

If calls generated by Call Service Connect are co-resident with business-to-business calls, it is important to allow PSTN access to Webex Teams users while blocking business-to-business users from unauthorized access of PSTN and other internal-only services.

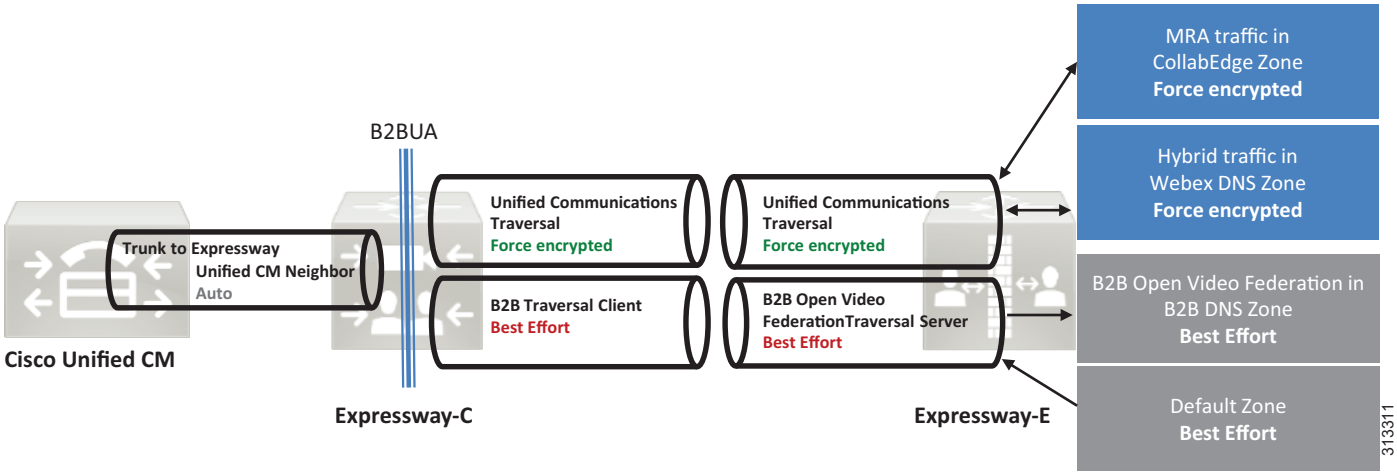
Standard business-to-business calls from other companies enter the Default Zone because these connections, even if they are configured for MTLS, will not present a certificate matching the TLS verify name configured on the Webex DNS zone. Therefore, we recommend configuring the Default Zone as non-authenticated. Call Processing Language (CPL) rules controlling access to the corporate network will thus be applied only to non-authenticated traffic, and Call Service Connect calls will bypass the control check of non-authenticated traffic on Expressway and will be routed to the enterprise Unified CM for call anchoring.

For an explanation on how authentication works with CPL rules, refer to the CPL information in the latest version of the *Cisco Collaboration System Solution Reference Network Designs (SRND)* guide, available at http://www.cisco.com/go/srnd.

It is possible to use a single traversal zone between Expressway-E and Expressway-C for business-to-business calls, Webex Hybrid Call Service calls, and mobile and remote access. However, separating traversal zones by traffic type will optimize consumption of resources on Expressway. As an example, using the same traversal zone for mobile and remote access (MRA) traffic together with Webex traffic preserves resources because they share the same encryption setting (**Force encrypted**), and this optimizes the engagement of the back-to-back user agent (B2BUA). However, the business-to-business traffic encryption policy might be different. A dedicated traversal zone for business-to-business traffic would prevent multiple engagements of the B2BUA on both Expressway-C and Expressway-E.

We recommend using the MRA traversal zone (called **Unified Communications** traversal zone on Expressway) for Webex Hybrid Services traffic as well, while using a separate traversal zone for business-to-business (B2B) traffic, as shown in Figure 5-6.

Figure 5-6 Separate Traversal Zone for Business-to-Business (B2B) Traffic



Traversal zones do not require any inbound port to be opened on a DMZ firewall; but if the corporate security policies block outbound access by default, then an outbound port has to be opened in the firewall for every new traversal zone. In this rare case, it is possible to use the Unified Communications traversal zone for all traffic types. Although supported, this deployment has some limitations, and it always engages the B2BUA on Expressway-E unless all business-to-business communications use encryption.

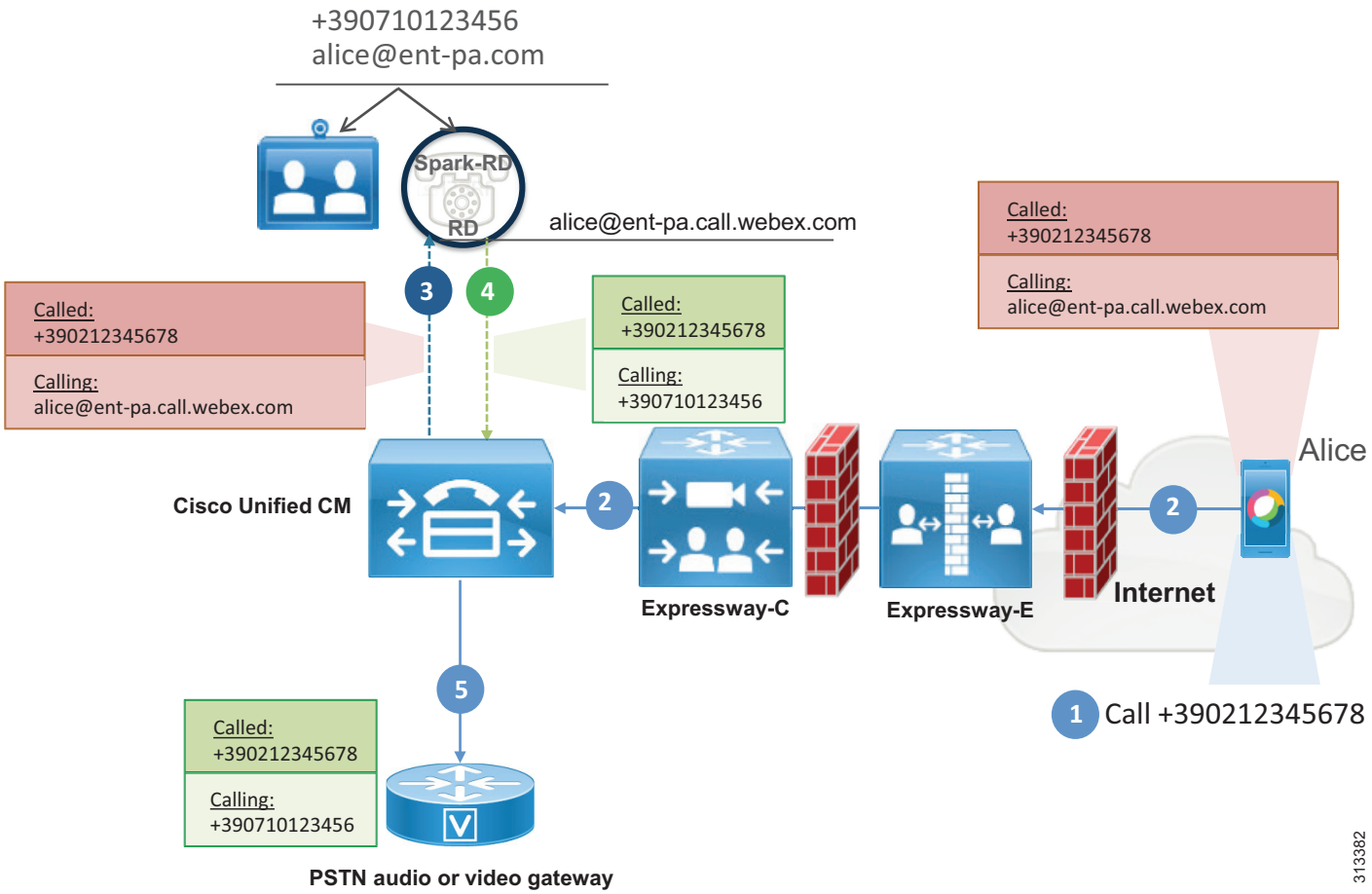
Caller ID and Class of Service

When a Webex Teams user calls a Cisco Unified CM endpoint or service, or when the user dials out to the PSTN, the desired behavior is to present the calling user's Unified CM directory URI or +E.164 number as the caller ID.

When the call leaves Webex, the caller ID is set to the Webex Teams SIP address of the calling user, such as alice@ent-pa.call.webex.com. Because this address matches the associated identity configured in the Cisco Spark Remote Device associated with the calling user, the call is anchored on the calling user's Cisco Spark Remote Device and then routed as if it originated from this device. This also sets the caller ID for the outgoing call leg to the enterprise identity (directory number and directory URI) of the calling user.

In the example in Figure 5-7, Alice dials a PSTN number using Webex Teams. When a call is placed from the Webex Teams application using the Calls tab, any number (such as a +E.164 number) can be entered. In this case the Request URI of the call leg forked to Expressway to route the call to the calling user's Unified CM is set to *<number>@<CFQDN>*, where CFQDN is the Cluster Fully Qualified Domain Name of the Cisco Unified CM cluster. The CFQDN of every user enabled for Call Service Connect is pushed to Webex by the Call Connector during the initial provisioning phase and is derived from the CFQDN enterprise parameter of the Unified CM cluster where the user is provisioned. Because the CFQDN enterprise parameter allows for provisioning multiple values in a space-separated list, the Call Connector always picks the first value and pushes that value to Webex. After the call is anchored on the calling users's Spark Remote Device, it follows the standard routing behavior of Unified CM and the call is routed according to the numeric call routing logic of Unified CM because the host portion (right hand side) of the Request URI matches a CFQDN configured on Unified CM. On the initial call leg to the enterprise, the caller ID is set to Alice's Webex Teams SIP address alice@ent-pa.call.webex.com. Because the Webex Teams SIP address matches the associated identity set in the Cisco Spark Remote Device, this call is identified as belonging to Alice on Cisco Unified CM and is forwarded to the final destination as if it originated from Alice's directory number. Therefore, Alice's caller ID and Alice's calling search space as set in Unified CM will be used instead. This is shown in Figure 5-7, where steps 3 and 4 indicate logical processes inside Cisco Unified CM and not call flows.

Figure 5-7 Call Anchoring and Caller ID



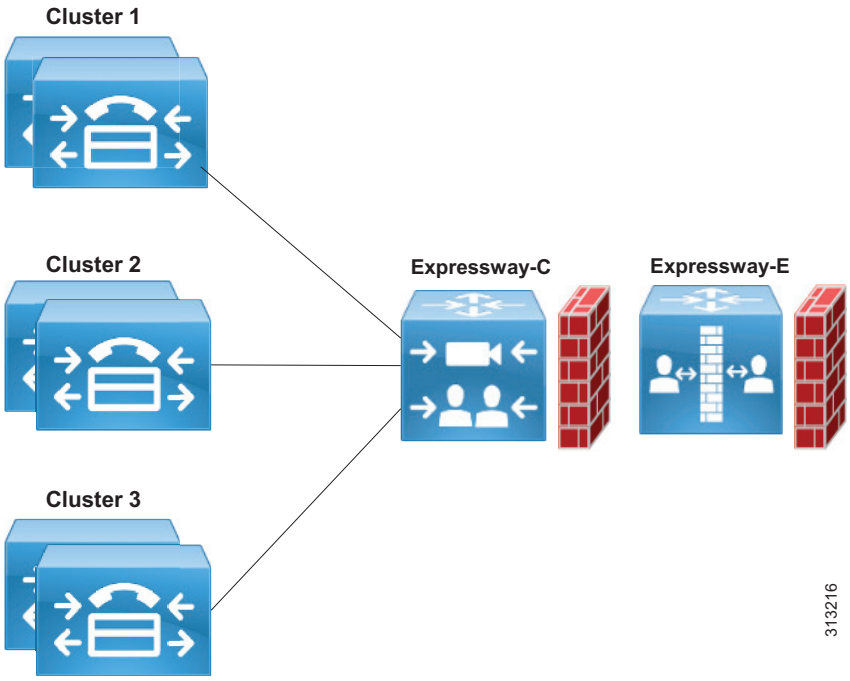
Call anchoring based on a successful match between caller ID and remote destination is a mobility feature and happens independently from the dialed destination.

Note Webex has no knowledge of the enterprise dial plan. For this reason, if Alice cannot call Bob using her endpoint on the enterprise network due to a restricted class of service, Alice may still call Bob if both use Webex Teams. If Alice uses Webex Teams, Cisco Unified CM will prevent the call from reaching Bob's endpoint, but Bob's Webex Teams application will ring.

Deployment Considerations for Multiple Unified CM Clusters

Webex Hybrid Call Service supports multiple Cisco Unified Communications Manger clusters. In this case, Expressway-C can be associated to every cluster, as shown in Figure 5-8.

Figure 5-8 Expressway-C Supporting Multiple Unified CM Clusters



When multiple clusters are deployed, the incoming call from Webex has to be routed to the calling user's Cisco Unified CM cluster for call anchoring and not to the Unified CM of the called user, in order to associate the call with the calling user's Spark Remote Device and correctly set the calling user's enterprise caller ID and apply the calling user's class of service. This is known as home cluster-based routing. With home cluster-based routing, the call is always anchored to the Cisco Unified CM of the calling user.

With home cluster-based routing, when Webex sends a call to the Expressway-E, it populates both the SIP Request URI and the Route Header. Even though the following considerations and examples apply to multiple Cisco Unified CM clusters, the use of the Route Header is a general concept and applies also to single-cluster deployments. Thus, Expressway search rules always have to match on Route Header and not Request URI values.

When both a Request URI and a Route Header are present in a SIP INVITE, the Route Header takes precedence in the routing processes if routing based on the route header is enabled on the zone that the call ingresses through on Expressway. As an example, when Alice on the US cluster dials Bob in the EMEA cluster using her Webex Teams application, Expressway-E receives this INVITE:

```
INVITE sip:bob@ent-pa.com SIP/2.0
Via: SIP/2.0/TLS 10.10.10.10:5062;branch=z9hG4bK-393139-4880f133ef84798fb3625da14a87ad32
Call-ID: 87c778d0a17c9a3a93ef90ff530fda50@30.30.30.30
CSeq: 1 INVITE
Contact: "l2sip" <sip:l2sip@10.10.10.10:5062;transport=tls>;call-type=squared
From: "Alice" <sip:alice@ent-pa.call.webex.com>;tag=1381736467
To: <sip:bob@ent-pa.com>
Max-Forwards: 70
Route: <sip:l2sip@20.20.20.20:5062;transport=tls;lr>,<sip:us-cm-pub.ent-pa.com;lr>
```

Expressway-E receives this call on the Webex DNS Zone enabled for TLS with mutual authentication. The Webex DNS Zone, Webex traversal client, and traversal server zone must be enabled for route header support or else the call will be dropped.

Expressway-E considers the presence of route headers when routing the call; and since the route header takes precedence over the Request URI, the routing process will analyze us-cm-pub.ent-pa.com instead of alice@ent-pa.com in our example. Search rules on Expressway-E will thus match us-cm-pub.ent-pa.com and route the call to the next hop, Expressway-C first and Cisco Unified CM after.

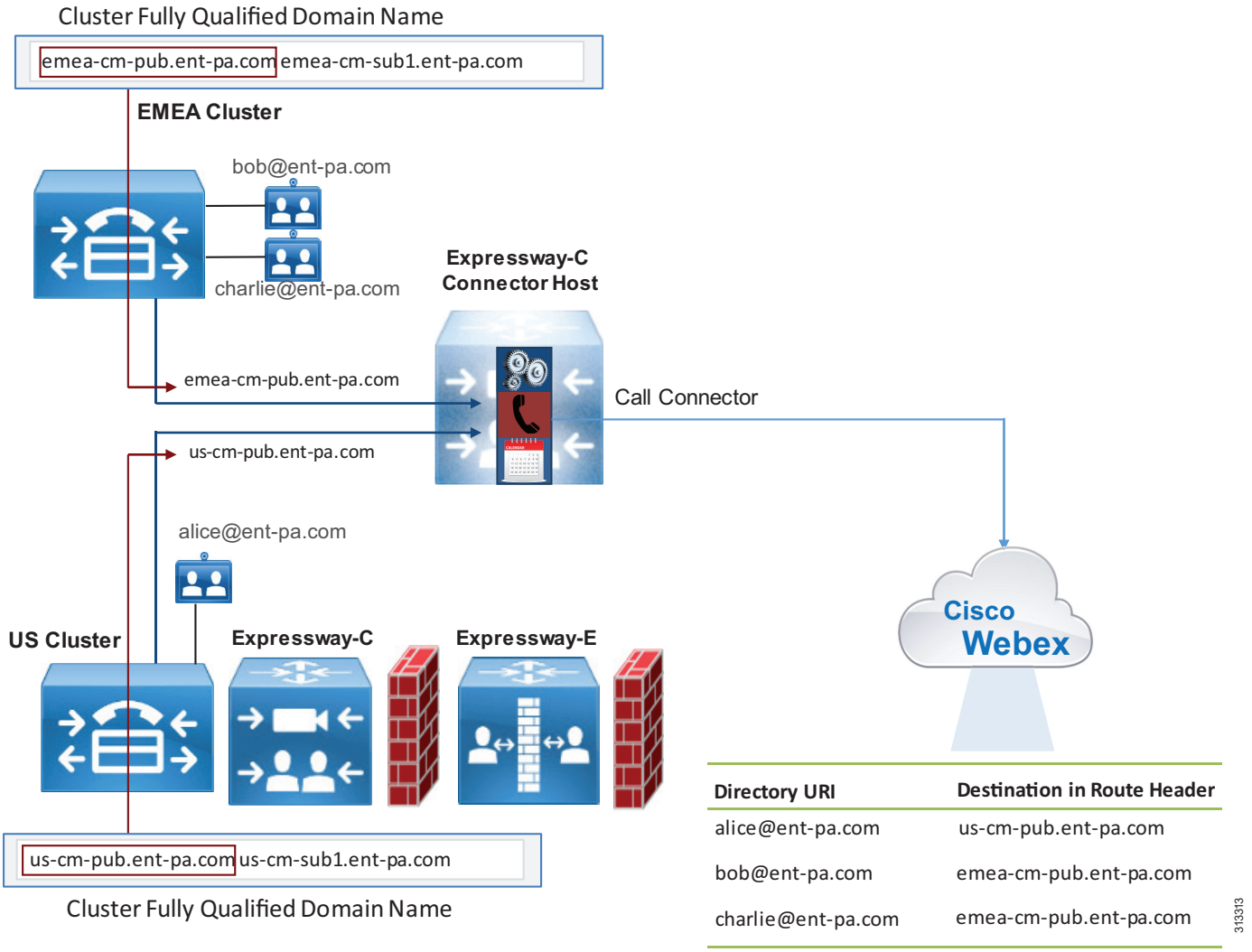
When Charlie on the EMEA cluster calls Bob, the INVITE looks different:

```
INVITE sip:bob@ent-pa.com SIP/2.0
Via: SIP/2.0/TLS 10.10.10.10:5062;branch=z9hG4bK-393139-4880f133ef84798fb3625da14a87ad32
Call-ID: 87c778d0a17c9a3a93ef90ff530fda50@30.30.30.30
CSeq: 1 INVITE
Contact: "l2sip" <sip:l2sip@10.10.10.10:5062;transport=tls>;call-type=squared
From: "Charlie" <sip:charlie@ent-pa.call.webex.com>;tag=1381736467
To: <sip:bob@ent-pa.com>
Max-Forwards: 70
Route: <sip:l2sip@20.20.20.20:5062;transport=tls;lr>,<sip:emea-cm-pub.ent-pa.com;lr>
```

This time Expressway routes the call based on the destination emea-cm-pub.ent-pa.com, and thus the INVITE is sent to the EMEA Unified CM through the Route Header, where Charlie's devices are registered.

Webex populates the Route Header based on the information received by the Call Connector and specifically taken from the Cisco Unified CM Cluster Fully Qualified Domain Name (CFQDN) enterprise parameter. Specifically, if multiple values are present in the CFQDN enterprise parameter, then the first value is considered. Using this mechanism, Webex creates associations between users and their respective CFQDNs. When a call is sent from Webex, the dialed destination (URI or numeric destination) of the call is used to populate the INVITE Request URI, and the home cluster of the calling user populates the Route Header, as illustrated in Figure 5-9.

Figure 5-9 Cluster Fully Qualified Domain Name (CFQDN)



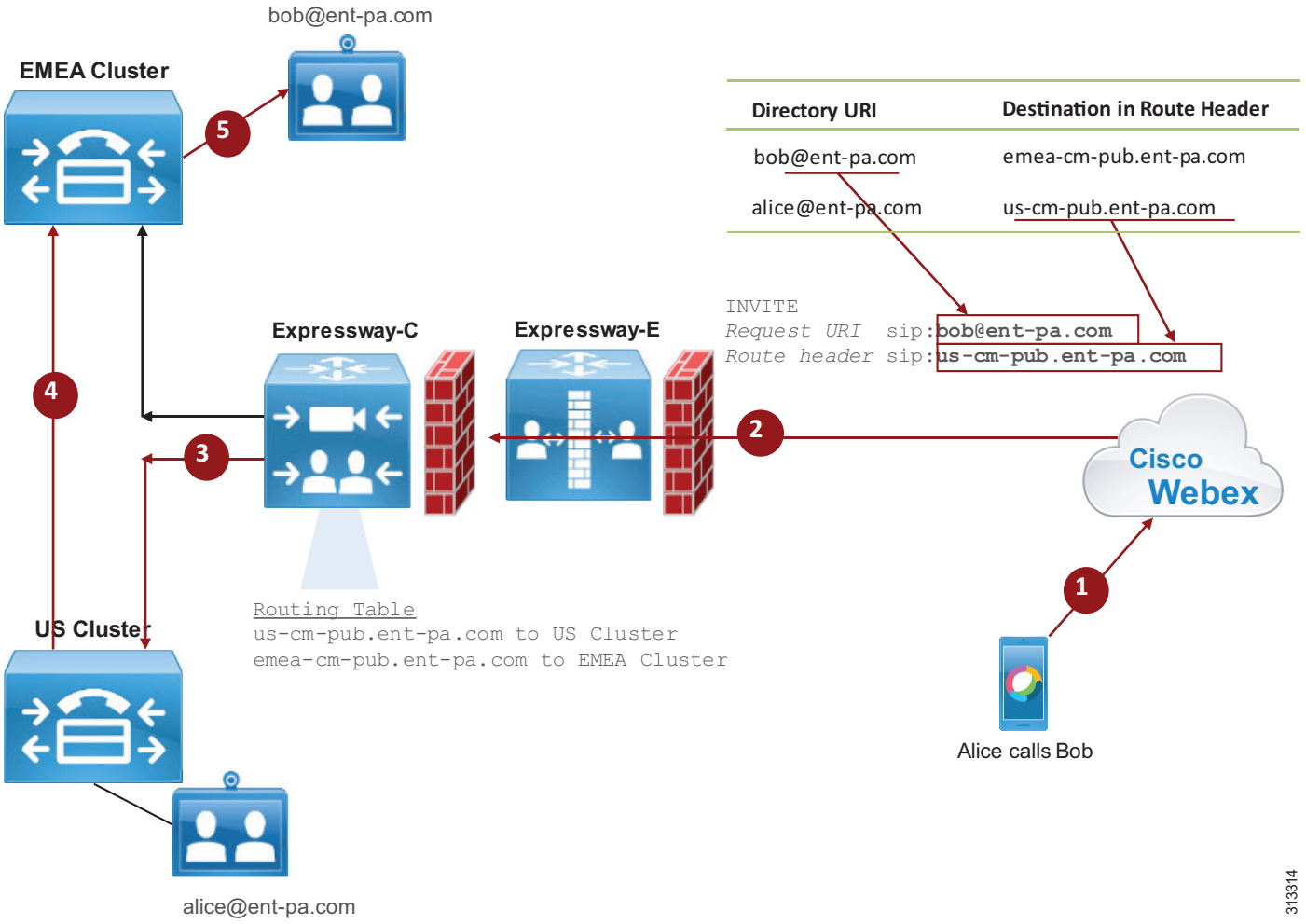
Although the CFQDN enterprise parameter in Unified CM allows the use of wildcards (for example, *.ent-pa.com), the use of the first value of the CFQDN enterprise parameter as the SIP route header for Call Service Connect call flows prohibits the use of wildcards in the first CFQDN value. If a wildcarded value is required to maintain the existing call routing logic on Unified CM, then a non-wildcard CFQDN has to be added as the first entry, such as in the following example:

```
CFQDN: us-cm-pub.ent-pa.com *.ent-pa.com
```

Note The CFQDN must be different than the Cisco Expressway-C or Expressway-E DNS domain. As an example, if the CFQDN is set to ent-pa.com and the DNS domain of Expressway is also set to ent-pa.com, Expressway might not be able to route the call because this creates an ambiguity between regular inbound business-to-business calls and Call Service Connect call flows.

Expressway-C therefore has to be provisioned with search rules to route the call to the correct Cisco Unified CM cluster based on the Route Header, as shown in Figure 5-10.

Figure 5-10 Call Routing Based on Route Header



For the scenario in Figure 5-10, two search rules are built on Expressway-C: the first matches calls with destination us-cm-pub.ent-pa.com and sends them to Cisco Unified CM in the US cluster, and the second matches calls with destination emea-cm-pub.ent-pa.com and sends them to Cisco Unified CM in the EMEA cluster.

With multiple clusters, each CFQDN must be unique for home cluster-based routing to work properly, as shown in Figure 5-9 and Figure 5-10.

Figure 5-10 shows the following actions:

1. Alice starts a call to Bob using her Webex Teams application.
2. The call is extended to Expressway-E and Expressway-C.
3. Based on the route header, the call is sent to the Unified CM cluster in the US.
4. The call is first anchored on the Unified CM US cluster and then sent to the destination in the Unified CM EMEA cluster.

Starting with release 12.0, Cisco Unified CM also can be configured to route calls based on the SIP route header. This allows support of Cisco Unified CM Session Management Edition (SME) architectures.

If Expressway-C and Expressway-E run Webex Hybrid Services but no business-to-business traffic, it is important to reject any SIP message not generated by Webex Hybrid Services. This is referred to as a *dedicated deployment*. A dedicated deployment uses Expressway's SIP signaling and media for Webex Hybrid Services only, and not for business-to-business traffic.

Cisco Expressway permits the creation of Call Processing Language (CPL) rules to mitigate fraudulent call attempts. We highly recommend deploying CPL rules for toll fraud mitigation.

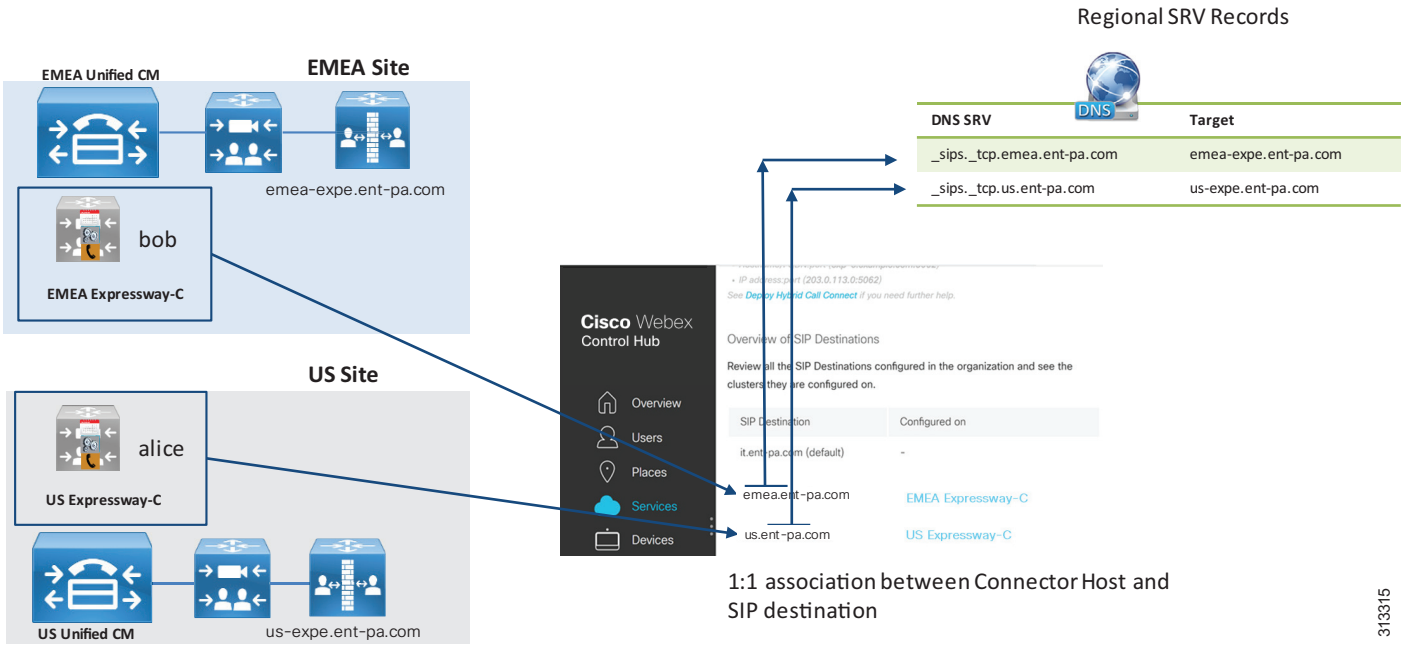
If business-to-business traffic is not included in the same Expressway, and because this traffic enters from the Default Zone, a CPL rule blocking any access to the Default Zone will prevent fraudulent access to Expressway-E. See the Call Connector Deployment Process for further details.

Multiple Cisco Unified CM and Expressway Clusters

When Cisco Unified CM is deployed in regional installations, every Cisco Unified CM cluster serves a specific region. That region might also have a dedicated Internet connection. In this case, the Expressway-C and Expressway-E cluster might also be dedicated to that region. In this scenario, Webex is able to route the call to the Expressway cluster connected to the Unified CM cluster where the calling user is configured.

In order for this routing architecture to work, it is important that an Expressway-C Connector cluster is dedicated to each Cisco Unified CM cluster. That way, it is possible to associate a specific SIP destination to each Connector Host, as shown in Figure 5-11.

Figure 5-11 Multiple Unified CM and Expressway Clusters



With the configuration in Figure 5-11, if Alice calls Bob, because Alice is provisioned by the US Expressway-C Connector Host, the SIP destination associated to the US Connector Host is chosen, and Webex performs the DNS SRV query to _sips._tcp.emea.ent-pa.com, which resolves into the Expressway-E in the US. The call is sent to the US Unified CM and is anchored before being routed to the destination Unified CM in EMEA.

Toll Fraud and Identity Theft Mitigation on a Shared Deployment

If Expressway-E allows business-to-business traffic together with hybrid call traffic, this is referred to as a *shared deployment*. For shared deployments, it is important to set up rules to minimize toll fraud attempts on Expressway-E. As a first step, the rules should determine if the calling ID is legal and should ensure that is does not contain an IP address of Expressway itself, the enterprise SIP domain, or the enterprise Webex Teams SIP address domain. Then the rules should analyze the called alias, preventing access to protected resources such as the PSTN gateway. See the Call Connector Deployment Process for further details.

The administrator might want to block +E.164 aliases coming through the Default Zone, other forbidden destinations, or protected services. The PSTN can also be accessed through different escape codes. In those scenarios, the rules need to be customized.

Also, the Authentication Policy in the Default Zone has to be set to **do not check credentials**, and the SIP authentication trust mode in the Webex DNS Zone must be set to **On**, while the Authentication Policy in the traversal client and server zone must be set to **check credentials**. In this way, traffic coming from the Default Zone and containing the Webex Teams SIP domain will be marked as unauthenticated and will thus be rejected by the rules. Legal traffic from the Default Zone will be sent to Unified CM as unauthenticated (P-Asserted-Identity Header stripped off), while traffic from Webex will be delivered to Unified CM as authenticated (P-Asserted-Identity Header preserved).

For more details on CPL rules, refer to the information on dial plan protection and Call Processing Language (CPL) in the *Cisco Collaboration System Solution Reference Network Designs (SRND)* guide, available at http://www.cisco.com/go/srnd.

Toll Fraud and Identity Theft Prevention on Cisco Unified CM

As a second line of defense, Cisco Unified CM 12.0 and later releases have the ability to distinguish between a trusted and untrusted identity. This is done through a parameter available on the SIP trunk called **Trusted Received Identity**. If this parameter is set to **Trust PAI Only**, Cisco Unified CM will not anchor any call received from that trunk if PAI is not present. Because Expressway-E trusts PAI only if the call has been previously authenticated through MTLS and the certificate clearly shows that the call is coming from Webex, the absence of PAI means that the call is coming from a different destination. In this case the call will not be anchored, and as a consequence the calling search space of the trunk will be used instead of the calling search space of the line of the anchored identity. Because calling search spaces of Expressway-C trunks should not include PSTN access, this will prevent any fraudulent attempt to access PSTN gateways and any identity theft attempt.

High Availability

Webex Hybrid Services will be highly available if Cisco Unified CM and Cisco Expressway are deployed in a cluster. Specifically, Expressway-C Connector Host can be deployed in a cluster to provide redundancy. The same guidelines that apply to Cisco Expressway also apply for Expressway-C Connector Host clustering. However, note that Call Service Connect takes an active role during the provisioning phase only, and if no Call Connector is available due to outages, calls will still work. With a non-redundant Call Connector, any user provisioning will be blocked during a Call Connector outage, planned or unplanned.

Call Connector Deployment Process

For detailed instructions on how to install and configure Call Connector, refer to the latest version of the *Deployment Guide for Cisco Webex Hybrid Call Service*, available at

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

Call Service Prerequisites

1. On Cisco Unified CM, set the mail ID of the user or import it from the LDAP directory.
2. On Cisco Unified CM, associate a directory URI to the user's directory number.
3. On Cisco Unified CM, set the telephone number attribute and associate it to the user's primary directory number.
4. On Cisco Unified CM, configure the enterprise parameter **Cluster Fully Qualified Domain Name**.
5. On Cisco Unified CM, associate users with devices.
6. On Cisco Unified CM, set the home cluster on the user configuration page.
7. Deploy Cisco Expressway-C and Expressway-E for firewall traversal capabilities.

Deploying Call Service Connect

1. On Cisco Unified CM, enable users for Cisco Unified Mobility.
2. On Cisco Unified CM, configure a Cisco Spark Remote Device for each user's primary extension. Alternatively, the administrator can configure automatic creation of the Cisco Spark Remote Devices, with the limitation that settings such as Device Calling Search Space, Rerouting Calling Search Space, Location, and Device Pool will be shared among all Cisco Spark Remote Devices. Note also that Line Calling Search Space is copied from the user's primary extension, and as such is user-specific
3. On Cisco Unified CM, set the Cisco Spark Remote Device to the user's primary extension and partition.
4. On Cisco Unified CM, associate the Cisco Spark Remote Device to the user's account.
5. On Expressway-E, set up a new DNS Zone for Webex Teams.
6. On Expressway-E, configure the DNS Zone for TLS with mutual authentication on a dedicated port (for example, port 5062). First enable port 5062 for MTLS globally under **Configuration -> Protocols -> SIP**, then set the Default Zone parameter **Enable Mutual TLS on Default Zone** to **off**. This will allow MTLS on port 5062 while continuing to support TLS with port 5061. If port 5062 must be used, make sure this port is open on the firewall.
7. On Expressway-E:
   a. Enable the Route Header support for this zone by setting the SIP parameter preservation to **On** (otherwise an INVITE containing a route header will not be processed), and set the SIP authentication trust mode to **On**.
   b. Make sure that the Authentication policy in the Default Zone is set to **do not check credentials**.

8. On Expressway-E:
   a. Configure a Webex traversal server zone (standard traversal server zone enabled for SIP only) or re-use the existing MRA traversal zone (called Unified Communications Traversal).
   b. If you are setting up a new zone, set the media encryption mode to **force encrypted** in order to have encrypted communications between Webex and Expressway-C.
   c. Enable Route Header support (see step 7a).
   d. Set the Authentication policy to **check credentials**.
9. On Expressway-E, create a search rule matching any call with a domain portion that includes <*subdomain*>**.call.webex.com** and with the destination set to the DNS Zone, such as:

```
Mode: Alias pattern match
Pattern Type: Regex
Pattern String: .*@example\.call\.webex\.com
```

10. On Expressway-E, create a search rule specifying that anything received from the Cisco Webex DNS Zone must be sent to the Cisco Webex Traversal Server Zone (or to Unified Communications Traversal):

```
Source Zone: Named
Source Name: Cisco Webex DNS Zone
Mode: Any alias
Target: Cisco Webex Traversal Server Zone
```

11. On Expressway-E, create the CPL rules as described for toll fraud and identity theft mitigation in the section on Deployment Considerations for Multiple Unified CM Clusters and as illustrated by the examples in the following tables:

    a. Call Service Connect Dedicated Expressway

Source Type	Originating Zone	Destination Pattern	Action
Zone	Default Zone	.*	Reject

    b. Call Service Connect Shared Deployment

    The following rules block calls from the Expressway-E Default Zone that contain the Webex Teams SIP domain ent-pa.call.webex.com, the corporate domain ent-pa.com, or the IP addresses of Expressway-E (10.10.10.10 and 10.10.10.11 in the example) in the calling alias.

Rule	Source Type	Rules Applies to	Source Pattern	Destination Pattern	Action
1	From address	Unauthenticated callers	.*@example\.call\.webex\.com.*	.*	Reject
2	From address	Unauthenticated callers	.*@example\.com.*	.*	Reject
3	From address	Unauthenticated callers	.*@10\.10\.10\.(10|11)	.*	Reject

    The following CPL rules are used to screen the called destinations. These rules block calls with a leading 0 or 9 (calls to the PSTN), allow calls if they contain the corporate domain in the called alias, and block all other calls.

Rule	Source Type	Originating Zone	Destination Pattern	Action
4	Zone	Default Zone	[0|9]\d*(@.*)?	Reject
5	Zone	Default Zone	.*@example\.com.*	Allow
6	Zone	Default Zone	.*	Reject

Note The order of these rules is important because Expressway-E analyzes them top-down.

12. On Expressway-C:

    a. Configure a Webex traversal client zone (standard traversal client zone enabled for SIP only) or re-use the existing MRA traversal zone (called Unified Communications Traversal).

    b. If you are setting up a new zone, set the encryption type to **force encrypted** in order to have encrypted communications between Webex and Expressway-C.

    c. Enable Route Header support and SIP parameter preservation to preserve the Contact Header, so that Webex is able to detect the loops.

    d. Set the Authentication policy to **check credentials**.

13. On Expressway-C:
    a. Configure a neighbor zone to Cisco Unified CM for Hybrid Call Services, different from the neighbor zone used for business-to-business calls.
    b. If mobile and remote access is configured in the same Expressway-C server, set the port to a value different than 5060 and 5061, such as 5560 or 5561.
    c. Enable Route Header support if the call will be sent to Cisco Unified CM SME 12.0.1 or later release. This step is not relevant for deployments where transit nodes are not used.
    d. The neighbor zone should be configured with a custom zone profile. In the custom zone profile, the SIP Parameter preservation should be set to **On**.
    e. For further information on how to set up the Cisco Unified CM zone, 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.
14. On Expressway-C, create a search rule matching any call with a domain portion that includes <*subdomain*>**.call.webex.com** and with a destination set to the Webex traversal client zone or to the Unified Communications Traversal zone:

```
Mode: Alias pattern match
Pattern Type: Regex
Pattern String: .*@example\.call\.webex\.com
```

15. On Expressway-C, create as many search rules as there are Cisco Unified Communications Managers deployed with hybrid services users. Those search rules must match the Cisco Unified CM CFQDN, and the destination must be set to the corresponding Unified CM neighbor zone:

```
Rule name: Calls to US UCM
Mode: Alias pattern match
Pattern Type: Prefix
Pattern String: us-cm-pub.ent-pa.com
Target: US-UCM neighbor Zone

Rule name: Calls to EMEA UCM
Mode: Alias pattern match
Pattern Type: Prefix
Pattern String: emea-cm-pub.ent-pa.com
Target: EMEA-UCM neighbor Zone
```

16. On Cisco Unified CM, create a SIP Trunk Security Profile with a listening port set to match what has been configured in step 13b (for example, 5560 or 5561, in case security is turned on).
17. On Cisco Unified CM, create a SIP trunk linked to the security profile created in step 16, and point it to the Expressway-C. Include the SIP trunk in a route group and a route list.
18. On Cisco Unified CM, create a SIP route pattern (if not present) to route the domain *.webex.com to the Expressway-C, and specify the previously created route list as the target.

Bandwidth Management

Revised: October 4, 2019

This chapter describes the bandwidth management strategy for the Preferred Architecture (PA) for Cisco Webex Hybrid Services.

Overview

Bandwidth management architecture and deployment for the Cisco Collaboration on-premises solution is covered in depth in the latest version of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*, available at https://www.cisco.com/go/pa. This chapter covers the additional bandwidth management considerations for implementing Cisco Webex Hybrid Services in an existing deployment of the Enterprise Preferred Architecture for Collaboration. Therefore, before continuing with this chapter, it is a requirement for you to read and understand the concepts and deployment recommendations in the *Bandwidth Management* chapter of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*.

The first part of this chapter provides an architectural overview and introduces some fundamental design concepts at a high level. A more detailed discussion of the architecture and design considerations for Cisco Webex Hybrid Services is then articulated in order to situate the hybrid products and components within the bandwidth management strategy and policies covered in the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*.

The second part of this chapter covers deployment procedures, again focusing only on the hybrid components within an on-premises Cisco Collaboration solution. The Architecture section discusses how the hybrid endpoints, clients, products, and components fit within the identification and classification, queuing and scheduling, provisioning and admission control architecture, using the hypothetical customer topology presented in the examples throughout this document. The Deployment section of this chapter describes the deployment procedures at a high level. The deployment examples in that section help explain the implementation of certain design decisions more clearly than an abstract discussion of concepts can. The order of the topics in the Deployment section follows the recommended order of configuration.

Core Components

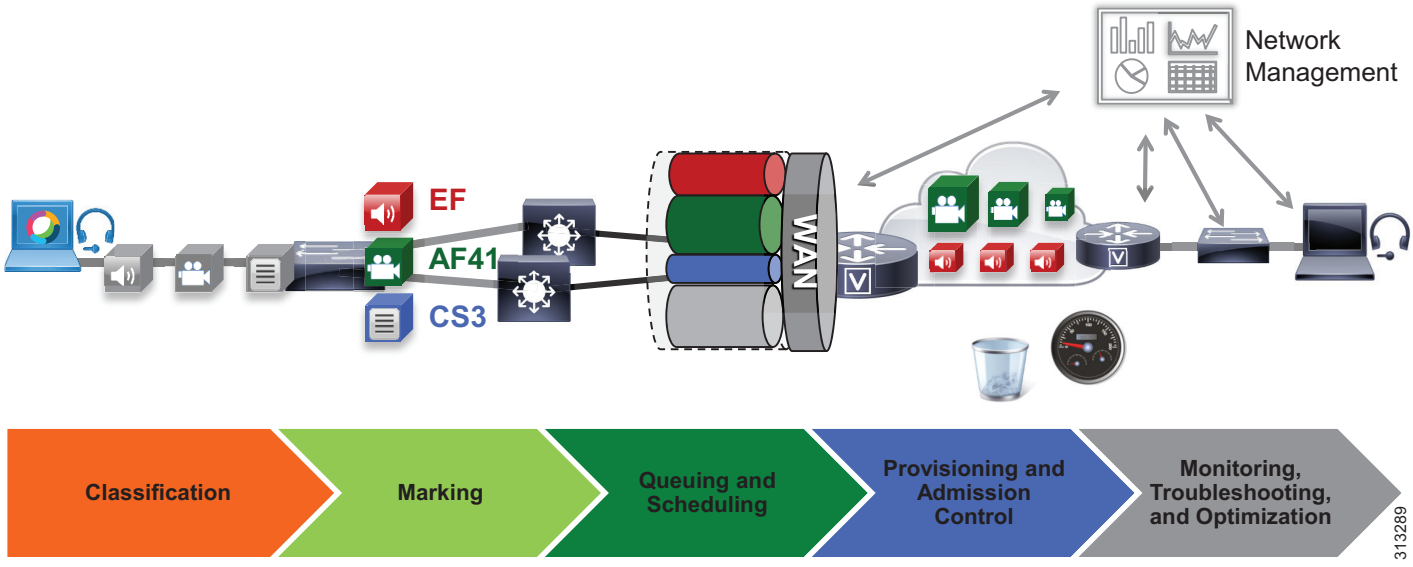
Cisco Webex Hybrid Services architecture contains these key components:

- Cisco Unified Communications Manager
- Cisco Webex Teams applications and endpoints
- Cisco Expressway
- Cisco Webex
- Cisco Webex Video Mesh Node
- Network infrastructure:
  - Cisco routers
  - Cisco switches

Figure 6-1 illustrates the design approach to Quality of Service (QoS) used in the Cisco PA for Enterprise Collaboration. This approach consists of the following phases:

- **Classification and Marking** — Refers to concepts of trust and techniques for identifying media and call signaling for endpoints and applications. It also includes the process of mapping the identified traffic to the correct DSCP markings to provide the media and signaling with the correct per-hop behavior end-to-end across the network.
- **Queuing and Scheduling** — Consists of general WAN and Internet queuing and scheduling, the various types of queues, and recommendations for ensuring that collaboration media and signaling are correctly queued on egress to the WAN and Internet.
- **Provisioning and Admission Control** — Refers to provisioning the bandwidth in the network and determining the maximum bit rate that groups of endpoints will utilize. This is also where call admission control can be implemented in areas of the network where it is required. Admission control applies only to the on-premises solution.
- **Monitoring, Troubleshooting, and Optimization** — Ensures the proper operation and management of voice and video across the network. Cisco Prime Collaboration offers a suite of tools to perform these functions. Monitoring, troubleshooting, and optimization are not covered in the Preferred Architectures but are part of the overall approach.

Figure 6-1 Architecture for Bandwidth Management



Recommended Deployment

Modify the existing on-premises QoS switch and WAN and Internet policies to include Webex Hybrid Services identification, classification, and marking. As mentioned, it is assumed that the QoS policies in place are those articulated in the *Bandwidth Management* chapter of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*, available at https://www.cisco.com/go/pa.

- Identify and classify media and SIP signaling traffic from the Webex Teams applications and the Webex Video Mesh Nodes.
- Media and signaling marking recommendations:

  1. Mark all audio with Expedited Forwarding class EF (includes all audio of voice-only calls as well as audio for all types of video calls).

  2. Mark all Webex Teams application video with an Assured Forwarding class of AF42 for an opportunistic video class of service or with AF41 for a prioritized video class of service. The marking of AF41 or AF42 will depend on the choice of whether or not to deploy opportunistic video during the on-premises deployment phase.

  3. Mark all call signaling with CS3. (All call signaling in HTTPS traffic will be marked based on the enterprise's current policy of traffic marking for HTTP/HTTPS.)
- Configure QoS on all media originating and terminating applications such as the Video Mesh Nodes.
- Update the WAN edge ingress re-marking policy.
- Update the WAN edge egress queuing and scheduling policy if applicable.

Key Benefits

This deployment of bandwidth management provides the following benefits:

- Provides prescriptive recommendations to simplify deployment with a simplified QoS architecture that integrates with the Enterprise PA for Collaboration
- Makes more efficient use of network resources
- Supports mobile and multi-media collaboration devices
- Takes into account unmanaged network segments (Internet)
- Is "future-proof" because it facilitates introduction of new services, features, and endpoints

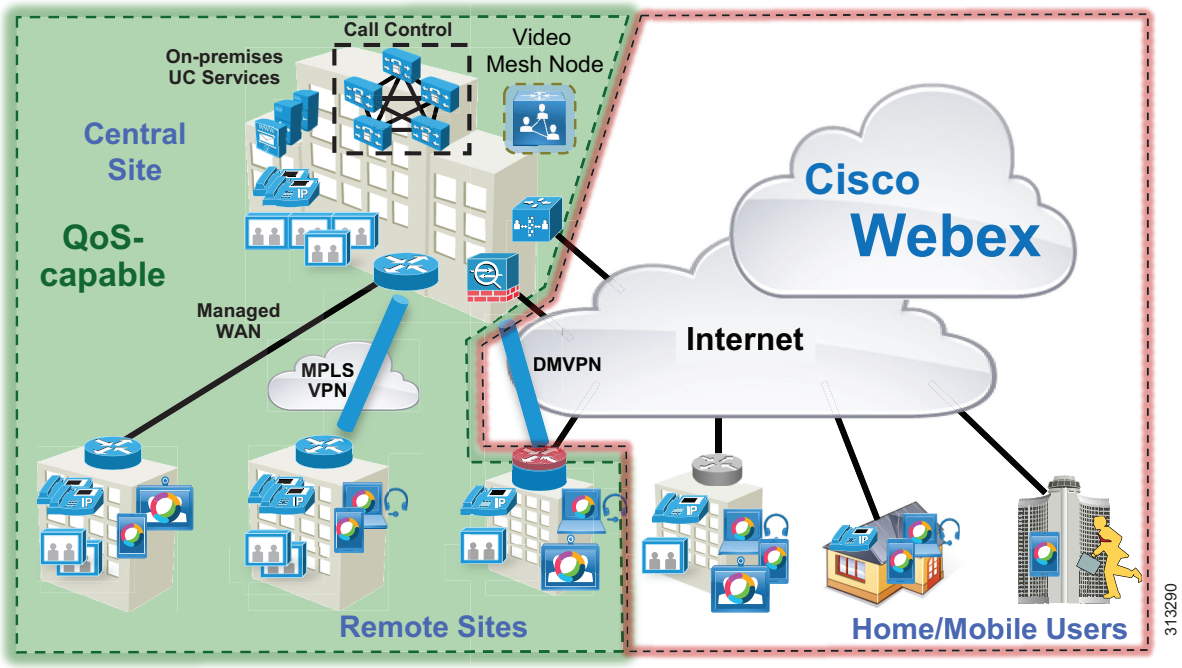
Architecture

In this Preferred Architecture, usage of the Internet and cloud-based services such as Webex Teams is an important aspect of the solution, which means that some of the collaboration infrastructure is located outside of the managed enterprise network and located in the cloud. The enterprise office connectivity options also range from remote sites and mobile users connected over managed leased lines directly connected to MPLS or other technologies, to connectivity over the Internet through technologies such as Dynamic Multipoint VPN (DMVPN), for example. With Webex Teams an office can be anywhere there is sufficient Internet connectivity.

Figure 6-2 illustrates the convergence of a traditional on-premises collaboration solution in a managed (capable of QoS) network with cloud services and sites located over an unmanaged (not capable of QoS) network such as the Internet. On-premises remote sites are connected over this managed network, where administrators can prioritize collaboration media and signaling with QoS, while other remote sites and branches connect into the enterprise over the Internet, where collaboration media and signaling cannot be prioritized or are prioritized only outbound from the site. Many different types of mobile users

and teleworkers also connect over the Internet into the on-premises solution. So the incorporation of the Internet as a source for connecting the enterprise with remote sites, home and mobile users, as well as other businesses and consumers, has an important impact on bandwidth management and user experience.

Figure 6-2 Managed and Unmanaged Networks



This section presents a strategy for leveraging smart media techniques in Cisco video endpoints, building an end-to-end QoS architecture, and using the latest design and deployment recommendations and best practices for managing bandwidth to achieve the best user experience possible based on the network resources available and the various types of networks that collaboration media traverse.

Media Assure

When deploying video pervasively across an organization, administrators will inevitably encounter insufficient bandwidth to handle the load of video required during the busy hour in some bottleneck areas of the Wide Area Network (WAN). In light of this, it is important to prioritize video correctly to ensure that audio is not affected by any video packet loss that may occur and to ensure that certain types of video can leverage video rate adaptation to manage the amount of bandwidth used during times of congestion. The media resilience and rate adaptation techniques allow for an optimized video experience in the face of congestion and packet loss over managed and unmanaged networks, but that is not all. These techniques, when used as a strategy coupled with QoS, enable an organization to deploy video pervasively while at the same time maximizing video quality. They allow endpoints to reduce their bit rate and thus their bandwidth utilization during periods of congestion and packet loss. In addition, during more idle times of the day outside of the busy hour, endpoints are able to increase their bit rate and thus utilize more of the available bandwidth.

Every Cisco video endpoint employs a number of media techniques to avoid network congestion, recover from packet loss, and optimize network resources. These techniques, termed Media Assure, have been broadly implemented across Cisco Collaboration endpoints and clients, including Webex Teams and Cisco's conferencing infrastructure.

Rate Adaptation

Rate adaptation or dynamic bit rate adjustments, part and parcel of Media Assure, adapt the call rate to the variable bandwidth available, down-speeding or up-speeding the video bit rate based on the packet loss condition. An endpoint will reduce bit rate when it receives messages from the receiver indicating there is packet loss; and once the packet loss has decreased, up-speeding of the bit rate may also occur.

The Self-Regulating Video Network

The self-regulating video network, prioritized audio, and opportunistic video are all QoS concepts as well as a QoS strategy. A self-regulating video network consists of leveraging the smart media and rate adaptation techniques of Media Assure discussed previously, along with proper provisioning and QoS to allow the video endpoints to maximize their video resolution during times when video bandwidth is not fully utilized in the network and to rate adapt or throttle down their bit rate to accommodate more video flows during the busy hour of the day.

Prioritized audio for both audio-only and audio of video calls ensures that all audio is prioritized in the network and is thus not impacted by any loss that can occur in the video queues. Prioritizing voice from all types of collaboration media ensures that even during times of extreme congestion when video is experiencing packet loss and adjusting to that loss, the audio streams are not experiencing packet loss and are allowing the users to carry on an uninterrupted audio experience.

In addition, opportunistic video allows for a group of video endpoints to be strategically marked with a lower class of video, thus allowing them to use available bandwidth when the opportunity arises. This enables endpoints to achieve optimal video resolution during times when the network is less congested and more bandwidth is available. Conversely, endpoints are able to down-speed their video more aggressively than the higher prioritized class of video during times of congestion when the network is in its busiest hour.

This concept of opportunistic video, coupled with prioritized audio, maintains an acceptable video experience while simultaneously ensuring that voice media for these opportunistic video calls is not compromised. This of course applies to the managed network, since an unmanaged network such as the Internet is not QoS enabled and thus provides no guarantees with regard to packet loss. Nevertheless, the media resiliency and rate adaptation mechanisms also attempt to ensure that media over unmanaged networks has the best possible quality in the face of packet loss, delay, and jitter.

Opportunistic video is an optional deployment choice that adds value to a self-regulating video network with prioritized audio; however, it is not mandatory for a self-regulating video network to function.

QoS Architecture for Collaboration

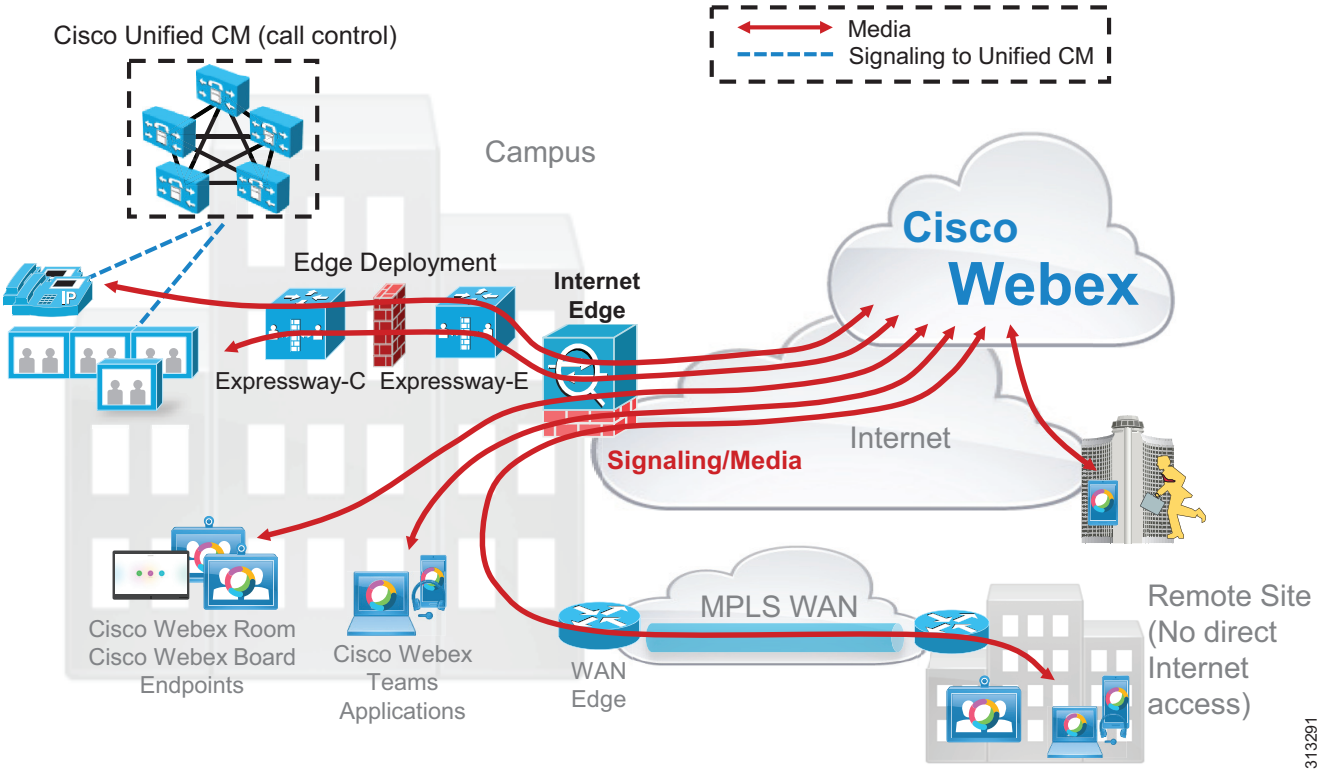
Quality of Service (QoS) ensures reliable, high-quality voice and video by reducing delay, packet loss, and jitter for media endpoints and applications. QoS provides a foundational network infrastructure technology, which is required to support the transparent convergence of voice, video, and data networks. With the increasing amount of interactive applications (particularly voice, video, and immersive applications), real-time services are often required from the network. Because these resources are finite, they must be managed efficiently and effectively. If the number of flows contending for such priority resources were not limited, then as those resources become oversubscribed, the quality of all real-time traffic flows would degrade, eventually to the point of futility. Media Assure and QoS ensure that real-time applications and their related media do not oversubscribe the network and the bandwidth provisioned for those applications. These smart media techniques coupled with QoS are a powerful set of tools used to protect real-time media from non-real-time network traffic and to protect the network from over-subscription and the potential loss of quality of experience for end users of voice and video applications.

Webex Teams Signaling and Media Path Overview

It is important to understand the path taken by interactive audio and video streams generated by one-to-one calls and multipoint meetings in a Webex Hybrid Services deployment, so that you can apply the QoS tools in the relevant parts of the network and can provision bandwidth correctly.

Figure 6-3 depicts the network paths taken by Webex Teams signaling and media traffic in a typical hybrid deployment where mobile users are connected directly to the Internet and thus the Webex Teams application and on-premises endpoints connect to the Webex Hybrid Services for connectivity to Webex Meetings and/or the Webex Teams application via the Cisco Expressway Edge deployment.

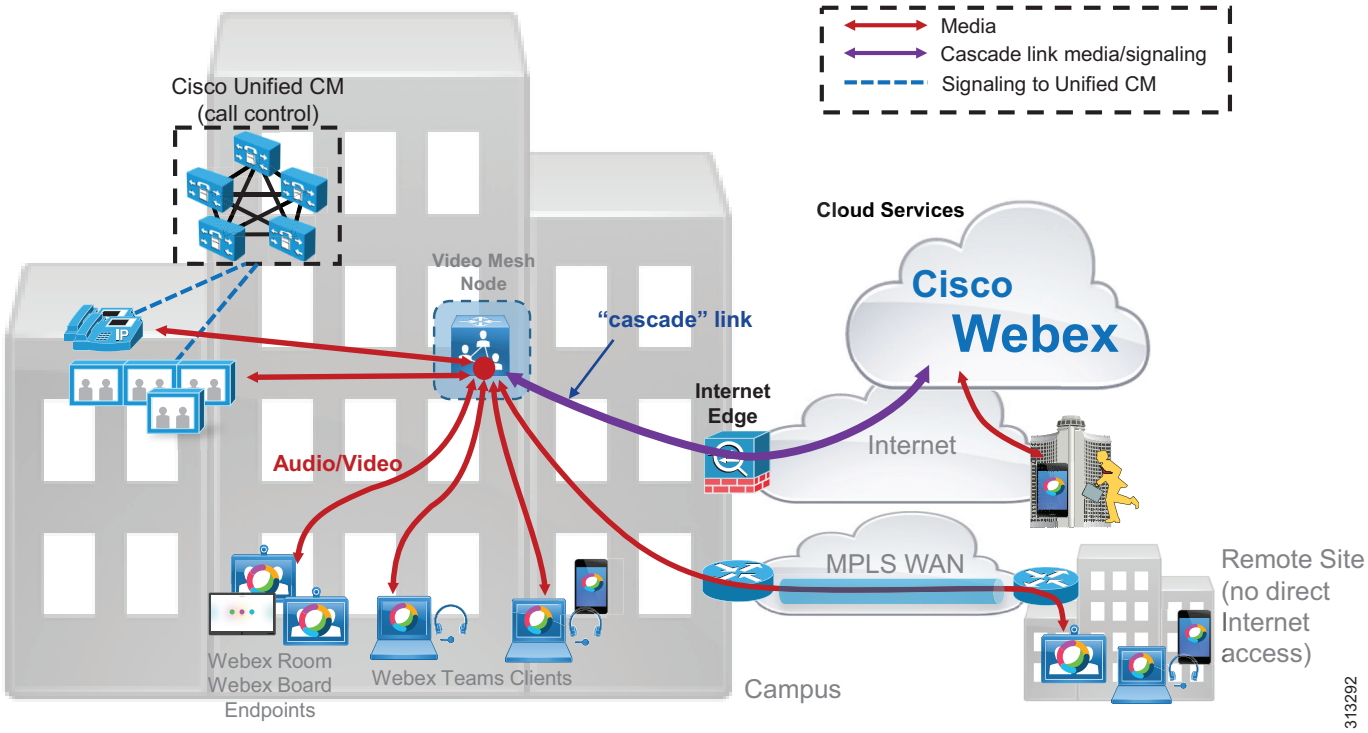
Figure 6-3 Signaling and Media Path for On-Premises Endpoints and Webex Teams Applications



As shown in Figure 6-3, audio/video traffic always flows between Webex Teams endpoints and Webex, whether it belongs to a point-to-point call, a multipoint meeting, or a wireless screen sharing session. Depending on the enterprise network topology, this media traffic might have to traverse the WAN before reaching the enterprise's Internet edge; for example, if the endpoints are located at a remote site that does not have direct Internet access (as seen in the Remote Site in Figure 6-3).

A unique aspect of Webex Hybrid Services is that it allows enterprise customers to deploy Webex Video Mesh Nodes on their corporate network to optimize media flows. Figure 6-4 shows a Webex Teams deployment with a Video Mesh Node located in the main site.

Figure 6-4 Webex Video Mesh Node Forms a Cascade Link to Webex



When a Video Mesh Node is present, Webex Teams endpoints and applications located inside the corporate network automatically detect it and send their audio/video streams to it. If any participants to a multipoint meeting are located on the Internet (for example, the mobile user in Figure 6-4), they will send their audio/video flows to Webex and a "cascade" link will automatically be set up between Webex and the Video Mesh Node, so that all meeting participants can have the same experience. For more information on the Video Mesh Node, see the chapter on Cisco Webex Video Mesh.

The exception to this is for on-premises endpoints connecting to meetings hosted by Webex. It is possible to configure a SIP trunk to an on-premises Video Mesh Node for Webex Meetings so that on-premises SIP endpoints can then connect to a Webex meeting by leveraging the on-premises Video Mesh Node. In this case the media and signaling from the Video Mesh Node for the on-premises endpoints will follow the same path and use the same destination ports as for the Webex Teams clients and endpoints. (Source ports for Unified CM endpoints are configured in the Unified CM SIP profiles.) See the Cisco Webex Video Mesh chapter for more information on integrating the Video Mesh Node for on-premises endpoints to connect to Webex Meetings.

Multistream Capabilities and Bandwidth Management

Webex Teams endpoints (Webex Teams applications and Webex Teams hardware endpoints) support multistreaming of video. This allows endpoints to render their own video experience instead of relying on the Cloud Video Services or Video Mesh Node to provide them with a transcoded composite experience. Webex Teams endpoints can typically send up to 4 video streams simultaneously. Streams are sent at different resolutions depending on what the other participants in the meeting are requesting based on their layout selection (for example, active speaker, equal layout, and so forth).

Typically resolutions of 1080p, 720p, 360p, and 180p can be sent. The exact resolutions may be affected by factors such as endpoint type, media assurance, and so forth. The resolutions are usually based on the following layouts:

- Active Speaker — 720p for the active speaker and 180p for the other participants in picture-in-picture (PIP) mode
- Equal Layout — 360p for all participants
- 1080p for Video Mesh meetings only, and enablement requires specific configuration on the Video Mesh cluster (See the Cisco Webex Video Mesh chapter for more details.)

Consider the example in Figure 6-5.

Figure 6-5 Example Webex Teams Meeting

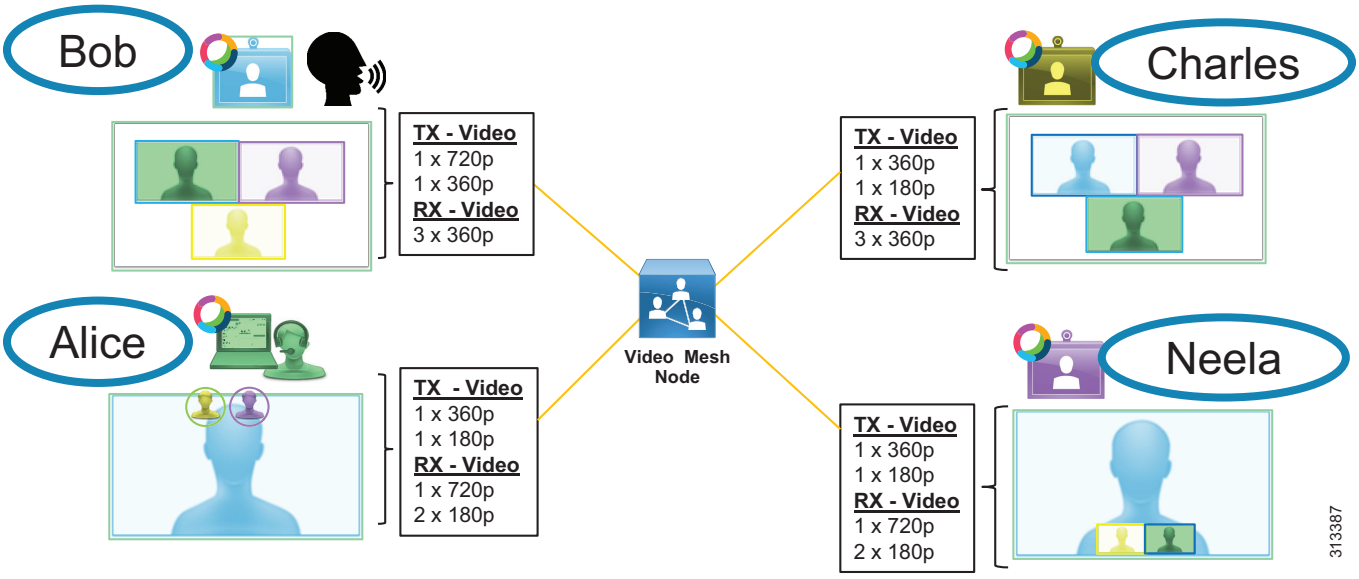


Figure 6-5 shows four participants in a meeting, which is being hosted on a Webex Video Mesh Node. Each participant is using a Webex Teams endpoint. Bob is the current active speaker. Bob and Charles have set their layout preference to Equal Layout. Alice and Neela have set their layout preference to Active Speaker with picture-in-picture.

Bob's endpoint will transmit (TX) 2 video streams:

- 720p stream as requested by Alice and Neela
- 360p stream as requested by Charles

Bob's endpoint will receive (RX) 3 video streams, each at 360p, from the 3 other meeting participants.

Charles' endpoint will transmit (TX) 2 video streams:

- 360p stream as requested by Bob
- 180p stream as requested by Alice and Neela

Charles' endpoint will receive (RX) 3 video streams, each at 360p, from the 3 other meeting participants.

Alice's endpoint will transmit (TX) 2 video streams:

- 360p stream as requested by Bob and Charles
- 180p stream as requested by Neela

Alice's endpoint will receive (RX) 3 video streams:

- One 720p stream from Bob
- Two 180p streams from Charles and Neela

Neela's endpoint will send 2 video streams:

- 360p stream as requested by Bob and Charles
- 180p stream as requested by Alice

Neela's endpoint will receive 3 video streams:

- One 720p stream from Bob
- Two 180p streams from Charles and Alice

If a user changes their endpoint layout mid-call, the other participants negotiate the send resolution to facilitate the requested layout. The send and receive bandwidths will also be impacted by changes to the send/receive resolutions.

Webex Teams endpoints send content as a single video stream, usually at 720p. Video bandwidths are variable, depending on a number of factors including network queuing, Media Assure, frame rate, and other factors such as video layout chosen by the user.

Webex Teams endpoints use the Opus audio codec, which adapts to current network conditions. Audio is typically sent at about 80 kbps (with headers); however, it is typically much less and averages around 48 kbps using the OPUS codec when a speaker is active. Receive audio, on the other hand, can be up to 3 audio streams from the last 3 active speakers. Thus, the receive audio can be as much as (3 * 80 kbps) or 240 kbps, but also tends to average around 100 to 120 kbps unless all 3 speakers are speaking at the same time.

At the time of this publication, SIP endpoints do not support multistreaming in a Webex Meeting.

Multistreaming also affects cascade links between Video Mesh Nodes or to the cloud.

Multistream Cascading

The multistream technology applied to Webex Teams endpoints also applies to the cascade link of the Video Mesh Nodes. For example, a Video Mesh Node can send multiple video streams per endpoint inside the cascade link to Webex. For more information on Video Mesh cascade links, see the section on Cascading in the Cisco Webex Video Mesh chapter.

Consider the example in Figure 6-6.

Figure 6-6 Multistream Cascading Example

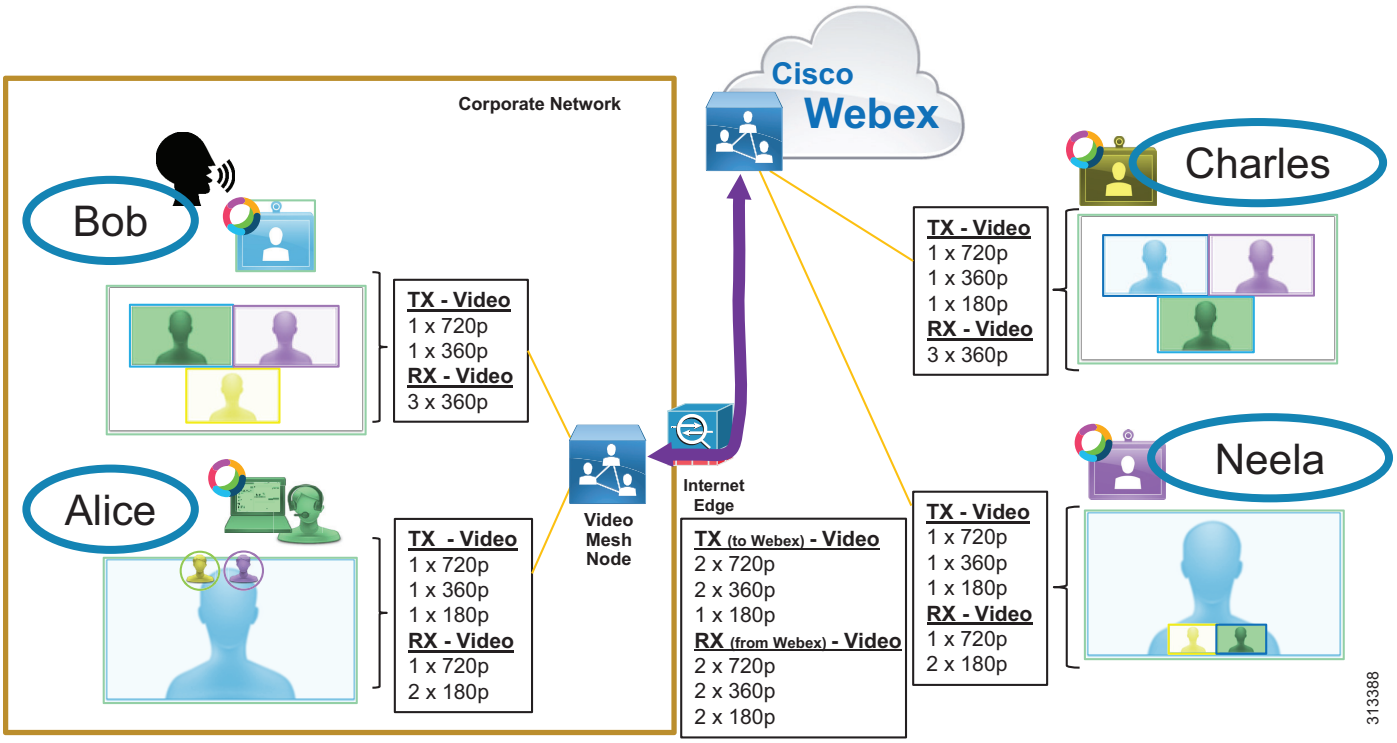


Figure 6-6 shows Bob, Alice, Charles, and Neela attending a meeting. Bob and Alice are on the corporate network. Their Webex Teams endpoints are sending media to, and receiving media from, the local Video Mesh Node.

Charles and Neela are not on the corporate network. Their Webex Teams endpoints have connected to the cloud media service. The Video Mesh Node has created a cascade link to the cloud to allow all participants to see remote attendees. Bob is speaking.

The cascade link must carry Bob and Alice's video streams to Webex. Charles and Neela's video streams are sent from Webex to the Video Mesh Node.

In this scenario there are 5 video streams sent in the cascade link to the Webex Cloud to provide the video layouts requested by Charles and Neela as well as the minimum of 2 HD video streams of 720p for participants, in this case Bob and Alice's 720p video. In the other direction there are 6 streams sent in the cascade link to the Video Mesh Node from the Webex Cloud to provide the video layouts requested by Bob and Alice as well as the minimum of 2 HD video streams of 720p for participants, in this case Charles and Neela's 720p video.

If a user changes their endpoint video layout mid-call, a request will be sent to the other endpoints to adapt their transmit (TX) resolutions to meet the need.

The cascade link carries up to 2 HD video streams of 720p from the on-premises Video Mesh Node to the Webex Cloud as well as from the Webex Cloud to the Video Mesh Node, regardless of the requested resolutions. This is to accommodate HD video of the primary and secondary active speakers for the highest resolutions for each side of the cascade link, so that the switching between speakers is quicker and seamless when requested.

There are many variables involved when calculating the expected bandwidth usage of the cascade link, including:

- Number of participants per meeting
- Location of participants
- Video endpoint types
- Video layouts
- Up to 2 HD video streams of 720p per side of the cascade link

It quickly can become complicated to determine how much bandwidth will be used by an endpoint or a Video Mesh cascade link in a meeting where endpoints are sending and receiving multistream video of varying bandwidth driven by the video layouts of the users. Therefore, we recommend regularly monitoring Internet egress bandwidth utilization as well as cascade link bandwidth reports in the Webex Control Hub. The cascade link bandwidth reports detail how much bandwidth is used for cascading to Webex on a per-cluster basis. See the section on Monitoring Analytics in the Cisco Webex Video Mesh chapter for more information.

It is important to make some assumptions about average bandwidth consumption and use that value together with the maximum number of concurrent calls to calculate an expected bandwidth utilization rate, and then monitor the system to evaluate those assumptions based on actual utilization.

See the section on Bandwidth Provisioning and Capacity Planning for recommended bandwidth values based on certain assumptions and for an example capacity planning exercise.

Classification and Marking

When you deploy Webex Teams on an enterprise network across multiple sites, you must classify real-time media flows correctly (that is, identify them as audio, video, or other application traffic) and mark them as close as possible to the media source or whenever they enter the enterprise network domain.

Webex Teams endpoints, applications, and the Video Mesh Node always attempt to set DSCP for the traffic they originate, as indicated in Table 6-1. The table also shows the corresponding 802.11 User Priority (UP) values used when the connection is to an enterprise wireless network.

Table 6-1 DSCP Values Used by Webex Teams Endpoints, Applications, and Video Mesh Nodes

Traffic Type	DSCP (PHB; decimal value)	802.11 User Priority (UP)	Notes
Audio	EF; 46	6	Includes audio streams of voice-only calls, audio streams of video calls, and related RTCP packets
Prioritized video	AF41; 34	5	Includes video streams (main video and presentations or content) and related RTCP packets
Opportunistic video	AF42; 36	5	Includes video streams (main video and presentations or content) and related RTCP packets
Other traffic	Best Effort; 0	0	Includes messaging, file transfer, configuration, call and meeting setup

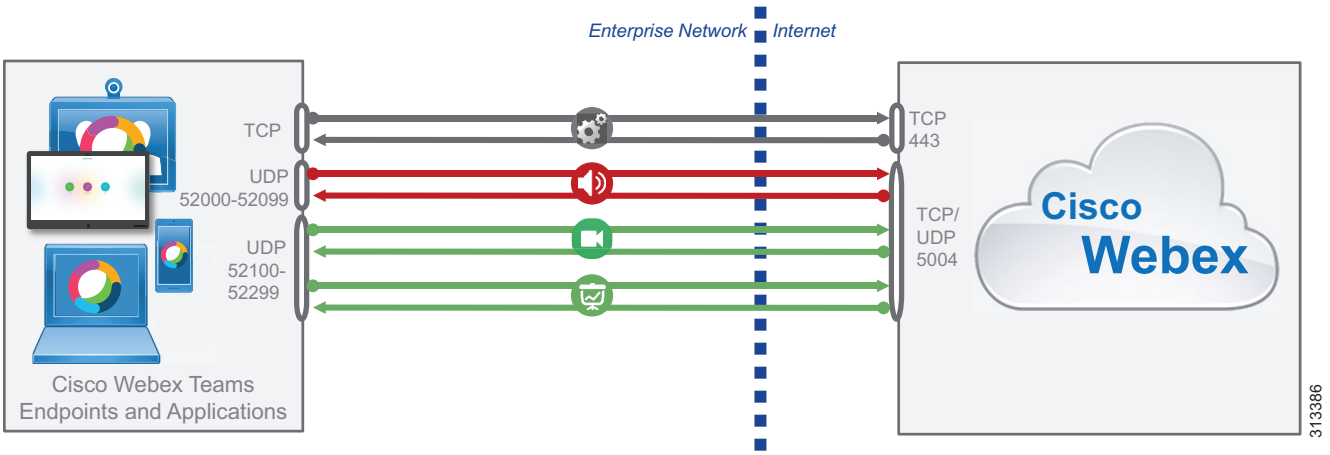
The DSCP values for media traffic are aligned with the RFC 4594 recommendations and with Cisco's design guidance for on-premises Collaboration deployments. (For more details, refer to the latest version of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*, available at https://www.cisco.com/go/pa.)

While it is possible to configure your network to pass through the DSCP values natively set by the endpoints, we recommend classifying traffic at the campus access layer in order to simplify ingress policy configuration. It is also worth noting that DSCP values are not preserved over the Internet, so network-based classification is necessary for media flows that originate from the cloud and are directed to endpoints on the enterprise network.

The ability of the network to identify Webex Teams media flows relies on a consistent usage of specific UDP port ranges for each media type, which essentially provide identifiable traffic "signatures." These traffic signatures can then be used to create access control lists (ACLs) to reclassify the flows in the network according to the implemented QoS policy. The traffic signatures are also leveraged by Cisco's Next Generation Network-Based Application Recognition (NBAR2) libraries and EasyQoS for easy creation of QoS policies.

As described earlier, Webex Teams endpoints and applications always send media to and receive media from a media node, which can be located either in Webex or on-premises. With media services located in Webex, all media streams from/to endpoints and clients are multiplexed over the same UDP port (5004). However, Webex Teams endpoints and applications use a different UDP port for each media stream they send and receive, with audio streams and video streams using distinct ranges as depicted in Figure 6-7.

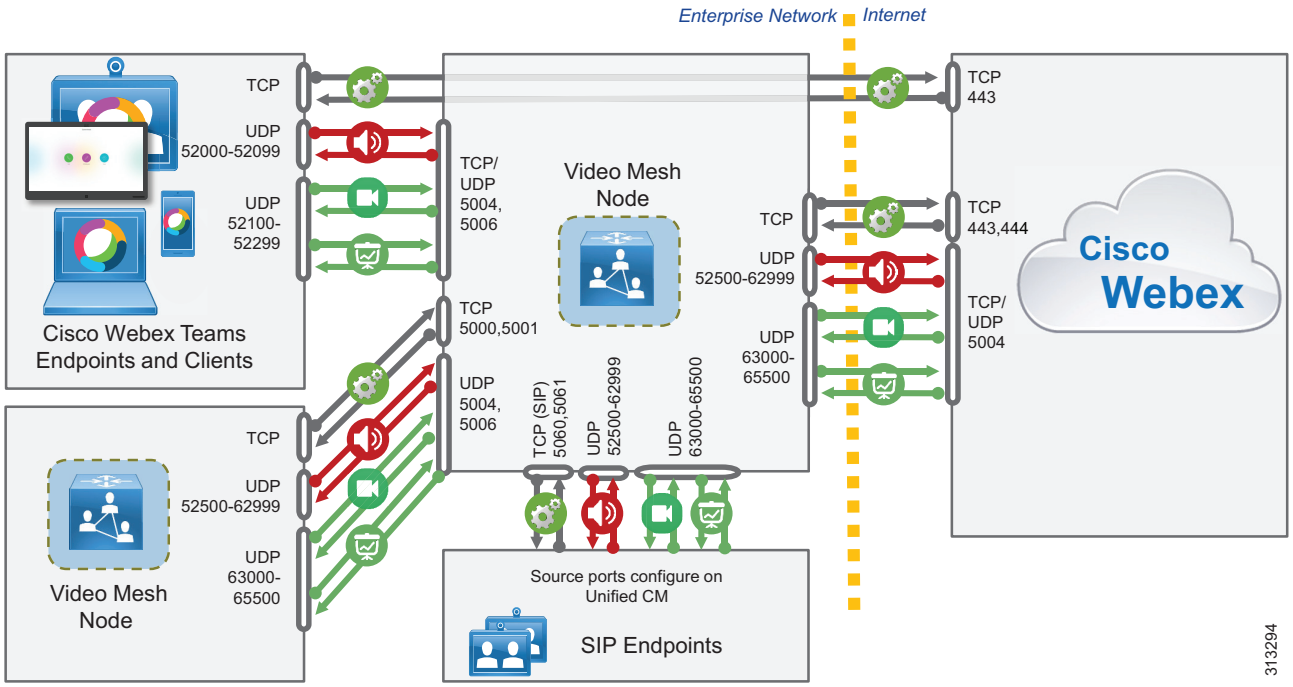
Figure 6-7 Dynamic Port Ranges for Webex Teams Endpoints and Applications



When a Video Mesh Node is deployed, the Webex Teams endpoints and applications use local ports from the same ranges to communicate with it, but media streams are terminated on different port ranges at the Video Mesh Node. A "cascade link" may also need to be created between the Video Mesh Node and the cloud if the meeting has external participants.

The Video Mesh Node requires larger port ranges than endpoints and applications, given the number of media streams that may be terminated by a single node. However, the IP addresses of Video Mesh Nodes are well known to the enterprise network administrator, so specific access control lists can be used to reclassify the traffic pertaining to these nodes if necessary. Figure 6-8 depicts the port usage for media flows between Webex Teams endpoints and applications, Video Mesh Node, and Webex Cloud media services.

Figure 6-8 Port Ranges for Webex Video Mesh Nodes



In summary, Table 6-2 shows all the traffic signatures for Webex Teams media flows and the corresponding recommended DSCP settings. In this table, flows are listed in the egress direction, which is from the endpoints toward the cloud, but the same port ranges apply to the flows in the ingress direction, which is from the cloud toward the endpoints. You can simply swap source and destination IP addresses and ports to obtain the traffic signatures for the ingress direction.

Table 6-2 Traffic Signatures for Webex Teams Real-Time Media (Symmetric[1])

Source IP Address	Destination IP Address	Source UDP Ports	Destination UDP Ports	Recommended DSCP[2]	Media Type[3]
Webex Teams application[4] or endpoint	Webex cloud media services or Video Mesh Node	52000 to 52099	5004	EF	Audio
Webex Teams application[4] or endpoint	Webex cloud media services or Video Mesh Node	52100 to 52299	5004	AF41 or AF42	Video
Video Mesh Node	Webex cloud media services or Video Mesh Node	52500 to 62999	5004	EF	Audio
Video Mesh Node	Webex cloud media services or Video Mesh Node	63000 to 65500	5004	AF41 or AF42	Video
Unified CM SIP endpoints	Video Mesh Node	Unified CM SIP Profile	52500 to 62999	EF	Audio
Unified CM SIP endpoints	Video Mesh Node	Unified CM SIP Profile	63000 to 65500	AF41 or AF42	Video

1. Symmetric in this case means that the same ports are used in the reverse direction where the source port becomes the destination port, and the destination port becomes the source port, for the return media path. For example, if the media source port from a Webex Teams application is 52004 and the destination port to the cloud is 5004, then the media return path from the cloud will have a source port of 5004 and a destination port to the Webex Teams application of 52004. Figure 6-8 illustrates the media paths and port ranges.
2. These values are the recommended values for DSCP marking based on UDP port ranges and not necessarily the “native marking” of the flows.

3. As elsewhere in this document, Audio in this table refers to audio streams of voice-only calls, audio streams of video calls, and related RTCP packets; while Video refers to video streams (main video and presentation or content sharing) and related RTCP packets.
4. This table does not currently apply to Webex Teams for Windows. Webex Teams for Windows currently uses ephemeral source ports for media provided by the windows OS. In an upcoming release expected in the next couple of months (from the date of this publication update) there will be a Control Hub configuration that will allow an Enterprise to change this behavior for the entire Org. It will allow an administrator the ability to set Webex Teams for Windows to use the same source port range as other Webex Teams Clients and as indicated in the above table. More information on this will be available in the next update of this chapter once this feature is Generally Available (GA). In the meantime contact your account team if you would like this enabled for your org prior to the feature GA.

With the traffic signatures listed in Table 6-2, you can classify Webex Teams real-time media using a common access control list (ACL) as close as possible to the network edge – that is, at the campus access layer and at the Internet edge.

If your deployment includes Video Mesh Nodes, you can also classify the audio and video traffic related to the cascade link between the Video Mesh Nodes and the Webex cloud media services, based on the UDP ports shown in Table 6-2 and the individual IP addresses of the Video Mesh Nodes.

All media traffic for calls to/from on-premises endpoints registered with Cisco Unified CM to/from Webex Teams meetings, endpoints, or applications is routed through the Expressway pair that is used for interconnecting the on-premises endpoints with the Webex Teams applications and meetings. The media and signaling DSCP values for the streams from the on-premises endpoints are set by Unified CM. This is covered in detail in the latest version of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*, available at https://www.cisco.com/go/pa.

Media and signaling DSCP values for the streams from Webex cloud media services to the on-premises endpoints are set by Expressway-C on ingress into the enterprise. The media and signaling are marked with the same DSCP settings as all other incoming Expressway media and signaling. Therefore, if the deployed Expressway edge equipment has been installed and configured as part of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*, then nothing more is required on Cisco Expressway.

For deployments where the Video Mesh Node sits in the DMZ, there is a Video Mesh Node configuration setting in the Webex Control Hub that allows the administrator to optimize the port ranges used by the Video Mesh Node. This **Quality of Service** setting, when disabled (enabled by default), changes the source ports that are used for audio, video, and content sharing from the Video Mesh Node to the range of 34000 to 34999. The impact of this, however, is that the Video Mesh Node will natively mark all audio, video, and content sharing to a single DSCP of AF41; and due to the fact that the source ports are the same for all media regardless of destination, it is not possible to differentiate the audio from video or content sharing based on port range with this setting disabled.

If your deployment requires the Video Mesh Node to be deployed in the DMZ, this setting may be helpful to reduce the firewall port openings. For more information on this setting and the impacts, refer to the *Deployment Guide for Cisco Webex Video Mesh*, available at

https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

Special Considerations for Cisco Webex Teams for Microsoft Windows

Webex Teams has special functionality for the Microsoft Windows platform that allows it to bind itself to specific source port ranges as shown in Table 6-2. These are the same port ranges that all other Webex Teams platforms (MacOS, Apple iOS, or Android) use natively.

In order to allocate source ports from the specific ranges shown in Table 6-2, Webex Teams for Windows application must make a request to the underlying operating system when it is first installed on a device. This results in the following behavior on devices running Microsoft Windows with Windows Firewall enabled:

> Because of a limitation in the Microsoft Windows APIs, whenever an application requests a specific source port from the operating system, it also gains permission to listen for unsolicited incoming traffic on that port. The Webex Teams application does not need these privileges because it receives packets only on a given port after transmitting from that same port, but it has no way of communicating this to the operating system.
>
> Therefore, in Microsoft Windows system configurations where Microsoft Windows Firewall is enabled, a security alert might be displayed to the end user when Webex Teams is first run, informing them that Windows Firewall has blocked some features of the application, and prompting them to allow access (which requires administrator privileges) or to cancel.
>
> It is important to note that, regardless of the action chosen by the end user for this alert, the Webex Teams application will operate correctly using the ports shown in Table 6-2, and no other alert will be displayed after the initial installation.

This applies only to Microsoft Windows and it does not affect the Webex Teams application on other platforms such as MacOS, Apple iOS, or Android.

Queuing and Scheduling

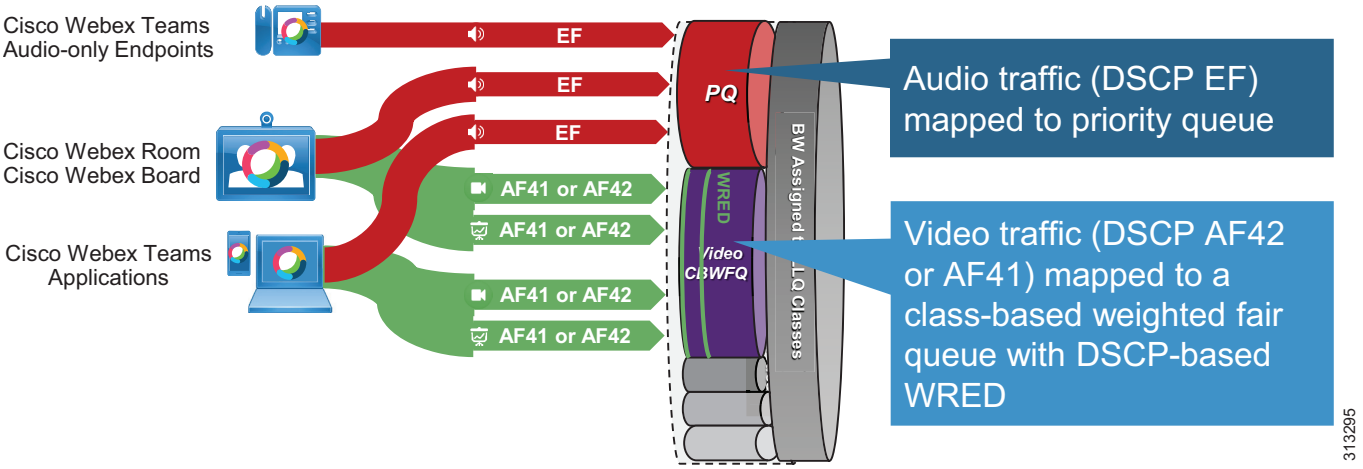
Once real-time media traffic has been correctly identified and classified with DSCP, it can be assigned to the appropriate queues in the network devices it traverses. Because WAN and Internet links are the most common bandwidth bottleneck points in an enterprise deployment, this section shows an example based on the Low-Latency Queuing (LLQ) features found in Cisco IOS routers, but the same considerations can be applied to other parts of the network such as the campus or data center.

In alignment with existing recommendations for on-premises Cisco Collaboration deployments, the WAN queuing and scheduling model adopted here is based on two separate queues for interactive media traffic, and the queue assignment is based on DSCP settings:

- A Priority Queue for all audio traffic marked with DSCP EF
- A Class-Based Weighted Fair Queue for all video traffic marked with DSCP AF41 for a prioritized class of video, or AF42 if an opportunistic class of video is configured

Figure 6-9 illustrates how media streams from Webex Teams endpoints and applications are assigned to queues in a Cisco IOS router.

Figure 6-9 Assigning Webex Teams Audio and Video Traffic to Queues



In Figure 6-9 the audio streams of voice-only calls and video calls are marked as EF and placed into a Priority Queue (PQ). Priority queues are generally associated with a policer that limits how much bandwidth can be allocated to the queue, in order to avoid starving other traffic types.

Video streams (main video and content or presentation sharing) are marked as AF41 or AF42 and placed into a Class-Based Weighted Fair Queue (CBWFQ) with Weighted Random Early Detect (WRED). AF42 marking is used if opportunistic video has been deployed and Webex Teams endpoints are used as the opportunistic video endpoints. These queues guarantee that the matching traffic will receive at least the configured bandwidth, but they can also take advantage of any unused bandwidth from other queues. WRED is a congestion avoidance mechanism that was originally developed for TCP applications, but it can also be effective with UDP applications that support loss-based dynamic rate adaptation, such as Cisco Collaboration endpoints that implement Media Assure. In a nutshell, when the queue length reaches a certain threshold, WRED preemptively starts to drop an increasing percentage of packets in the queue, thus triggering the loss-sensing rate adaptation algorithm before the tail of the queue is reached.

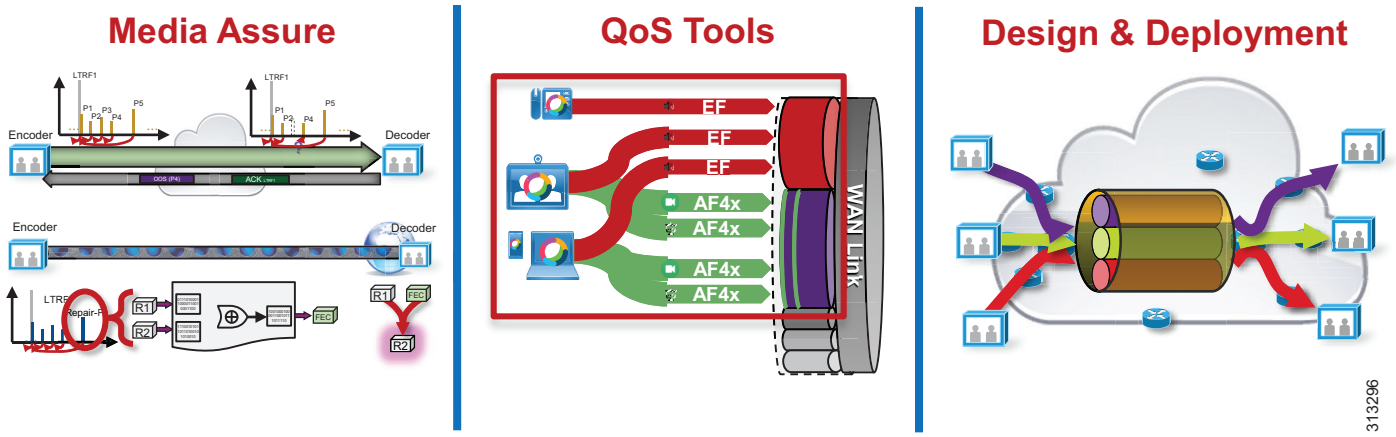
For more information about these features, refer to the latest version of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*, available at https://www.cisco.com/go/pa.

Deployment

The QoS and bandwidth management strategy for Webex Teams is based on the following three aspects, illustrated in Figure 6-10:

- Leverage the Media Assure tools to reduce the impact of packet loss (through media resilience techniques) and to minimize network congestion (through dynamic video bit-rate adaptation). These tools are valuable both on the public Internet and within the enterprise network.
- Consolidate mechanisms to identify real-time audio and video streams for Webex Teams in the enterprise network, and apply QoS classification and scheduling tools. This ensures that Webex Teams media gets the appropriate level of service when traversing the corporate internal network.
- Combine Media Assure and QoS classification and scheduling tools to simplify network provisioning and optimize bandwidth utilization on the enterprise network. This is achieved by integrating bandwidth provisioning best practices with the flexibility to allow a variable number of video streams to compete for the same bandwidth over the WAN or the Internet edge, knowing that during the busy hour the video streams will reduce their bit rate to avoid network congestion.

Figure 6-10 QoS and Bandwidth Management Tools



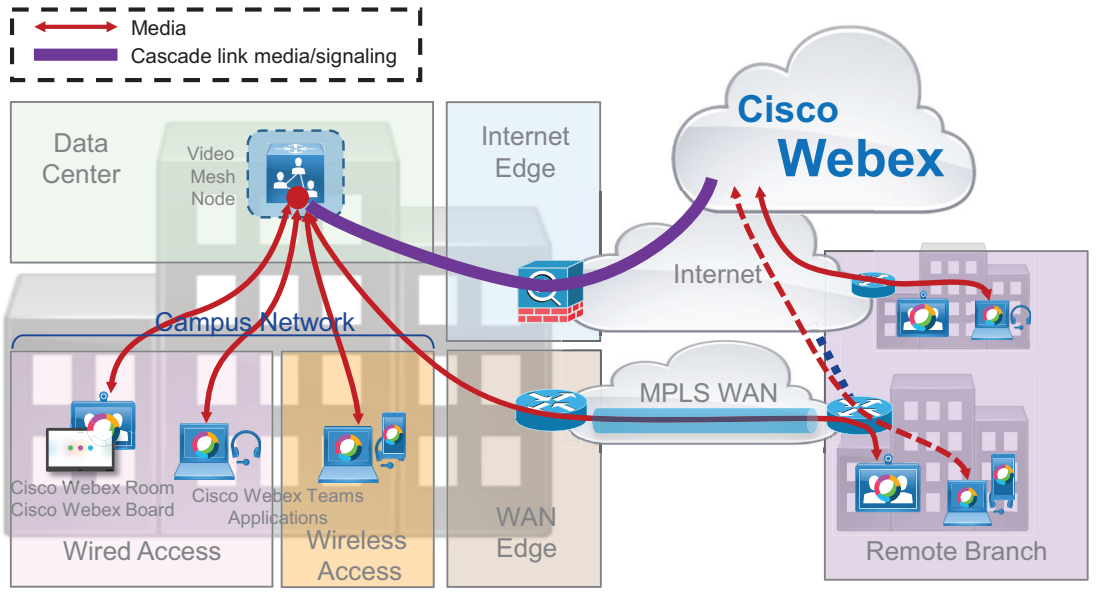
The remainder of this section provides deployment best practices to implement this strategy on an enterprise network.

Based on the identifiable media streams originated by Webex Teams endpoints and applications, common network QoS tools can be used to create traffic classes and to re-mark packets according to those classes. These QoS mechanisms can be applied in different parts of the network, such as the campus access layer (which is closest to the endpoint), the distribution or core layer, the WAN edge, and the Internet edge. Regardless of where classification and re-marking occurs, we recommend using DSCP to ensure end-to-end per-hop behaviors.

The recommendation is to classify and re-mark at the access layer, then trust through the distribution and core of the network, and finally re-classify and re-mark at the WAN or Internet edge if and when needed. For smaller networks such as branch offices where no Layer 3 switching components are deployed, QoS marking can be applied at the WAN edge router.

Figure 6-11 outlines the places in the network relevant to a Webex Teams deployment.

Figure 6-11 Places in the Network for Applying QoS Mechanisms



For each place in the network shown in Figure 6-11, we recommend the following configuration tasks that allow you to easily integrate Webex Teams media traffic into your network:

- Campus Wired Access and Remote Branch

  Configure IP access control lists (ACLs) to classify Webex Teams audio traffic with DSCP EF and video traffic with DSCP AF42 (or AF41) based on the UDP port ranges in Table 6-2 (for egress traffic from the endpoints to the cloud). Alternatively, you can classify traffic with NBAR2 on supported platforms.

- Internet Edge

  Configure IP ACLs to classify Webex Teams audio traffic with DSCP EF and video traffic with DSCP AF42 (or AF41) based on the UDP port ranges in Table 6-2 (reverse source and destination ports to match ingress traffic from the cloud to the endpoints). Alternatively, you can classify traffic with NBAR2 on supported platforms.

- Campus Wireless Access

  If your deployment includes Cisco 802.11 wireless access, use AireOS Application Visibility and Control (AVC) to classify Webex Teams traffic in the Cisco Wireless LAN Controller. Note that the native DSCP and 802.11UP marking applied by Webex Teams applications and endpoints allows for proper classification to also be applied to media traffic inside the CAPWAP tunnel between the wireless access point and the controller.

- WAN Edge and Internet Edge

  Adjust the bandwidth provisioning of relevant queues on outbound router interfaces to accommodate Webex Teams media traffic. (See the Bandwidth Provisioning and Capacity Planning section for details.).

- Data Center and Internet Edge

  If you deploy Webex Video Mesh Nodes, configure additional IP ACLs to classify audio and video traffic for the cascade links between the Video Mesh Nodes and the cloud.

- Remote Branch

  Consider providing direct Internet access to remote branch offices so that Webex Teams endpoints can connect directly to the cloud infrastructure. For design and configuration details, refer to the *IWAN Direct Internet Access Design Guide*, available at

  https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Dec2016/CVD-IWAN-DIADesignGuide-Dec16.pdf?dtid=osscdc000283

- Remote Branch

  If deploying Direct Internet Access at a branch site, you can use policy-based routing using the UDP port ranges in Table 6-2 to route media traffic from Webex Teams endpoints and applications directly to the cloud.

- All places in the network

  You can use the EasyQoS application in the APIC-EM SDN controller to simplify QoS policy configuration throughout your deployment. (More information about EasyQoS and APIC-EM is available on Cisco.com.)

Bandwidth Provisioning and Capacity Planning

While all Webex devices and applications use Media Assure to adapt their bit rate dynamically depending on network conditions and available bandwidth, it is important to know how much bandwidth is typically used by a call, so that WAN and Internet links can be provisioned to accommodate busy hour traffic without compromising the user experience. Table 6-3 lists audio and video bandwidth requirements for various types of Webex endpoints.

Table 6-3 Bandwidth Requirements for Webex Endpoints (Including Layer-3 Overhead)

Webex Endpoint	Audio Bandwidth	Video Bandwidth (Typical)	Video Bandwidth (Maximum[1])
Webex Teams applications	80 kbps	1 to 2 Mbps	3 Mbps
Webex DX Series, SX10	80 kbps	1 to 2 Mbps	3 Mbps
MX Series, SX20, SX80, Webex Room Kit, Webex Board	80 kbps	2 to 4 Mbps	10 Mbps
Video Mesh cascade	N/A	12 Mbps	20 Mbps

1. Maximum here refers to the sustained bandwidth usage with the highest possible video resolution. Due to the bursty nature of compressed video traffic, bandwidth usage can occasionally exceed these values for very short periods of time.

The bandwidth requirements in Table 6-3 take into account typical usage that includes Layer 3 overhead and multiple video streams for presentation sharing and local layout composition.

As indicated in Table 6-3, the maximum per-meeting negotiated cascade bandwidth is 20 Mbps for main video for all sources and the multiple main video streams they could send. This does not include the content channel or audio bandwidth. In a 3 month time-frame with the top 20 Webex Meetings customers using Video Mesh with an average of 9,100 meetings and 15,000 calls per month, the average per-meeting cascade bandwidth (TX + RX) was 11.6 Mbps. Therefore, using 12 Mbps for per-meeting cascade bandwidth is a good starting point to use in provisioning bandwidth; and with further monitoring of your system, bandwidth utilization can be better analyzed and estimated.

It can also be helpful to know what video resolution can be expected for a given bit rate of an individual video stream, as shown in Table 6-4.

Table 6-4 Video Resolutions and Bit Rate Ranges for Webex Teams Devices and Applications

Video Bit Rate Range	Webex Room Devices: Video Resolution	Webex Teams Applications: Video Resolution
Less than 128 kbps	176x144	180x90
128 kbps to 256 kbps	512x288	320x180
256 kbps to 320 kbps	512x288	480x270
320 kbps to 512 kbps	768x448	640x360
512 kbps to 900 kbps	1024x576	960x540
900 kbps to 1.8 Mbps	1280x720	1280x720
More than 1.8 Mbps	1920x1080	1920x1080

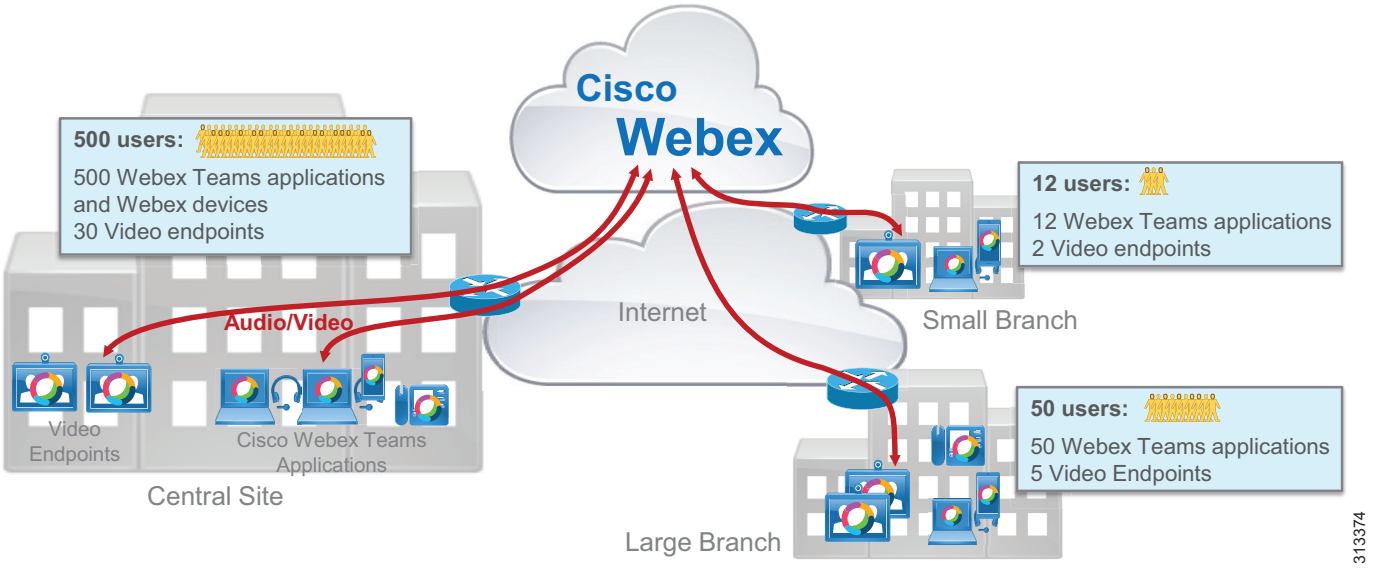
Taking into account the values shown in Table 6-3 and Table 6-4, you can plan the WAN and Internet bandwidth capacities based on the number of endpoints and/or users per site and the typical call volumes in the busy hour. No single formula will work for every deployment, but it can be useful to look at the following Provisioning Example to understand the steps involved in the capacity planning process.

Refer to the section on Multistream Capabilities and Bandwidth Management to understand the impact of multiple streams in Cisco Webex Teams environments.

Provisioning Example

Figure 6-12 shows an example of a multi-site Webex Teams deployment with three types of sites: the central site, a large branch office, and a small branch office. The number of users and endpoints at each site is also shown in the figure.

Figure 6-12 Bandwidth Provisioning Example for a Multi-Site Webex Teams Deployment



To keep things simple, we made a generalization in this example: All video endpoints such as Webex DX Series, Room Series, Room Kit Series, and Boards are all considered to be video endpoints running at a desired resolution of 720p.

A capacity planning exercise also requires some assumptions to be made with respect to busy-hour call attempts, call and meeting patterns, video endpoint utilization ratios, and average bandwidth per call. We assume the following average bandwidth values per call throughout this example:

- Voice call (or audio stream of a video call): 80 kbps
- Video streams of video endpoints: 2 Mbps at 720p resolution
- 2.5 Mbps at 1080p resolution (1080p is not applicable in this example)
- Video streams of Webex Teams application: 2 Mbps at 720p resolution, 1 Mbps at 540p resolution, and 500 kbps at 360p resolution

It is important to understand that these are ideal values based on desired call quality levels for each endpoint type. However, because the dynamic rate adaptation in Media Assure is based on observed instantaneous network congestion, it currently is not possible to enforce different bandwidth allocations for given groups of endpoints. Depending on relative call start time and resulting network congestion, it is therefore possible that several calls sharing the same bottleneck will adapt to different video bit rates, regardless of endpoint type.

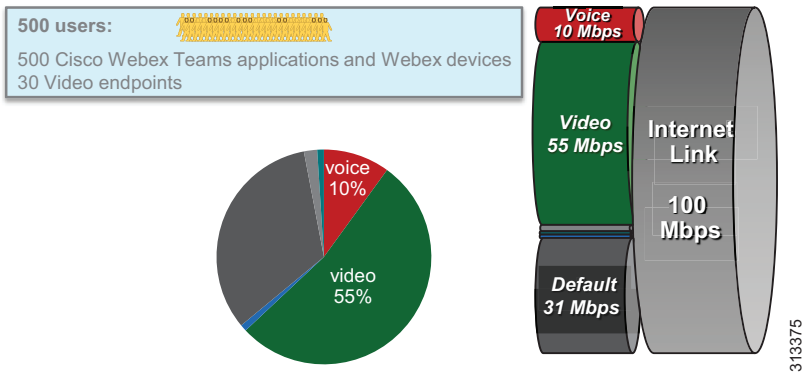
Also note that, although there is obviously no traffic prioritization on the Internet, it is always beneficial to configure queuing on the egress interface of the Internet edge router and to match the total bandwidth allocated for classes to the bandwidth provided by the Internet service provider. This ensures that the real-time media traffic from the endpoints toward the cloud is

guaranteed a share of the Internet access link even when competing with other applications. Throughout this example we assume a consistent distribution of bandwidth across classes that allocates 10% of the link bandwidth to the audio/voice queue and 55% of the link bandwidth to the interactive video queue.

The other assumptions are called out explicitly as we analyze the Internet bandwidth allocation at each site (central site, large branch, and small branch) and the bandwidth provisioned for each traffic class based on the number of users and endpoints.

First we look at the central site: In this example it is provisioned with a 100 Mbps connection to the Internet, which results in 10 Mbps allocated to the voice queue and 55 Mbps allocated to the video queue (see Figure 6-13).

Figure 6-13 Central Site Bandwidth Allocation Example



Based on the number of users and endpoints located at the central site, we made these additional assumptions about busy-hour calls and video endpoint utilization ratios:

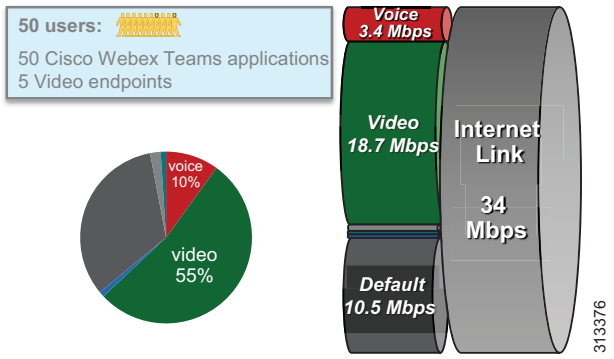
- At most 25% of the users are involved in a call (voice or video) at the same time.
- At most 50% of the video endpoints are involved in a call at the same time.

As a consequence, these are the numbers and types of calls that can be supported at the central site in this example:

- Voice queue: 10 Mbps; Supports 125 calls (80 kbps per call)
- Video queue: 55 Mbps
  - Video endpoints: 2 Mbps ∗ 30 calls ∗ 0.5 utilization ratio = 30 Mbps
  - Webex Teams application video: 55 - 30 = 25 Mbps; Supports 12 to 13 calls at 720p, 25 calls at 540p, or 50 calls at 360p

Next we look at the large branch site, which is provisioned with a 34 Mbps connection to the Internet, resulting in 3.4 Mbps allocated to the voice queue and 18.7 Mbps allocated to the video queue (see Figure 6-14).

Figure 6-14 Large Branch Site Bandwidth Allocation Example



Based on the number of users and endpoints located at the large branch site, we made these additional assumptions about busy-hour calls and video endpoint utilization ratios:

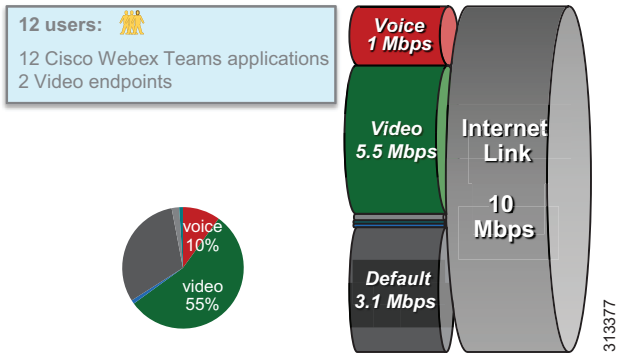
- At most 80% of the users are involved in a call (voice or video) at the same time.
- All video endpoints can be involved in a call at the same time.

As a consequence, these are the numbers and types of calls that can be supported at the large branch site in this example:

- Voice queue: 3.4 Mbps; Supports 42 calls (80 kbps per call)
- Video queue: 18.7 Mbps
  - Video endpoints: 2 Mbps ∗ 5 calls = 10 Mbps
  - Webex Teams application video: 18.7 - 10 = 8.7 Mbps; Supports 4 calls at 720p, 8 to 9 calls at 540p, or 17 to 18 calls at 360p

Next we consider the small branch site, which is provisioned with a 10 Mbps connection to the Internet, resulting in 1 Mbps allocated to the voice queue and 5.5 Mbps allocated to the video queue (see Figure 6-15).

Figure 6-15 Small Branch Site Bandwidth Allocation Example



Based on the number of users and endpoints located at the small branch site, we made these additional assumptions about busy-hour calls and video endpoint utilization ratios:

- All the users may be involved in a call (voice or video) at the same time.
- All video endpoints can be involved in a call at the same time.

As a consequence, these are the numbers and types of calls that can be supported at the small branch site in this example:

- Voice queue: 1 Mbps; Supports 12 calls (80 kbps per call)
- Video queue: 5.5 Mbps
  - Video endpoints: 2 Mbps ∗ 2 calls = 4 Mbps
  - Webex Teams application video: 5.5 - 4 = 1.5 Mbps; Supports 1 call at 720p, 1 to 2 calls at 540p, or 3 calls at 360p

Provisioning Best Practices

In summary, the following best practices described in this section can prove helpful when provisioning bandwidth for you Webex Teams deployment:

- Prioritize audio and video traffic on all outgoing router interfaces to the Internet.
- Provision Internet links for the busy hour – that is, for the highest simultaneous usage during the day – in order to optimize the user experience.
- Consider the typical per-call bandwidth requirements shown in Table 6-3, and apply utilization ratios depending on user behavior and your business goals. As a general rule, personal endpoints and clients have a lower utilization ratio than conference room systems, but this can vary depending on the nature of the user and the industry.
- On an appropriately sized Internet link, you can start with this general rule for relative bandwidth allocation:
  - 10% for voice traffic
  - 55% for video traffic
  - At least 30% for default traffic
- When provisioning queues and Internet links, continuously monitor bandwidth utilization and endpoint usage, and adjust the overall capacity and bandwidth allocations as needed.

Enterprise QoS Policy Access and Internet Edge Policy

Ingress Classification Policy

The following example represents an ingress policy definition that classifies audio traffic to and from Webex Teams applications and endpoints as EF, and video traffic to and from Webex Teams applications and endpoints as AF42. Replace AF42 (DSCP 36) with AF41 (DSCP 34) if you are marking Webex Teams video as Prioritized Video. This policy can be applied anywhere in the network, ideally close to the edge of the network, such as the campus access layer and the Internet edge, and it aligns with the QoS policy of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*. This policy assumes all traffic goes to the cloud and no Video Mesh Nodes are deployed. Refer to the Video Mesh Node section for a configuration example with a Video Mesh Node.

```
! This section configures the ACLs to match the UDP port ranges for audio and video,
! both for ingress (endpoint-to-cloud) and egress (cloud-to-endpoint) traffic
ip access-list extended QOS_WEBEX_AUDIO
permit udp any range 52000 52099 any eq 5004
permit udp any eq 5004 any range 52000 52099
ip access-list extended QOS_WEBEX_VIDEO
permit udp any range 52100 52299 any eq 5004
permit udp any eq 5004 any range 52100 52299
! This section configures the classes that match on the ACLs above.
class-map match-any VOICE
match access-group name QOS_WEBEX_AUDIO
class-map match-any OPPORTUNISTIC_VIDEO
match access-group name QOS_WEBEX_VIDEO
```

```
! This section configures the policy-map matching the classes configured
! above and sets DSCP for voice and video on ingress on this switch/router.
! Note that the class-default sets everything that does not match the
! above to a DSCP of 0 (BE).
policy-map INGRESS_MARKING
class VOICE
set dscp ef
class PRIORITIZED_VIDEO
set dscp af41
class OPPORTUNISTIC_VIDEO
set dscp af42
class class-default
set dscp 0
! This section applies the policy-map to the interface.
Switch (config-if)# service-policy input INGRESS-MARKING
```

Note In the QoS policy for the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*, the class map for opportunistic video for Jabber endpoints was called JABBER_VIDEO. In the above example it has been renamed to OPPORTUNISTIC_VIDEO.

An alternative option for Cisco Catalyst 3650 and 3850 switches running Cisco IOS XE 16.6+ is to use NBAR2 to identify Webex Teams traffic as well as Webex Meetings App traffic. In this case IP ACLs are not required, and the class-maps simplify to:

```
class-map match-any VOICE
  match protocol cisco-spark-audio
class-map match-any OPPORTUNISTIC_VIDEO
  match protocol cisco-spark-video
```

Video Mesh Node

The following example presents an additional ingress policy definition (based on a Cisco IOS switch) that classifies traffic originated by a Webex Video Mesh Node as well as cascade traffic from the cloud to that Video Mesh Node. These access lists can be combined with those shown in the previous section.

```
! This section configures the ACLs to match the UDP port ranges for audio and video
! for the cascade link between a Video Mesh Node (HMN) with IP address 10.10.10.10
! and the cloud
ip access-list extended QOS_WEBEX_VMN_AUDIO
permit udp 10.10.10.10 range 52500 62999 any eq 5004
permit udp any eq 5004 10.10.10.10 range 52500 62999
ip access-list extended QOS_WEBEX_VMN_VIDEO
permit udp 10.10.10.10 range 63000 65500 any eq 5004
permit udp any eq 5004 10.10.10.10 range 63000 65500
! This section configures the classes that match on the ACLs above as well as
! the ACL's shown in section above "Ingress Classification Policy"
class-map match-any VOICE
match access-group name QOS_WEBEX_AUDIO
match access-group name QOS_WEBEX_VMN_AUDIO
class-map match-any OPOORTUNISTIC_VIDEO
match access-group name QOS_WEBEX_VIDEO
match access-group name QOS_WEBEX_VMN_VIDEO
```

Wireless Configuration

The following AireOS WLC software configuration creates an AVC profile to mark Webex Teams audio and video traffic to EF and AF41 respectively, and it applies this policy to a specific WLAN (WLAN 10 in this example).

```
! This section creates the AVC Profile
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE create

! This section configures AVC to mark Webex Teams voice applications/sub-components to EF
! (DSCP 46)
(Cisco WLC) > config avc profile AVC-PROFILE rule add application cisco-spark-audio mark 46

! This section configures AVC to mark Webex Teams video to AF42 (DSCP 36)
(Cisco WLC) > config avc profile AVC-PROFILE rule add application cisco-spark-video mark 36

! This section applies the Platinum QoS Profile to the WLAN
(Cisco WLC) > config wlan qos 10 platinum

! This section enables AVC Visibility on WLAN 10
(Cisco WLC) > config wlan avc 10 visibility enable

! This section applies the AVC Profile to WLAN ID 10
(Cisco WLC) > config wlan avc 10 profile AVC-PROFILE enable
```

Sizing Cisco Webex Hybrid Services

Revised: May 31, 2019

Sizing the components of the Preferred Architecture for Cisco Webex Hybrid Services is an important part of the overall solution design. As in the latest version of the Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments, this chapter contains simplified sizing recommendations based on a number of assumptions. It is important to note that the assumptions in this chapter change some of the simplified sizing assumptions for the on-premises deployment. Therefore, it is important to be aware of these changes in order to size the on-premises deployment correctly.

For products deployed with virtualization, sizing corresponds to the selection of the virtual machine (VM) hardware specification defined in the VM configuration or Open Virtual Archive (OVA) template and the number of virtual machines. For the products that are not deployed with virtualization, sizing corresponds to the type and number of appliances or blades.

Sizing can be a complex exercise because of numerous parameters to take into considerations. To simplify the sizing exercise, this chapter provides some sizing examples with corresponding assumptions. We refer to these sizing examples as simplified sizing deployments. If the requirements for your particular deployment are within the limits of those assumptions, then you can use the simplified sizing deployments in this document as a reference. If not, then you will need to perform the normal sizing calculations as described in the *Sizing* chapter in the latest version of the *Cisco Collaboration System Solution Reference Network Design (SRND)* guide and related product documentation available at https://www.cisco.com/go/srnd.

As mentioned, sizing the components of the Preferred Architecture for Webex Hybrid Services is very similar to that of the Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments. One main difference is the addition of the Webex Hybrid Services Connectors and Video Mesh Nodes. The Cisco Expressway-C and Expressway-E pairs in this chapter are sized to handle Webex Hybrid Services. The other main difference is that the average busy hour call attempts (BHCA) is assumed to be 3; average BHCA below 3 fits within these recommendations, but average BHCA over 3 would require the sizing to be modified accordingly. The goal of this document is to provide simplified sizing guidance for those components.

For a given deployment, the goal of the sizing process is to determine:

- The type of platform to use
- The specifications and number of instances to deploy for each Cisco Collaboration product

Cisco Unified CM Sizing

For the most part, the sizing of Cisco Unified Communications Manager (Unified CM) for Webex Hybrid Services does not change compared to the sizing of Unified CM in the Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments. The main differences are:

- The Jabber clients are replaced with Webex Teams applications.
- The sizing assumes that each user has 2 devices: one Webex Teams application and one SIP endpoint.
- The average BHCA is 3.

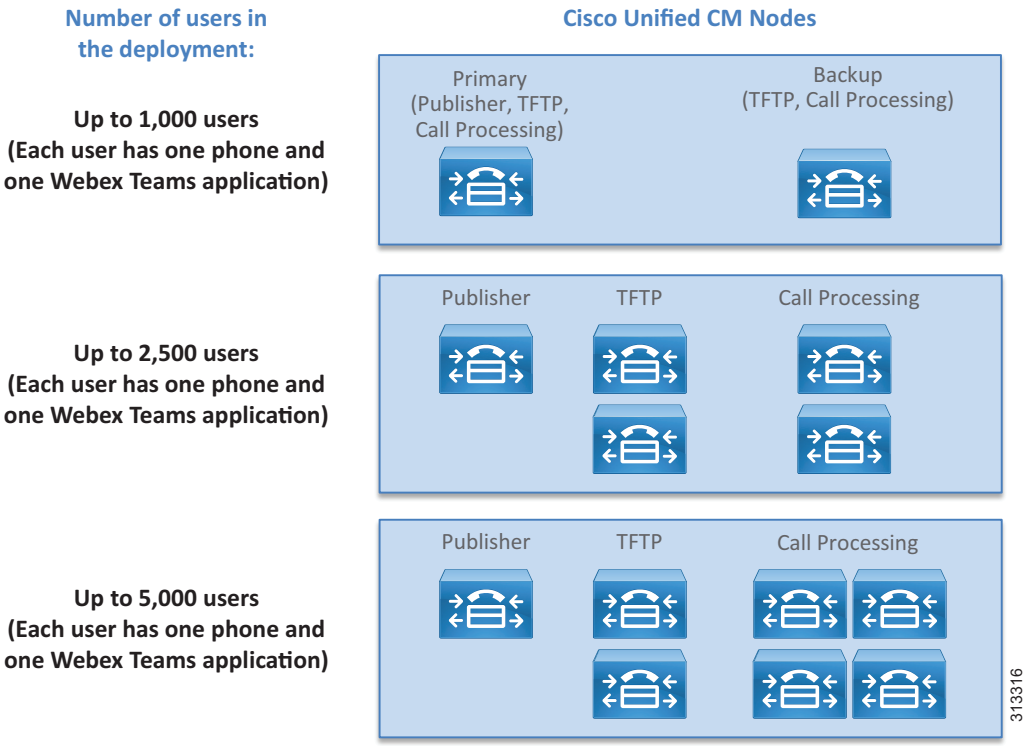
Other than the differences mentioned above, all other assumptions for the sizing of the on-premises deployment remain unchanged.

Table 7-1 and Figure 7-1 describe the simplified sizing deployments. For more details, refer to the latest version of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments, CVD*, available at https://www.cisco.com/go/pa.

Table 7-1 Cisco Unified CM Simplified Sizing Deployments

Deployment Size	Cisco Unified CM Nodes to be Deployed
Up to 1,000 users (2,000 devices)	2 nodes (1k-user VM configuration on Cisco Business Edition 6000H): • 1 primary node (publisher, TFTP, and call processing node) • 1 backup node (TFTP and call processing node)
Up to 2,500 users (5,000 devices)	5 nodes (7.5k-user VM configuration): • 1 publisher node • 2 TFTP node • 1 call processing pair (2 call processing subscriber nodes)
Up to 5,000 users (10,000 devices)	7 nodes (7.5k-user VM configuration): • 1 publisher node • 2 TFTP node • 2 call processing pairs (4 call processing subscriber nodes)

Figure 7-1 Cisco Unified CM Simplified Sizing Deployments



Webex Hybrid Services Connectors and Expressway Sizing

This section covers sizing Webex Hybrid Services connectors as well as the Expressway-C and Expressway-E sizing for Webex Hybrid Services. Expressway sizing with business-to-business and mobile and remote access (MRA) services is covered in the Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments CVD.

With Webex Hybrid Services, the Calendar and Call connectors are hosted on the Expressway-C servers. The Expressway-C and Expressway-E pairs are used for firewall traversal for SIP endpoints connecting to Webex. This occurs when a SIP endpoint is involved in a point-to-point call with a Webex Teams application or Webex device, or in a conference overflow scenario where the Webex Video Mesh cluster is full and a new SIP endpoint joins the conference. The Expressway-C and Expressway-E pairs are also used for the Call Service Aware and Call Service Connect services.

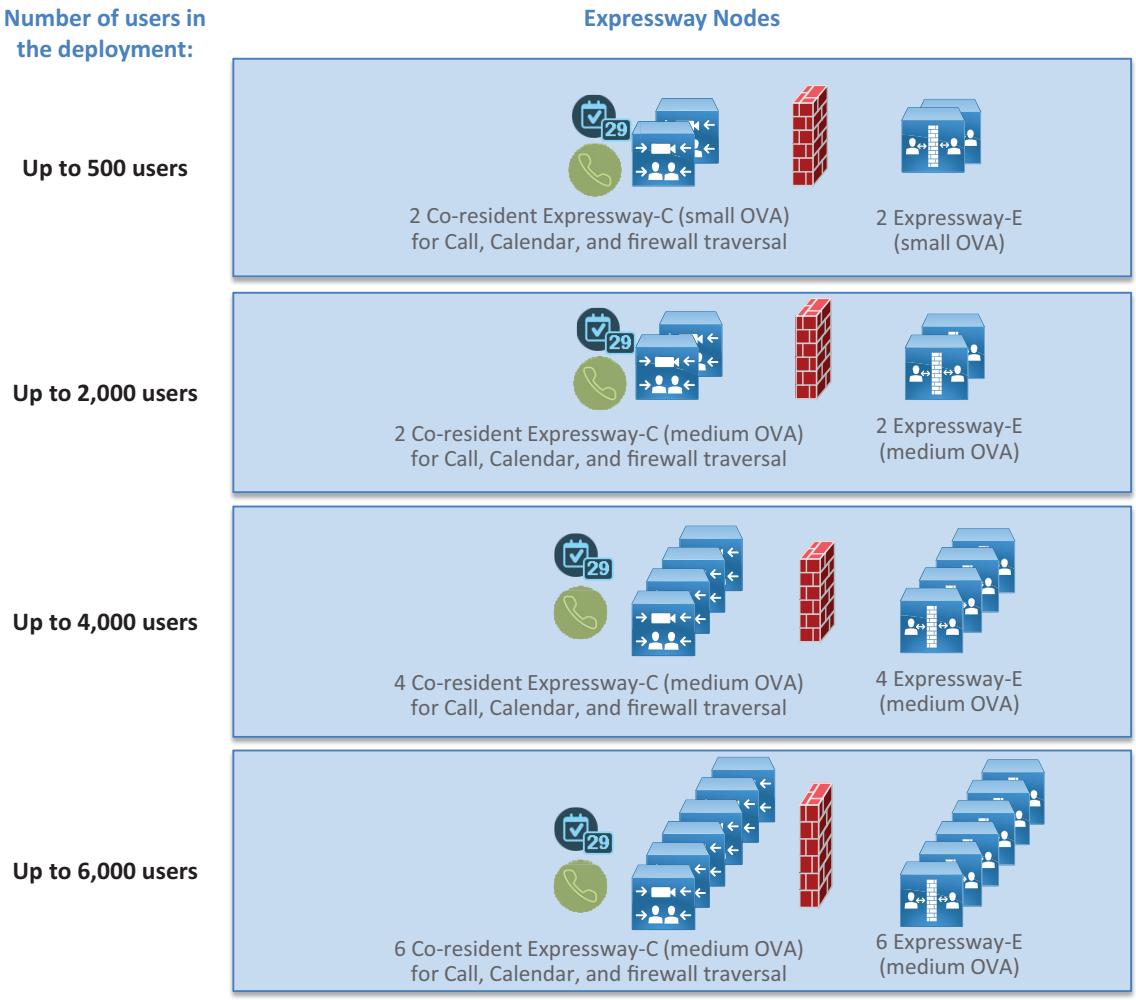
For simplicity, this section covers sizing for deployments where the Expressway-C servers are deployed with co-resident hosting of all three call, calendar, and firewall traversal services. This section does not cover sizing for configurations where there is a dedicated Expressway-C server for the call or calendar hybrid services. Moreover, the large Expressway VM configuration is also not considered in this section because it is not supported on Cisco Business Edition 6000 or 7000. If you are interested in other deployment and co-residency options, or in deployments leveraging the large Expressway VM configuration because you have a large deployment, refer to the information on *User Capacity Limits for Expressway-Based Hybrid Services* available at https://collaborationhelp.cisco.com/article/en-us/nv5p67g.

Table 7-2 and Figure 7-2 provide sizing guidance, with some assumptions that are listed below. As mentioned above, this information assumes that the large VM configuration, which is not supported on Cisco BE6000 or BE7000, is not used.

Table 7-2 Sizing for the Cisco Expressway Servers

Number of Users	Expressway-C and Expressway-E for Calendar, Call, and Firewall Traversal	Notes
Up to 500	2 Expressway-C and 2 Expressway-E (includes redundancy)	Requires Expressway small VM configuration and Cisco BE6000
Up to 2,000	2 Expressway-C and 2 Expressway-E (includes redundancy)	Requires medium VM configuration and Cisco BE7000
Up to 4,000	4 Expressway-C and 4 Expressway-E (includes redundancy)	Expressway medium VM configuration (for Cisco BE7000)
Up to 6,000	6 Expressway-C and 6 Expressway-E (includes redundancy)	Expressway medium VM configuration (for Cisco BE7000)

Figure 7-2 Sizing for the Webex Hybrid Services Connectors and Cisco Expressway



Assumptions

The following assumptions apply to the information in Table 7-2 and Figure 7-2.

- Microsoft Exchange is deployed on-premises.
- Mobile and remote access (MRA) and business-to-business services, if deployed, do not use the Expressway servers.
- Each user has 2 devices: one desk phone registered to Cisco Unified CM and one Webex Teams application.
- Each user makes an average of 3 busy hour call attempts (BHCA), with an average call hold time of 3 minutes.
- 50% of calls are on-network, 25% of calls are outgoing to the PSTN, and 25% of calls are incoming from the PSTN.
- The number of concurrent video calls and audio-only calls per Expressway server does not exceed the numbers in Table 7-3. In this table, the weight of video calls is effectively twice the weight of audio calls. For example, with a mix of audio and video calls, if there are 50 video calls, then the

remaining capacity for the audio calls is 100 audio calls. Note that this is not something that can be controlled, but it is a function of user calling, and it is important to understand for capacity considerations and for determining when more resources are necessary.

Table 7-3 Expressway Server Call Capacity

VM Configuration Template	Video Calls Capacity per Node	Audio-Only Calls Capacity per Node
Virtual machine with small or medium VM configuration or Cisco Expressway CE1100 Appliance with 1 Gb small form-factor pluggable (SFP) transceivers	100	200

Directory Connector Sizing

The Directory Connector is installed on a dedicated Windows Server and requires 8 GB of RAM. One CPU or vCPU is sufficient. For redundancy purposes, we recommend deploying two servers. For more details, refer to the latest version of the *Deployment Guide for Cisco Directory Connector*, available at

https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

Video Mesh Node Sizing

Webex Teams applications, Webex Teams endpoints, and SIP endpoints can connect to a local Webex Video Mesh Node during a conference, as described in the chapter on Cisco Webex Video Mesh. The sizing of the Video Mesh Nodes depends on the number of simultaneous calls going through the Video Mesh Nodes, the type of endpoints joining the conference, the video resolution on those endpoints, and the platform used for the Video Mesh Nodes.

For more information and for actual capacity limits, refer to the latest version of the *Deployment Guide for Cisco Webex Video Mesh*, available at

https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

When deploying Webex Video Mesh Nodes, we recommend monitoring the usage on those nodes via the Webex Control Hub. If more capacity is needed, you can add Video Mesh Nodes to the Webex Video Mesh cluster. Adding nodes to a cluster not only increases the capacity but also provides redundancy in case a single node becomes unavailable for any reason. There is no maximum limit to the number of nodes in a Video Mesh cluster.

As described in the chapter on Cisco Webex Video Mesh, if the Webex Video Mesh cluster becomes full, the meeting will cascade to the Webex cloud media services to handle the overflow. When this happens, Webex Teams applications and Webex devices joining the meeting will connect directly to the cloud, while SIP endpoints joining the meeting will connect to the cloud via an Expressway-C and Expressway-E pair. Again, monitor your system to understand how often this occurs and if this is acceptable to your users. If you want to reduce those occurrences of cascade links, add more Video Mesh Nodes as needed.

Virtual Machine Placement and Platforms

The virtual machine placement for this solution is similar to the one for the Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments. The main differences are:

- Deployment of Windows Servers for Cisco Directory Connector, and Expressway-C Connector Hosts for Cisco Calendar and Call Connector nodes
- Deployment of Expressway-C and Expressway-E nodes that handle Webex Hybrid Services calls
- Deployment of Webex Video Mesh Nodes on Cisco Meeting Server 1000

The virtual machine placement process is performed with the Collaboration Virtual Machine Placement Tool (VMPT), which requires a cisco.com login account and which is available at https://www.cisco.com/go/vmpt.

Figure 7-3 shows an example of using the VMPT for a deployment with 4,000 users and 8,000 endpoints (including 4,000 hardware endpoints and 4,000 Webex Teams applications). This example assumes that Cisco Business Edition 7000M is deployed. It does not show the Cisco Video Mesh Nodes, which would be deployed on the Cisco Meeting Server 1000 platform for this example.

Figure 7-3 Virtual Machine Placement Example Using the VMPT