Cisco Preferred Architecture for Webex Edge Audio

Design Overview

June 2021

Contents

Preface

Cisco Preferred Architectures provide recommended deployment models for specific market segments based on common use cases. They incorporate a subset of products from the Cisco Collaboration portfolio that is best suited for the targeted market segment and defined use cases. These deployment models are prescriptive, out-of-the-box, and built to scale with an organization as its business needs change. This prescriptive approach simplifies the integration of multiple system-level components and enables an organization to select the deployment model that best addresses its business needs.

Documentation for Cisco Preferred Architectures

- 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 details for deploying components within the Cisco Preferred Architectures. These guides support planning, deployment, and implementation (PDI).
- Cisco Collaboration Solution Reference Network Design (SRND) guide provides detailed design options for Cisco Collaboration. This guide should be referenced when design requirements are outside the scope of Cisco Preferred Architectures.

About This Guide

The *Cisco Preferred Architecture for Webex Edge Audio* is for:

- Sales teams that design and sell collaboration solutions
- Customers and sales teams who want to understand the Webex Edge Audio architecture, its components, and general design best practices.

Readers of this guide should have a general knowledge of Cisco Voice, Video, and Collaboration products and a basic understanding of how to deploy these products.

This guide simplifies the design and sales process by:

- Recommending products in the Cisco Collaboration portfolio that are built for the enterprise and that provide appropriate feature sets for this market
- Detailing a collaboration architecture and identifying general best practices for deploying in enterprise organizations

For detailed information about configuring, deploying, and implementing this architecture, consult the related CVD documents on the Cisco Collaboration Preferred Architectures.

Introduction

Webex Edge Audio is a solution where audio calls for Webex Meetings originating from the enterprise go through the company network to connect to the Webex cloud via the Internet or a dedicated Edge Connect circuit. Similarly, Webex Meetings audio callbacks route through the enterprise network to leverage the on-premises audio call control routing. This provides great cost savings for customers as it eliminates PSTN charges created by Webex attendees. At the same time, it provides users with all the benefits of high quality wide-band codecs that Webex offers for better audio quality.

Technology Use Cases

The Cisco Preferred Architecture (PA) for Webex Edge Audio delivers design capabilities that enable organizations to realize cost reduction by intelligently changing the call routing to a simple to deploy on-net path. It's a service that allows any company of any size that uses Cisco Unified Communications Manager (Unified CM) to intelligently and automatically route audio calls over VoIP or utilize existing PSTN services. Additionally, this use case details design considerations for:

- Dialing into Webex meetings from an enterprise registered endpoint
- Callback to an enterprise registered phone
- Customer owned numbers for calling into Webex
- Optimization of PSTN country callback usage

Benefits

Decreased PSTN costs

Webex Edge Audio provides savings across the collaboration deployment. Customers can leverage their existing Cisco Unified CM environment to manage their calls or can continue to use Webex PSTN or a cloud-connected audio provider. Enterprise administrators can control how they want to route audio callback from Webex (via internet or via PSTN) on a per country basis.

Security

Webex Edge Audio architecture protects access to the enterprise network and implements toll fraud protection mechanisms that can prevent unauthorized access to the telephony system

Enhanced Quality

For Cisco Unified CM registered devices, Webex Edge Audio creates an end-to-end voice over IP (VoIP) path, whether users are dialing in or requesting Webex callback. Enterprises can connect to Webex over internet or Webex Edge Connect providing all the benefits of G.722, G.711ulaw, G.711alaw high-quality codecs .

No change in user behavior

Webex Edge Audio lets participants automatically join a Webex meeting via a direct VoIP route to the Webex cloud or via their existing PSTN services, with no change in behavior.

Flexible on- and off-network deployment

Webex Edge Audio lets customers choose the on-network path in locations where they can save on PSTN costs. It also allows them to buy Webex PSTN minutes in locations where they do not have an on-premises or Unified CM deployment.

Available Services

- Webex Meetings
- Webex Event

- Webex Training
- Webex Support Center
- Webex Meetings for FedRAMP

Webex Edge Audio Components and Roles

The main elements, defined below, of the architecture include Endpoints, Call Control, Collaboration Edge, Webex Control Hub, Webex PSTN, Cloud Connected Audio Service Provider (CCA-SP) and Webex Edge Connect.

Endpoints: Collaboration room endpoints, IP phones and software clients use VoIP technologies for placing and transmitting calls over an IP network. In the context of Webex Edge Audio, the endpoint media traffic refers to audio traffic and does not include video or content sharing.

Call Control: Call control decodes addressing information and routes phone calls from one endpoint to another. It also handles supplementary features such as call hold/resume, three-way calling, call transfer and others. Cisco Unified CM is the core of Cisco's on-premises collaboration portfolio, and it delivers people-centric user and administrative experiences while supporting the full range of collaboration services including video, voice, instant messaging and presence, and mobility as well as third-party devices. In the context of Edge Audio, for call-in to Webex, SIP normalizations are performed to send the information Webex requires to route the call. For callback calls from Webex, Cisco Unified CM takes the call routing decision to route the call to an endpoint, to the PSTN or to reject the call.

Collaboration Edge: Collaboration Edge consists of Expressway(s) or CUBE(s) located at the perimeter of the network to deliver integrated calling experiences between the enterprise network and Webex.

> **Expressway**: Cisco Expressway Series (Expressway) is an advanced collaboration gateway used to extend services to users inside and outside your firewall. It establishes highly secure firewall-traversal technology and helps to redefine traditional enterprise collaboration boundaries. A typical Expressway system is deployed as a pair: an Expressway-C with a trunk and line-side connection to Unified CM, and an Expressway-E deployed in the DMZ and configured with a traversal zone to an Expressway-C. This document focuses on the Expressway trunk aspects and not lineside capabilities.
>
> **Cisco Unified Border Element (CUBE):** CUBE is an enterprise-class Session Border Controller (SBC) solution that links the enterprise networks with cloud collaboration services like Webex. As CUBE terminates and re-originates signaling and media traffic, it is able to provide a secure demarcation between internal and external services, while interworking signaling protocols and encoded media streams between them.

Webex Control Hub: Webex Control Hub is a web-based, intuitive, single-pane-of-glass management portal that enables provisioning, administration and management of Webex services.

Webex PSTN: Webex PSTN is a cloud-based Public Switched Telephone Network (PSTN) audio option from Webex. Webex Meetings Audio provides a broad coverage footprint with toll call-in, toll-free call-in, and call-me capabilities for local and global connections. The Webex meetings subscription requires a committed or uncommitted Webex PSTN plan for Edge Audio to be enabled.

Cloud Connected Audio Service Provider (**CCA-SP):** CCA-SP is a peering architecture where a connection is made between the PSTN Service Provider's data center and a Webex data center through a dedicated and direct IP connection.

Webex Edge Connect: Edge Connect is a dedicated, managed IP link from the customer premises to Webex, achieved through a direct peering over the Equinix Cloud Exchange (ECX).

Architecture

Webex Edge Audio is a solution that routes audio calls from the enterprise over the top (OTT) via the public internet or through Edge Connect to Webex. Webex Edge Audio decouples the PSTN from Webex by changing the call routing to make use of the customer's on-premises UC infrastructure. Enterprise administrators must provision the network infrastructure that is required to route the audio calls to and from Webex.

It is important to define the meaning of dial-in or call-in and callback.

Call-in is when a participant dials the phone number in the meeting invite to join the meeting audio. The call is initiated by the endpoint. Call-in or dial-in in this document have the same meaning and are used interchangeably.

Callback is when a participant requests Webex to call a phone number that the participant provides. The call is initiated by Webex.

Figure 1 illustrates a high-level overview of an enterprise UC infrastructure connecting to Webex. For call-in, an on-premises phone dials the Webex global access phone number in the meeting invite to get connected by audio. Signaling is routed via the on-premises call control device (Unified CM) whereas audio media is connected via the Webex PSTN connection between the Webex cloud, the PSTN GW and the on-premises phone. For off-net call-in, the cell phone's signaling, and media is routed to Webex Meetings audio service directly and does not use any of the on-premises UC infrastructure.

For Callback, the Webex cloud dials the on-premises phone to get connected by audio and the call routes through the PSTN Gateway. Signaling takes the call control path and media is routed between the phone and the PSTN gateway. For off-net callback the cell phone's signaling, and media is routed to Webex Meetings audio service directly and does not use any of the on-premises UC infrastructure.

Figure 1. High-level Overview of on-premises calls to and from Webex

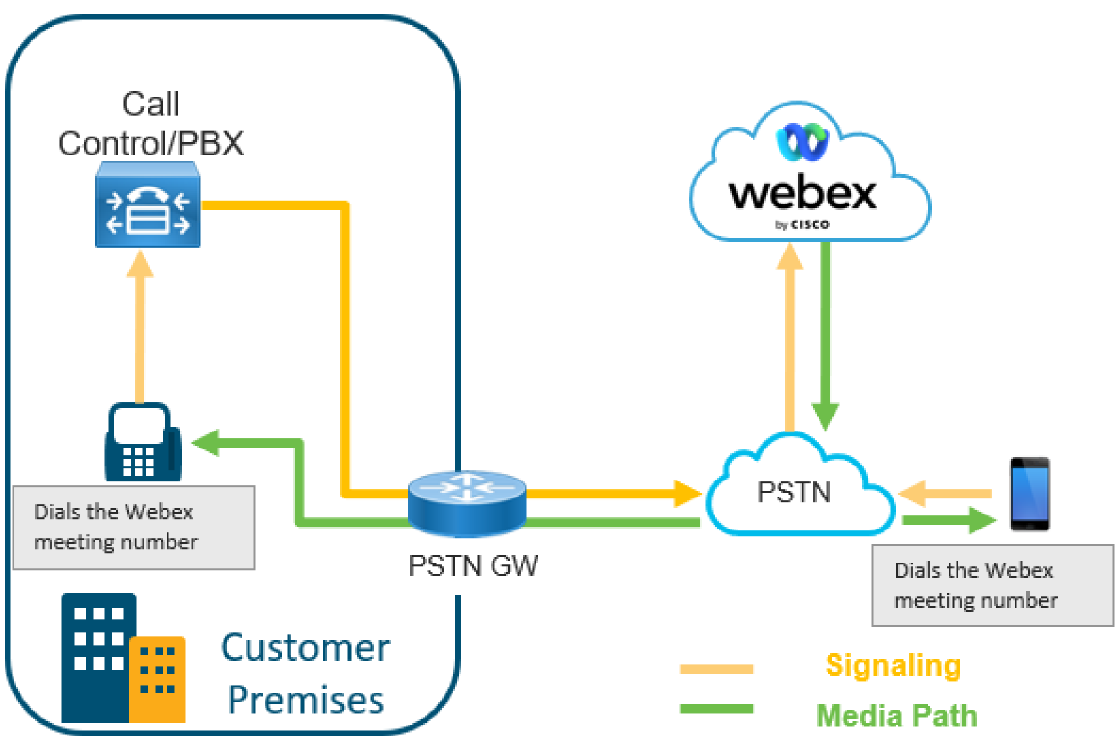
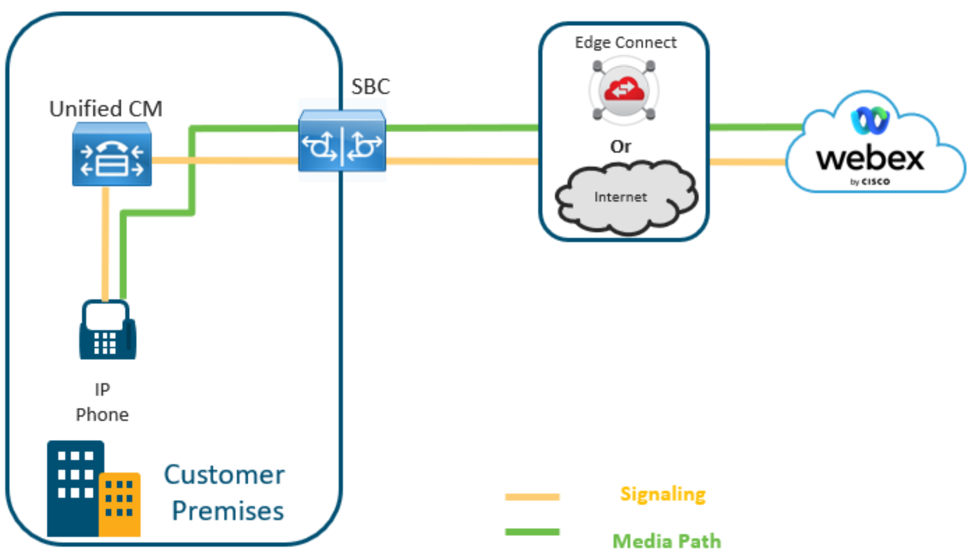


Figure 2 illustrates a high-level overview of Webex Edge Audio. A Session border controller or SBC is a network element that protects an enterprise network by acting as a demarcation point between a service provider network and the enterprise network. The SBC in Figure 2 represents the Cisco Expressway, CUBE or a third-party SBC. Figure 2 also shows that the connection from the enterprise to the Webex cloud can be through the internet or through a dedicated direct peering link, Edge Connect, to Webex.

When a user performs an audio call-in to Webex, the on-premises phone dials the Webex global access number to get connected into the meeting by audio. Signaling is routed via the on-premises call control system (Unified CM) through the SBC to the Webex Meetings audio service. Audio media is routed from the Webex meeting to the SBC and then to the on-premises phone and vice versa.

When a user performs an audio callback, the Webex cloud dials the on-premises phone to get connected by audio. The call routes through the SBC, the signaling takes the call control path via the Unified CM whereas media is routed directly between the phone and the SBC. For off-net callback, the cell phone signaling, and media is routed to Webex Meetings audio service directly and does not use any of the on-premises UC infrastructure. One of the main benefits of this architecture is to save on PSTN cost as the call path is over the top (OTT).

Figure 2. High-level Overview of Webex Edge Audio



The reference architecture in this document provides an end-to-end design for the Webex Edge Audio solution. This architecture solution is also supported for FedRAMP sites.

Webex Edge Audio Deployment Models

This section discusses the different traffic flow options for Webex Edge Audio. Cisco supports several different deployment models:

- Expressway-C and Expressway-E
- Expressway-E only with Edge Connect
- Cisco Unified Border Element (CUBE)
- Third party SBC
- Third party call control

When deploying any of the models referenced above, there is a common call-in and callback process that is followed.

These are the steps involved for the participant to join a meeting by call-in:

1. A user schedules a Webex meeting and Webex assigns a meeting ID (for example, 123456).
2. A user dials the phone number that is associated with the meeting (for example, 2403332200). The SIP INVITE carries the Request URI as the phone number associated to the meeting.
3. Unified CM translates the phone number to an access code using a SIP normalization Lua script. Lua is a powerful and fast programming language used in this case to modify the outbound SIP Invite message. This normalization script contains information to associate the call to the meeting site. The modified outbound SIP message is sent to the Collaboration Edge with the access code and site identifier, or universally unique identifier (UUID). Also, the hostname of the request URI is changed to the DNS SRV for a Webex region. Collaboration Edge resolves the SRV record and performs firewall traversal functions or a translation from an internal network to an external network facing Webex.
4. Webex receives the SIP INVITE and answers the call.
5. A user enters the meeting ID (for example, 123456) using DTMF, Webex verifies the access credentials and then lets the user join the meeting.

The following are the steps involved for the participant to join a meeting using the callback method:

1. A user schedules a Webex meeting and Webex assigns a meeting ID (for example, 123456).
2. A user requests a call from Webex to their desired +E.164 (international public telecommunication numbering plan with + sign) number to join the meeting using the Webex App or Webex Meeting client.
3. Webex initiates a SIP INVITE to the Collaboration Edge infrastructure based on the callback DNS SRV record provisioned in Control Hub. The SIP INVITE Request URI contains the phone number that must receive the call and is sent to Collaboration Edge for firewall traversal and SIP interworking towards the enterprise network. A call routing decision is made to send the call to Unified CM.
4. Unified CM checks the SIP INVITE to make a call routing decision to deliver the call to an endpoint, to the PSTN, or to reject the call.

Expressway-C and Expressway-E

Figure 3 illustrates the Expressway-C and Expressway-E deployment model. This deployment option utilizes the Internet or Edge Connect for connectivity to Webex. Cisco recommends having a dedicated Expressway-C and Expressway-E cluster for Edge Audio. This dedicated Expressway-C and Expressway-E cluster can have 1 to 6 nodes in the cluster.

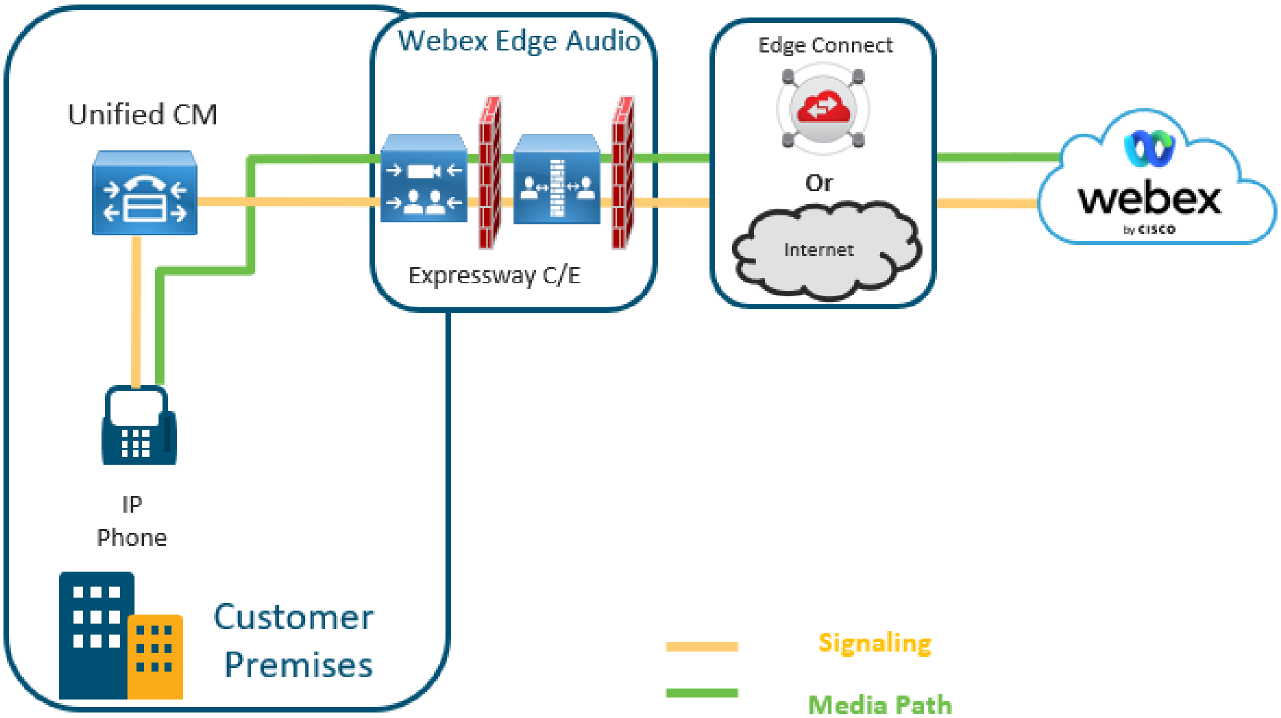
For customers with low Edge Audio call volume a shared model with other services can be deployed. When sharing Expressway with other services, the recommendation is to have dedicated Edge Audio zones between Expressway-C and Expressway-E and towards Unified CM. In this architecture there is not a dedicated call volume capacity calculation through the Expressways as the CPU is shared with all other services.

Cisco recommends a dedicated SIP trunk from Unified CM to Expressway-C as this simplifies troubleshooting in case of any issues.

When deploying an Expressway-C and Expressway-E for Edge Audio, Expressway Rich Media Session (RMS) licenses are not required. The RMS licenses are required for Business to Business calling but in the case of Webex Edge Audio the licenses are not consumed.

For configuration details check the following configuration guide https://help.webex.com/en-us/xmsy7d/Cisco-Webex-Edge-Audio-Customer-Configuration-Guide

Figure 3. Expressway-C and Expressway-E deployment model



Expressway-E Only with Edge Connect

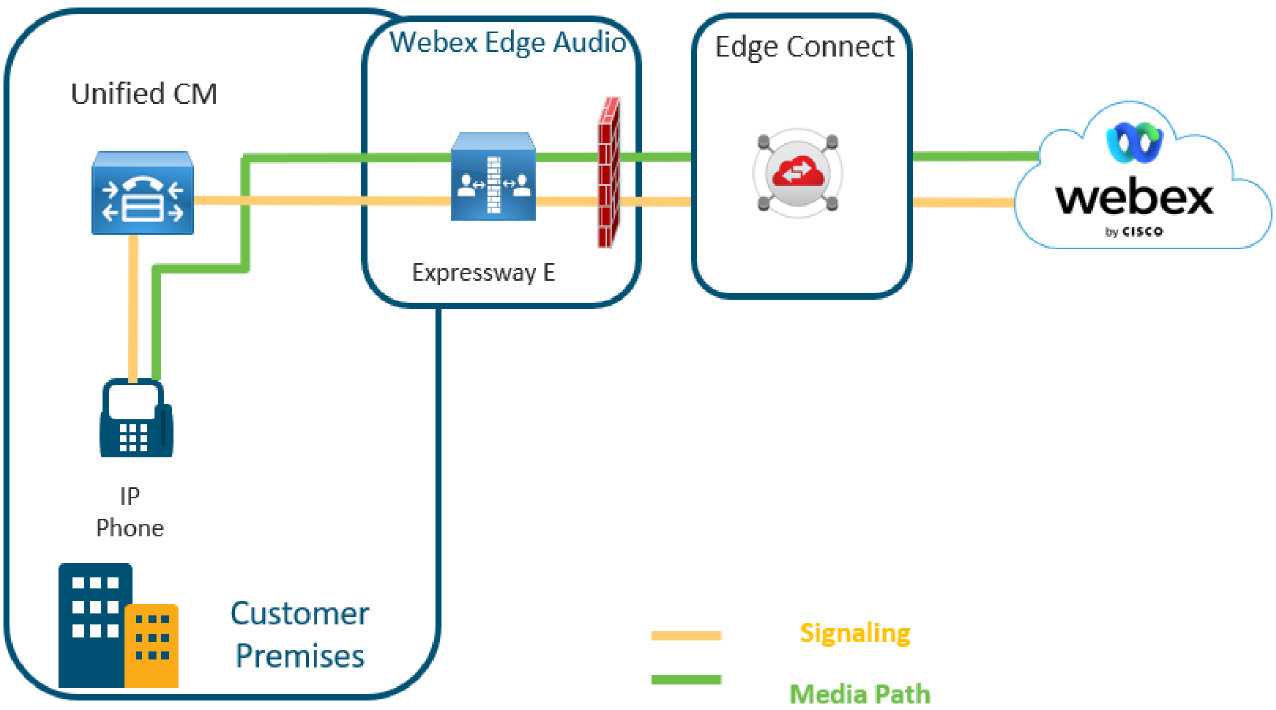
Figure 4 illustrates the Expressway-E only with Edge Connect deployment model. This deployment option requires Edge Connect which allows a dedicated, managed, QoS-supported IP link from the customer premises to Webex, achieved through direct peering over Equinix Cloud Exchange (ECX).

One advantage of deploying the Expressway-E only with Edge Connect architecture is that the computer and data center cost reduction gained by not deploying Expressway-C. This deployment model does not require Expressway Rich Media Session (RMS) licenses. RMS licenses are required for Business to Business calling but in the case of Webex Edge Audio the licenses are not consumed.

Since Edge Connect is a dedicated direct path to Webex, this is viewed as a trusted link between the customer edge and Webex, therefore the full firewall traversal connection is not required.

For configuration details check the following configuration guide: https://help.webex.com/en-us/o02v0i/Cisco-Webex-Edge-Audio-for-Only-Expressway-E-Customer-Configuration-Guide

Figure 4. Expressway-E only deployment model



Cisco Unified Border Element (CUBE)

Figure 5 illustrates the Edge Audio CUBE deployment model. This deployment option can use the Internet or Edge Connect to connect to Webex. Cisco recommends having a dedicated CUBE for Webex Edge Audio for simplicity of troubleshooting. In addition, there is no sizing guidance for multiple call flows collocated with one CUBE instance.

One of the main advantages of CUBE is support for high availability. The details are covered in the High Availability and Redundancy section.

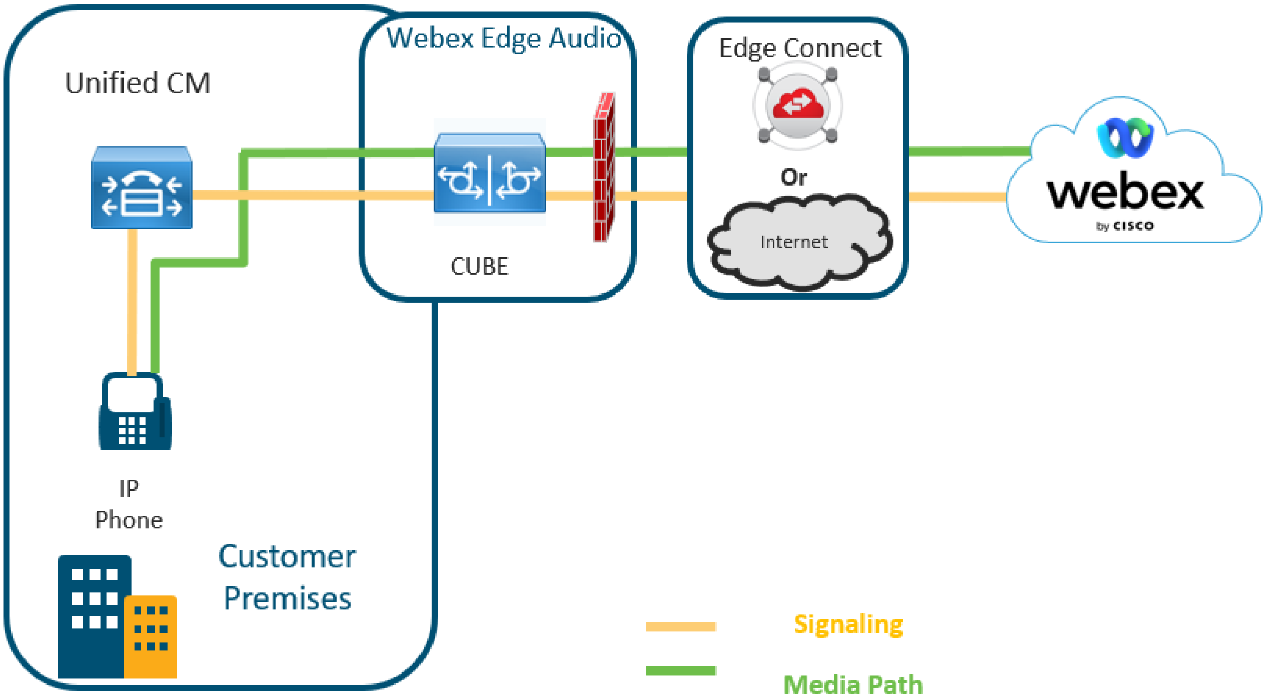
When deploying CUBE versus the Expressway models, CUBE requires additional licenses as opposed to the Expressways because in CUBE every SIP end-to-end call requires a CUBE license. The CUBE license can be a standard or enhanced license where the enhance license can be used for CUBE HA deployments. CUBE uses Smart Licensing to report the peak number of concurrent SIP calls across all Edge Audio CUBEs at any given time. In the event the number of licenses reported by CUBE exceeds the number of licenses in the smart account, the administrator will receive an out of compliance notification in the smart licensing portal. In this out of license scenario the extra calls traversing the CUBE will not be dropped.

CUBE Smart Licenses may be pooled across many devices and there is not a limit to the quantity of licenses that may be ordered. When sizing CUBE for Edge Audio, ensure that the call processing capacity of the chosen platform(s) can accommodate the maximum number of concurrent sessions required in addition to some capacity for growth.

For more details about licensing please check https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-cisco-smart-licensing.html

For Webex Edge audio deployment configuration details check the following configuration guide https://help.webex.com/en-us/b6vrdc/Cisco-Webex-Edge-Audio-for-CUBE-Customer-Configuration-Guide

Figure 5. CUBE deployment model



Third party Session Border Controller (SBC)

Figure 6 illustrates the third-party SBC deployment model. This deployment option works with Internet or Edge Connect. When deploying this model, it is the customer's responsibility to test and verify the solution end-to-end. Cisco provides an overall test plan to validate functionality with Edge Audio and the third-party SBC. The customer needs to make sure all tests pass in their testing before installing Edge Audio with a third-party SBC solution.

The third-party SBC deployment model requires SBC licenses, and it fragments the end-to-end solution support by adding a non-Cisco device in the call flow. Cisco TAC will not be able to assist with the SBC portion of the call flow in case of any troubleshooting effort requirements.

The solution test plan can be shared with Product Management approval. Please contact your local Cisco Account team for additional details.

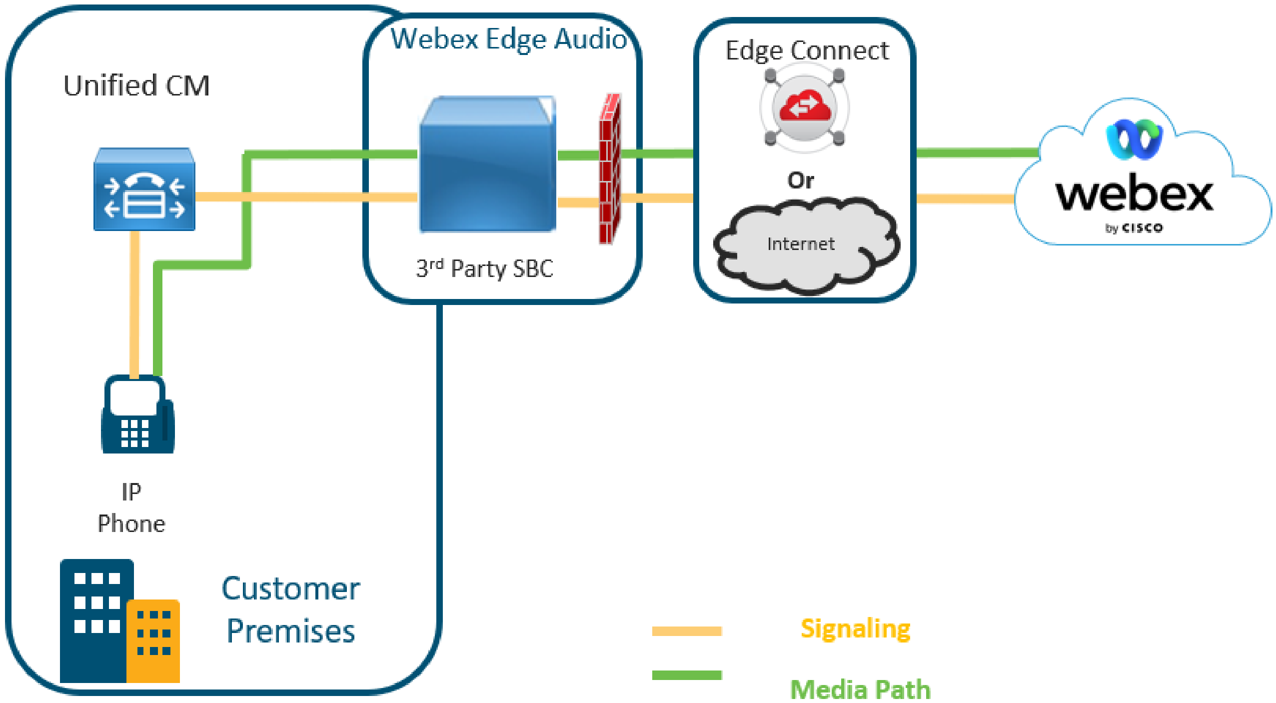


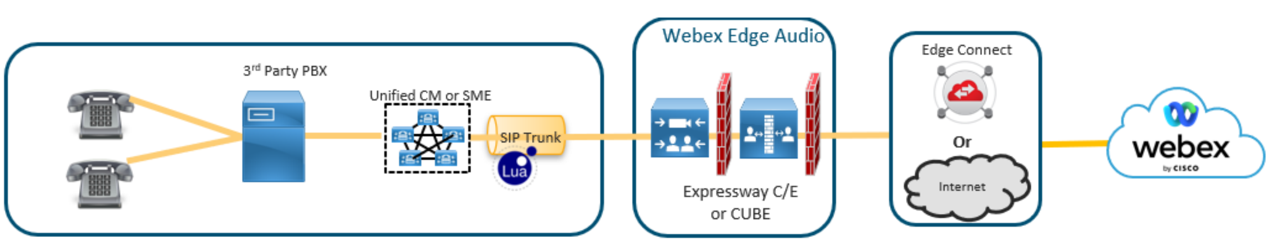
Figure 6. Third party SBC deployment model

Third party Call Control

Figure 7 illustrates the third-party call control deployment model. In this model a 3rd party call control system such as an IP PBX provides line side capabilities to IP phones used by the organization. To utilize Webex Edge Audio, a Unified CM or Unified CM Session Management Edition (SME) is required to have a SIP trunk to the IP PBX to provide connectivity to the IP PBX IP devices. Additionally, a SIP trunk to the Collaboration Edge applies the Lua script to provide the signaling information needed by Webex to process the call. From the Collaboration Edge perspective, the deployment is the same as the Expressway-C and Expressway-E or CUBE deployment model.

This deployment model works with either the Internet or Edge Connect as connectivity options to the Webex Cloud.

Figure 7. Third-party call control deployment model



Webex Edge Audio Design Considerations

This section includes details about capacity planning for Webex Edge Audio including how to determine the maximum concurrent number of calls for the Collaboration Edge. This section also covers sizing considerations for Expressways, CUBEs and Edge Connect.

Capacity planning

Sizing CUBE or Expressways for Edge Audio is an important part of the overall solution design. For products deployed with virtualization like Expressway and vCUBE, 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. CUBE and Expressway can be deployed as a VM or also as a dedicated hardware platform. For the Expressway installation details please check the Cisco Expressway on Virtual Machine Installation Guide. For vCUBE installation details please check the Cisco CSR 1000v Software Configuration Guide or the Cisco Catalyst 8000V Edge Software Installation Guide.

Ensuring that enough capacity is available for all the active participants during busy hours and ensuring that there is enough capacity for growth can be a daunting task. In order to simplify this task, Cisco recommends calculating the number of active meeting participants (equivalent to active calls in this example) based on current usage values (monthly meeting minutes).

Determining Active Participants (Active Calls)

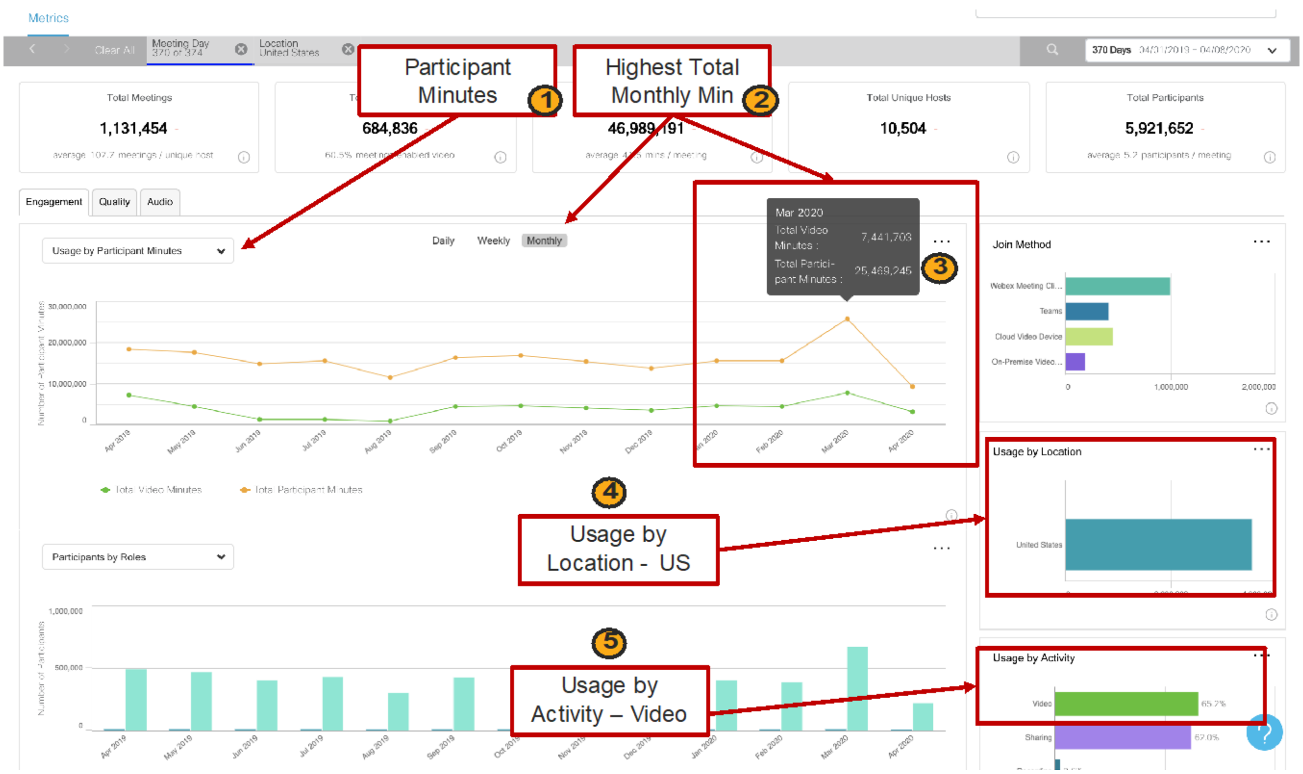
A validated method to determine the value of concurrent or active calls is to use the monthly participant minutes recorded in Webex Control Hub Analytics and divide that by a port efficiency value. A port in this case is equivalent to an active call. A port efficiency value is a value that can help determine the number of potentially active calls based on monthly participant minutes. This means the administrator can garner an understanding of the probability of the active connections required during the busy hour based on the number of participant minutes used whereby so many participant minutes equals a port and thus a required active connection. Based on data from existing customers with reasonable port efficiencies (that is utilization rates based on resources allocated) the port efficiency value is estimated between 500 and 8500 minutes per port. This is dependent on a range of monthly participant minutes because as systems become larger (more active calls), they become more efficient and thus the port efficiency value grows as a result. See Figure 9 below for the port efficiency values used in the calculation.

Sizing summary:

1. Determine the “monthly participant minutes”
2. Locate where that fits in the monthly minutes range to get a “port efficiency value”
3. Divide “monthly participant minutes” by the “port efficiency value” to calculate active calls (“monthly participant minutes” / “port efficiency value” = “active calls”)
4. Once the number of active calls is determined we can start calculating the approximate number of concurrent Edge audio calls

The first step is to verify the maximum number of participant minutes per month in Webex Control Hub Analytics (Figure 8 - 1-5). In Webex Control Hub Analytics viewing the “Usage by Participant Minutes” (Figure 8 - 1) over a 12-month period (Figure 8 - 2) is an easy method to determine the highest usage of participant minutes during any given month (Figure 8 - 3). Ensure that the location is appropriate, for example if sizing for a “United States”, you’d only want to include the “United States” under “Usage by Location” (Figure 8 - 4) if that was appropriate for the traffic envisioned over the Edge Audio.

Figure 8. Example of Monthly Participant Meeting Minutes in Webex Control Hub Analytics



The next step is to calculate the active calls by taking the value “monthly participant minutes” (Figure 8 - 3) and dividing it by the “port efficiency value” equivalent to the range in which the monthly minutes occur. Table 1 shows the recommended values:

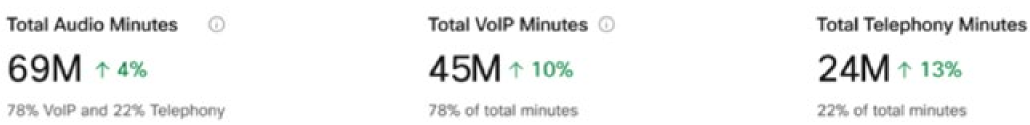
Table 1. Monthly minutes range to port efficiency calculation value

Monthly Minutes	Port Efficiency Value
0k – 50k	Monthly Minutes / 500
50k – 500k	Monthly Minutes / 1,000
500k – 1m	Monthly Minutes / 2,000
1m – 2m	Monthly Minutes / 3,000
2m – 8m	Monthly Minutes / 4,000
8m – 15m	Monthly Minutes / 5,700
15m - 30m	Monthly Minutes / 6,500
30m - 40m	Monthly Minutes / 7,000
40m – 100m	Monthly Minutes / 7,500
>100m	Monthly Minutes / 8,500

So, for example if the maximum participant minutes for a given month are 25.5 million, they would fall into the category of Monthly Minutes / 6500 calculation. So, 25,500,000 / 6,500 = 3,923 active connections. We can also round this up to

3,950 active connections to simplify and over-provision. Then the administrator needs to identify the percentage of calls that are telephony (PSTN) instead of VoIP, for this the administrator can review the Control Hub Audio Analytics Key Performance Indicators (KPI) shown in Figure 9. This shows percentage of meetings that use telephony audio.

Figure 9. Control Hub Audio Analytics KPIs



For this example, the total number of concurrent calls would be 22% of 3,950 which is a total of 869. If the number is higher than 800, the design will potentially require multiple medium and/or large Expressway OVAs. It is recommended to understand the global distribution of usage to identify where and how many OVAs are required. If you need assistance to determine global distribution of meeting usage, please engage your Cisco Account team and/or Cisco Customer Success Manager (CSM).

Expressway Capacity

Cisco recommends having a dedicated Collaboration Edge (Expressway or CUBE) for Webex Edge Audio. The primary way to determine sizing for the Edge devices is by determining the number of simultaneous voice-only calls. Table 2 shows the recommended amount of concurrent Edge Audio calls that an Expressway cluster can process simultaneously. With a cluster of 2 or 3 nodes, one node can fail without impacting the cluster capacity. With a cluster of 6 nodes, two nodes can fail without impacting the cluster capacity. For details about Expressway clustering, please review the Expressway sizing section of the On-Premises Deployments Preferred Architecture.

When deploying Edge Audio is recommended to size the Expressway clusters based on peak load and regional traffic. For global customers, the recommendation is to have an Expressway cluster per geographic region, for example one cluster in the Americas, one cluster in Europe, and one cluster in the Asian region.

Table 2. Webex Edge Audio Expressway Voice-Only Call Capacity

Nodes in an Expressway-C and Expressway-E cluster	Medium Expressway	Large Expressway
1	300	1,000
2	600	2,000
3	900	3,000
4	1,200	4,000
5	1,200	4,000
6	1,200	4,000

For Expressway installation details review this document
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/install_guide/X14-0/virtual-machine/exwy_b_cisco-expressway-on-virtual-machine-installation-guide-x14-0/exwy_b_vm-install-guide_chapter_010.html

Cisco Unified Border Element (CUBE) Capacity

Table 3 shows the recommended amount of concurrent Edge Audio calls with RTP to SRTP interworking a CUBE can support along with the number of calls per second (CPS). In a call overload situation where the number of calls exceeds the CUBE capacity, Cisco recommends configuring Call Admission Control (CAC) on the individual CUBEs.

Table 3. CUBE Call Capacity

Platform	Encrypted Audio calls w/SHA1_80 sRTP(G711)-RTP(G711)	CPS
4331 (4 GB)	600	3
4351 (4 GB)	750	4
4431 (8 GB)	750	4
4451 (8 GB)	2100 (16.12.2)	11
4461 (8 GB)	5400 (17.3.1)	30
C8300-1N1S-6T (8 GB)	1600 (17.3.2)	9
C8300-2N2S-6T (8 GB)	1800 (17.3.2)	10
C8300-1N1S-4T2X (8 GB)	2100 (17.3.2)	12
C8300-2N2S-4T2X (16 GB)	4300 (17.3.2)	24
CSR1Kv - 2 vCPU (4 GB)	1000	6
CSR8Kv - 2 vCPU (4 GB)	1000	6
ASR1001-X (16 GB)	2700	13
ASR1002-X (16 GB)	6500	36
ASR1004/6/6-X RP2/ESP40 (16 GB)	3500	20

Edge Connect

Cisco recommends deploying Edge Audio over Edge Connect for better quality audio calls if the customer has more than 250 maximum concurrent active calls. For Webex Edge Connect design considerations, please review the Webex Edge Connect Preferred Architecture for Webex Meetings design document.

Security considerations

This section includes security consideration for Edge Audio deployments including firewall requirements and certificate requirements for Expressway, CUBE, Unified CM configuration follow by the Secure Edge for Callback feature in Webex Control Hub.

Firewall requirements

For a successful Webex Edge Audio deployment, the network administrator, the firewall and proxy security administrators need to allow Webex Edge Audio signaling and media flow through the proxy and firewalls to prevent signaling and media problems. Table 4 shows the TCP and UDP ports required for Webex Edge audio, including the direction of the traffic.

Cisco recommends reviewing the document for the latest ports and IP addresses required for Webex Edge Audio connectivity as the requirements do change from time to time with the expansion and enhancements of the Edge Audio service**:**

Table 4. Ports required for Webex Edge Audio

Source	Source Ports	Destination	Destination Ports	Protocol	Description
Webex	Ephemeral	Expressway	5061, 5062	TCP	mTLS 1.2 Inbound SIP signaling for Webex Edge Audio.
Expressway	Ephemeral	Webex	5061, 5065	TCP	mTLS 1.2 Outbound SIP signaling for Webex Edge Audio.
Webex	Ephemeral	Expressway	8000-59999	UDP	SRTP Firewall pinholes need to be opened up for incoming media traffic to Edge audio.
Expressway	8000-59999	Webex	8000-59999	UDP	SRTP Firewall pinholes need to be opened up for outgoing media traffic to CUBE.
Webex	Ephemeral	CUBE	5061	TCP	mTLS 1.2 Inbound SIP signaling for Webex Edge Audio.
CUBE	Ephemeral	Webex	5061, 5065	TCP	mTLS 1.2 Outbound SIP signaling for Webex Edge Audio.
Webex	Ephemeral	CUBE	8000-48198	UDP	SRTP Firewall pinholes need to be opened up for incoming media traffic to Edge audio.
CUBE	8000-48198	Webex	Ephemeral	UDP	SRTP Firewall pinholes need to be opened up for outgoing media traffic to CUBE.

Expressway Certificates

The Expressway uses its signed server certificate which can be validated by communicating devices to verify that the Expressway node is the device it says it is. This can be used with neighboring devices such as Webex or Unified CM, as well as administrators using the web interface.

A certificate identifies the Expressway. It contains names by which it is known and to which traffic is routed. If the Expressway is known by multiple names for these purposes, such as if it is part of a cluster, this must be represented in the X.509 subject data, according to the guidance of RFC5922. The certificate must contain the FQDN of both the Expressway and of the cluster. The following lists show what must be included in the X.509 subject, depending on the deployment model chosen.

If the Expressway is not clustered:

- Subject Common Name = FQDN of the Expressway
- Subject Alternate Names = leave blank

If the Expressway is clustered, with individual certificates per Expressway:

- Subject Common Name = FQDN of the cluster
- Subject Alternate Name = FQDN of the Expressway peer and the FQDN of cluster

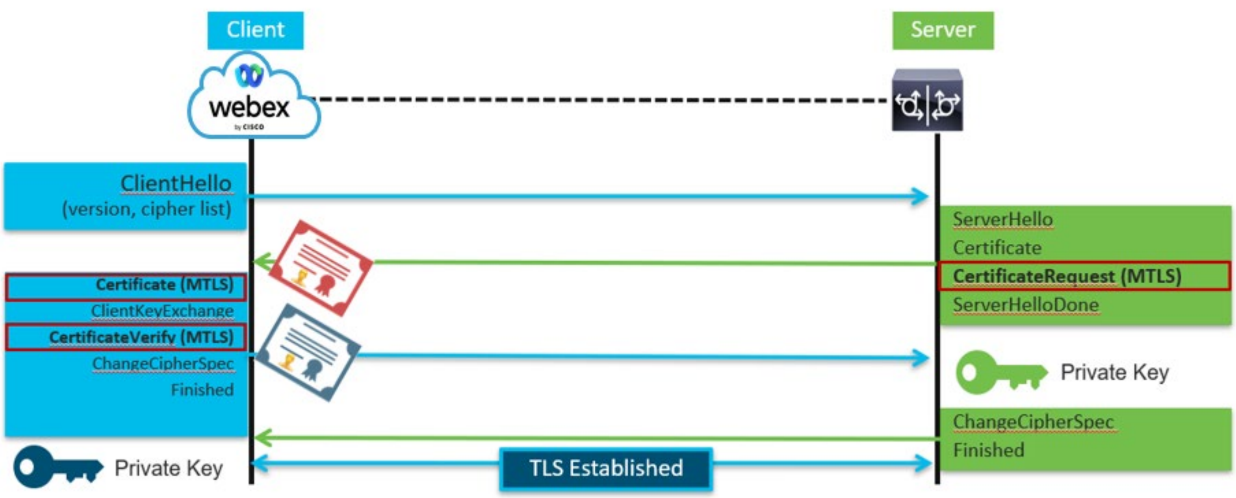
Wildcard certificates manage multiple subdomains and the services names they support. They can be less secure than Subject Alternat Name (SAN) certificates and are not supported by the Expressway.

The administrator can manage the Expressway's server certificate through the Server certificate page (Maintenance > Security > Server certificate). This certificate is used to identify the Expressway when it communicates with client systems using TLS encryption,

Webex Edge Audio uses mutual transport layer security (MTLS) version 1.2 for authentication between Webex and the Expressway-E. This means that both Collaboration Edge and Webex will check and inspect the certificates exchanged. For MTLS connections to establish, Edge Audio, Expressway-E, or CUBE must offer a signed certificate from a trusted certificate authority CA. The administrator can find the list of Root Certificate Authorities supported by Webex here.

For SIP connections from Webex to the enterprise Expressway, Webex acts as the client side and Expressway-E as the server side. With MTLS, both Webex and the Expressway-E authenticate each other based on certificates. There is a verification of the Common Name (CN) or the Subject Alternative Names (SANs) of the certificate presented by Webex to the Expressway-E during TLS handshake. Successful authentication also requires that trust is established with the CA that signed this certificate. Webex checks if domain in the CN or SAN of the certificate matches the DNS SRV domain configured in the Callback DNS SRV in Webex Control Hub. After these two conditions are satisfied, the connection is allowed. If authentication is not successful, this means that the certificate validation has failed. Figure 10 shows an expected MTLS session establishment from Webex to the Edge.

Figure 10. MTLS session establishment.



Two types of certificates must be present in the trusted CA list on your Cisco Expressway-E to complete the secure calling configuration:

- The root certificate (and intermediate certificate, if applicable) of the public CA that the administrator used to sign your SSL server certificate.
- The certificates of the public CAs used by the Webex cloud.

To obtain these certificates, copy and paste the contents of each of the following certificates into a separate text file with a PEM extension:

- QuoVadis Root CA 2
- IdenTrust Commercial Root CA certificate
- HydrantID SSL ICA G2

For detailed instructions on configuring the trusted CA list, see the applicable guide:

Cisco Expressway Certificate Creation and Use Deployment Guide

Expressway Webex Edge Audio configuration guide

Cisco Unified Border Element (CUBE) Certificates

Edge Audio requires that CUBE import the IdenTrust Commercial Root CA certificate. This certificate is used during the TLS handshake. When Webex sends its certificate, CUBE will validate it against the list of certificates available in the trustpool. Trustpool certificates are well-known CA certificates with which trust can be established. IOS PKI has both built-in CAs and also has an option to download a trustpool bundle.

The trustpool bundle must be updated with the Cisco Root CA by downloading the latest "Cisco Trusted Core Root Bundle" from http://www.cisco.com/security/pki/ using the command:

```
crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_core.p7b
```

CUBE MTLS supports wildcard certificate which means that the subject-name is generic (e.g. *.example.com). Wildcard certificates are helpful especially in CUBE HA deployments where the same certificate could be used for the active and standby CUBEs.

Cisco Unified CM Certificates

The connection from Unified CM to Expressway does not require mixed mode to be enabled on the cluster because Unified CM negotiates non-encrypted RTP media traffic to Expressway-C which terminates the endpoint RTP connection. Any time the Expressway performs RTP-to-SRTP conversion, it engages a back-to-back user agent (B2BUA), Cisco recommends enabling force encryption on Expressway-C instead of Expressway-E so that the traffic in the DMZ is encrypted.

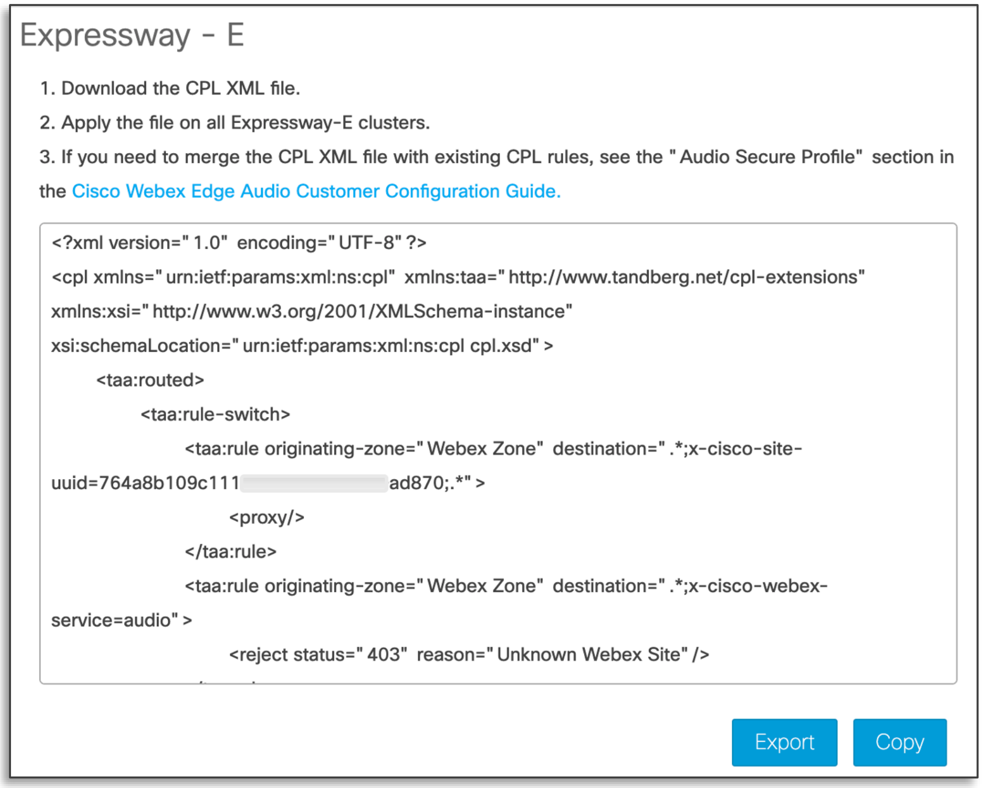
Callback Secure Edge

Webex Edge Audio provides the administrator with the ability to accept calls from only the sites the enterprise owns. It can reject any call from Webex if the originating site is not recognized. The enterprise edge identifies the call based on the "x-cisco-site-" parameter added to the request URI coming from Webex. In case of UUID mismatch, calls are rejected with SIP "403 Unknown Webex Site". Cisco recommends using the Secure Edge feature for added security in Webex Edge Audio.

Within Webex Control Hub, the administrator can click on the "Secure Edge" button under Audio Settings to download the CPL XML file. The CPL XML file needs to be applied into the enterprise edge (Expressway) to secure their enterprise from spurious calls and to allow or reject calls from the Default Zone. If there is an existing file, configuration can be added manually to merge the information into a single file. The CPL should be added to all the Expressway-E servers within the enterprise that are resolved in the callback SRV record in DNS for Edge Audio.

An example CPL file is shown in figure 11.

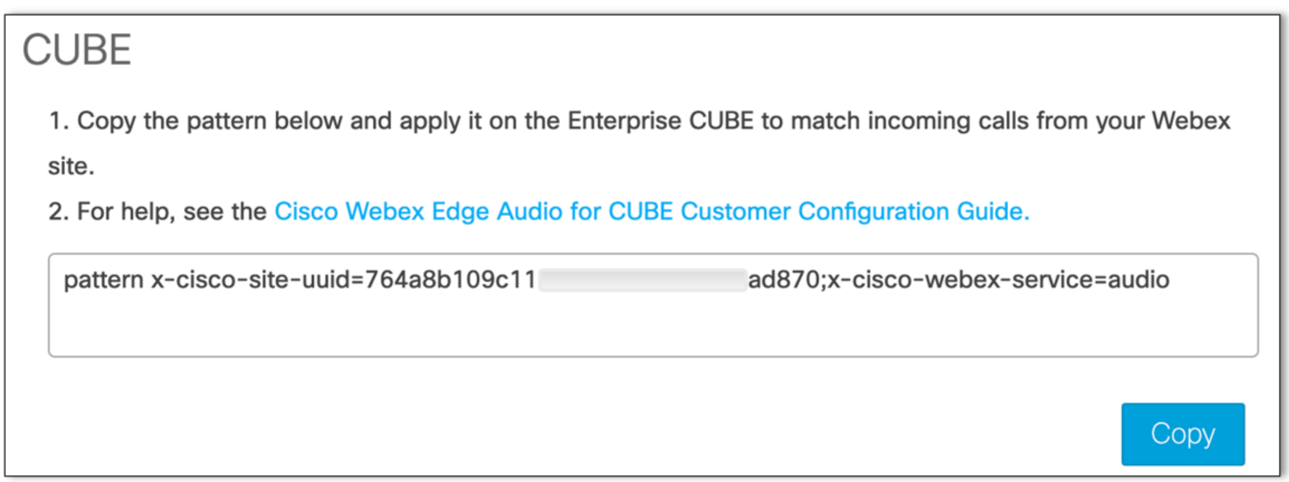
Figure 11. Example CPL file



From the Control Hub "Audio Secure Profile" page, the administrator can also download the CUBE configuration required to implement the Secure Edge feature.

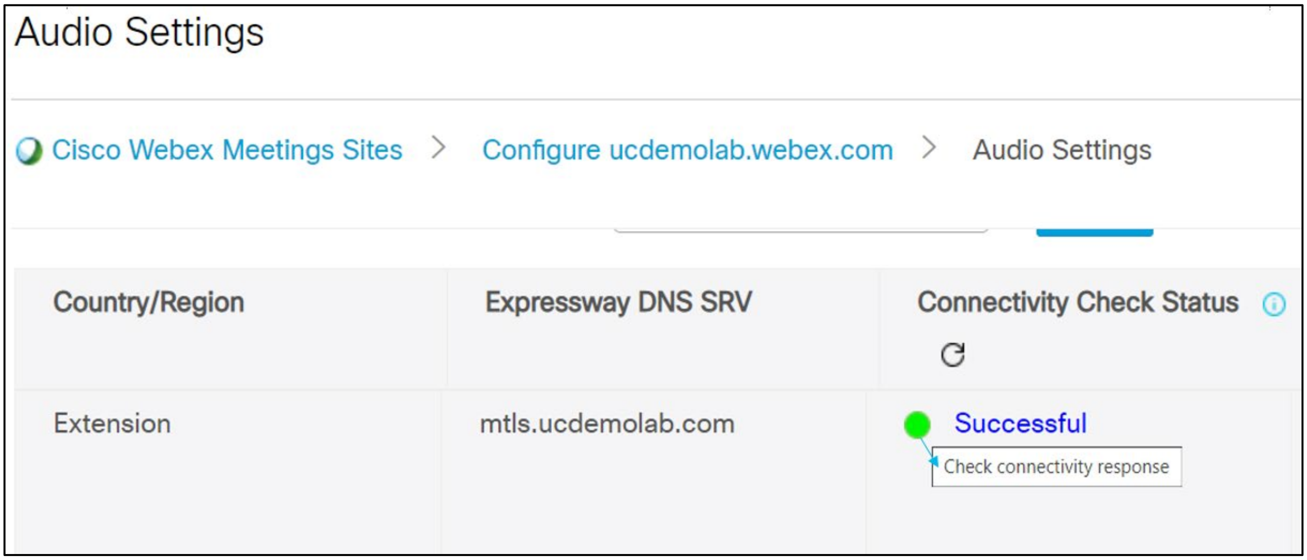
For customers who want to configure CUBE to accept calls from multiple sites that are resolved in the callback SRV record in DNS for Edge Audio, the required configuration includes additional 'voice class uri' and 'dial-peers' commands to attach Site UUID from all Webex sites. Figure 12 shows the CUBE configuration example recommended by Webex Control Hub.

Figure 12. Example Secure Edge configuration for CUBE



Once the Secure Edge configuration is implemented in the Expressway-E or CUBE, the next step is to verify TLS connectivity from Webex to the Collaboration Edge. Enterprise administrators can verify the TLS connection from the Edge Audio Allowed Callback Numbers section from Audio Settings in Webex Control Hub. Figure 13 shows an example connectivity check in Webex Control Hub callback.

Figure 13. Webex Control Hub callback connectivity check



The connectivity test includes DNS, TCP, SSL handshake and TLS version errors, the results can be three possible states:

- Green or successful, no connectivity errors found.
- Yellow or partial, at least one node had connectivity errors
- Red or error, all nodes did not pass the connectivity check

Custom Numbers

As a cloud-based PSTN audio option, Webex Meetings Audio provides a broad coverage footprint with toll dial-in, toll-free dial-in, and call-me capabilities for local and global connections. Webex offers global access numbers in:

- 66 countries with toll call-in access
- 85 countries with toll free call-in access
- 202 country access for callback

Due to rapidly changing and unpredictable global telecommunications laws and regulations, availability of certain Webex Meetings Audio services and related offerings may become restricted. While Webex routinely monitors applicable telecommunications law and regulations to readily adapt to changing legal environments, Webex reserves the right to modify its Country Coverage Listing for all affected Webex Meetings Audio offerings, without notice, as necessary to meet all country legal requirements. For details on PSTN country coverage please visit Webex Meetings Audio PSTN Coverage

Enterprises may want to use their own number for its employees to dial into a Webex meeting instead of a global access number. The Edge Audio architecture allows the administrator to add customer owned enterprise numbers or direct inward dial (DID) numbers to join a Webex meeting audio.

The option for enterprises to use their own custom number increases the coverage of toll and toll-free call-in to 198 countries. This feature applies to customers with a Webex Audio PSTN Plan, and it is not available with Cloud Connected

Audio Service Provider (CCA-SP) PSTN because their call-in numbers are controlled and routed via the partner infrastructure.

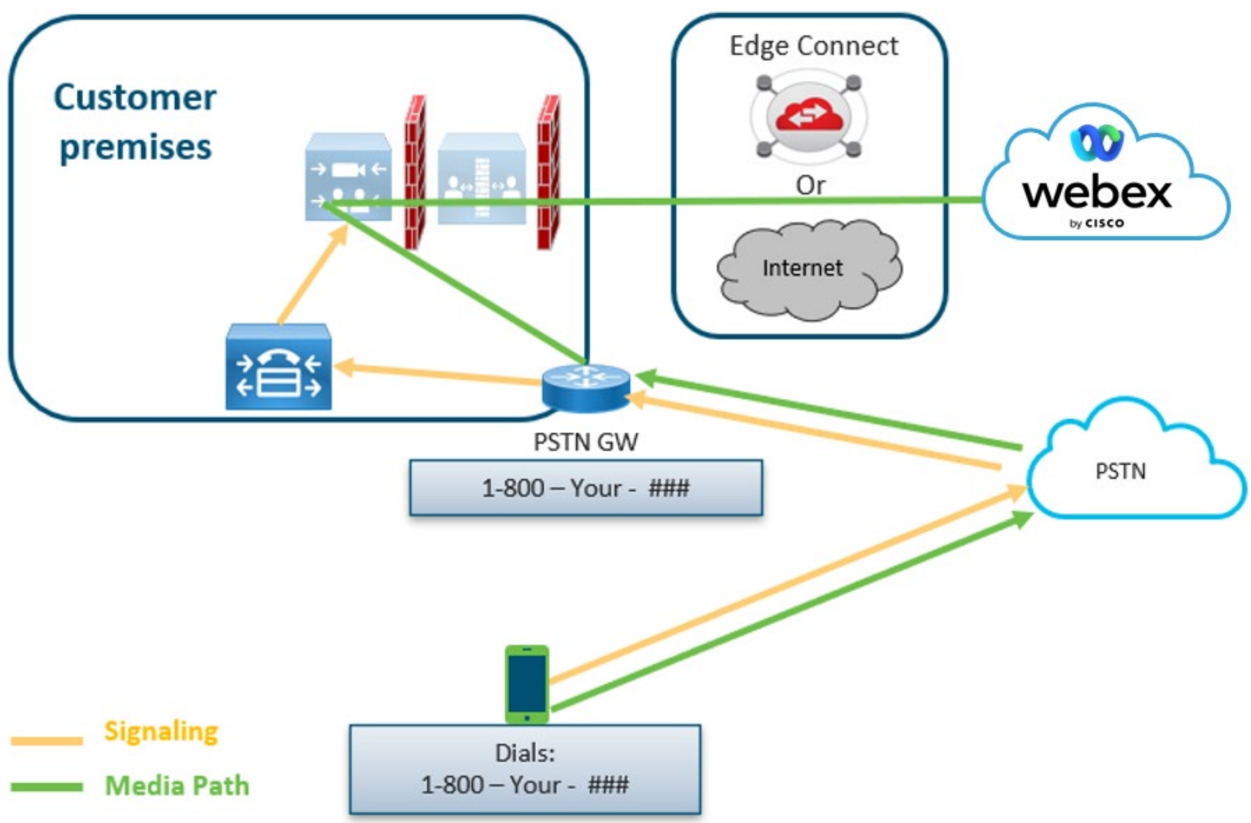
When configuring customer numbers in Edge Audio, the administrator can add up to 100 telephone numbers in Webex Control Hub. These numbers can apply to all countries except India. India is not allowed because of country regulations. If more than 100 customized numbers are needed, the administrator can disable other global access numbers listed by Webex to gain more customized numbers. Global access numbers are defined in the "Allowed Call-in Numbers" section of the audio settings page in Webex Control Hub shown in Figure 15.

A Webex user can set the default global call-in numbers or provide the option for meeting hosts to control which call-in numbers are displayed on the meeting. Webex meetings hosts can change the default call-in numbers by:

1. Log in to the Webex site. (Example: SITENAME.webex.com)
2. Select Preferences in the left navigation bar, then select Audio and Video.
3. Under Default call-in number, set up to two default call-in numbers for the sessions that will be hosted or attended:

Each custom number must be unique to a single Webex site and cannot be used on two Webex sites at the same time. The reason this is not supported is because each custom number needs to have a site identifier parameter when the call goes to Webex and the Lua script in Unified CM can only apply one site identifier per number. Figure 14 provides a high-level overview of the custom numbers call flow.

Figure 14. High-level overview of the custom numbers call flow



Allow or Deny Countries

When using Webex PSTN for call-in, the administrator has the flexibility to enable or disable Webex countries' Webex phone number for toll, toll-free or both types of calls. Figure 15 shows how this can be done by simply checking or unchecking the country and hitting save to apply the changes.

Once the change of enabling or disabling happens, the user that scheduled the meeting needs to reschedule the meeting. In case of disablement a Webex access number, the user needs to reschedule the meeting so that the disabled number does not show in the Webex email invite, this avoids having users try to use a disabled access number to access a meeting. Just like call-in, the administrator has the flexibility to disable callback countries as shown in Figure 16.

If the Webex subscription is using CCA-SP PSTN services, enabling, and disabling a country for callback for the CCA-SP site is possible through Webex Control Hub.

Figure 15. Enable or disable call-in toll and toll-free countries

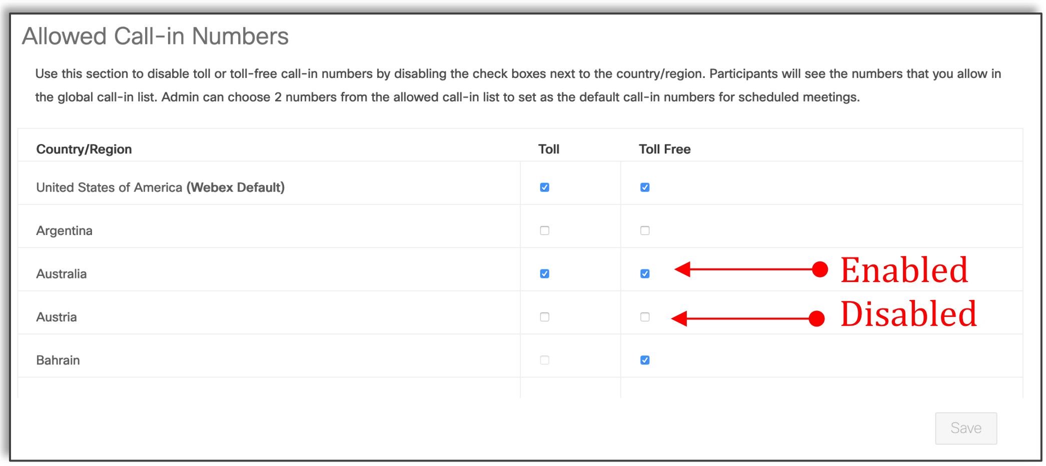
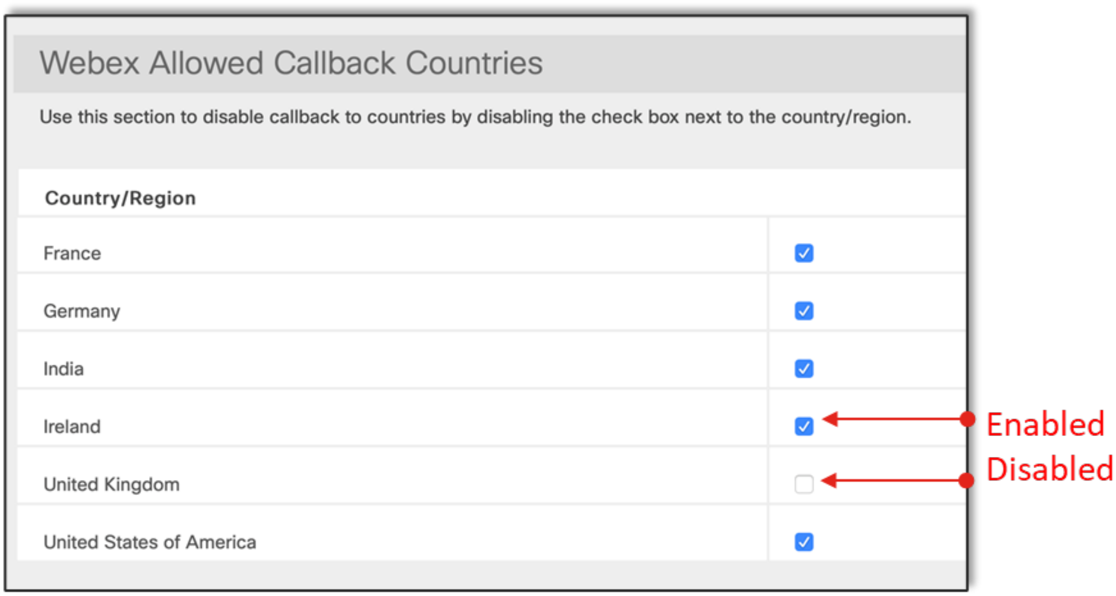


Figure 16. Enable or disable call-back country



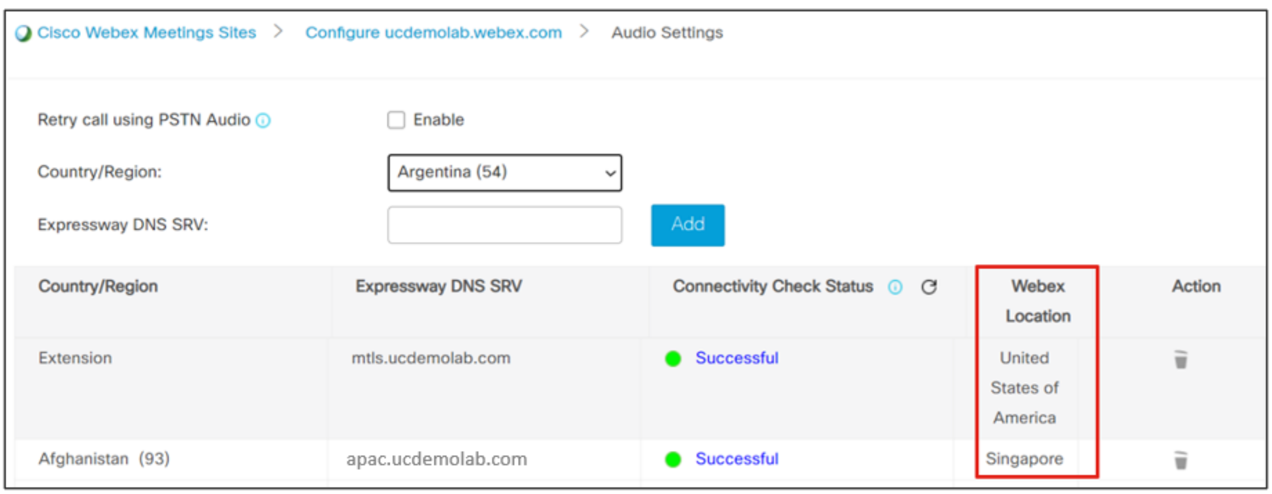
Callback Global Distributed Media

Global Distributed Media (GDM) is a feature of Webex Meetings that enables a meeting to be distributed to multiple servers running in different data centers. With this feature, an attendee will automatically be connected to an optimized location when joining a Webex meeting. To achieve better globally distributed media connectivity, Webex selects the nearest media node to the enterprise Expressway-E or CUBE. Traffic then passes through the Webex cloud to the nearest media node, and then utilizes Webex's high quality, low latency, global backbone to connect the meeting host's site. This routing minimizes the time that the meeting traffic spends on the slower internet and improves the quality of the audio call.

To configure the Edge Audio service to use GDM, Webex need to understand where the Collaboration Edge devices are located. This is done by SRV record lookup. When customer administrator configures an SRV in Webex Control Hub, Webex resolves the SRV record and gets the IP addresses and uses a discovery service using Maxmind GeoIP database which provides location the location of the IP address. This information is stored and later used during call routing. This process sets the nearest media node for that location. To change the media node, delete the current record and add the country again with an updated SRV record. Figure 17 shows an example of the nearest media node location for callback in Webex Control Hub where callbacks to Afghanistan are using the Singapore location.

Edge Audio uses GDM for all callbacks including extension callbacks.

Figure 17. Webex location based on SRV record IP address



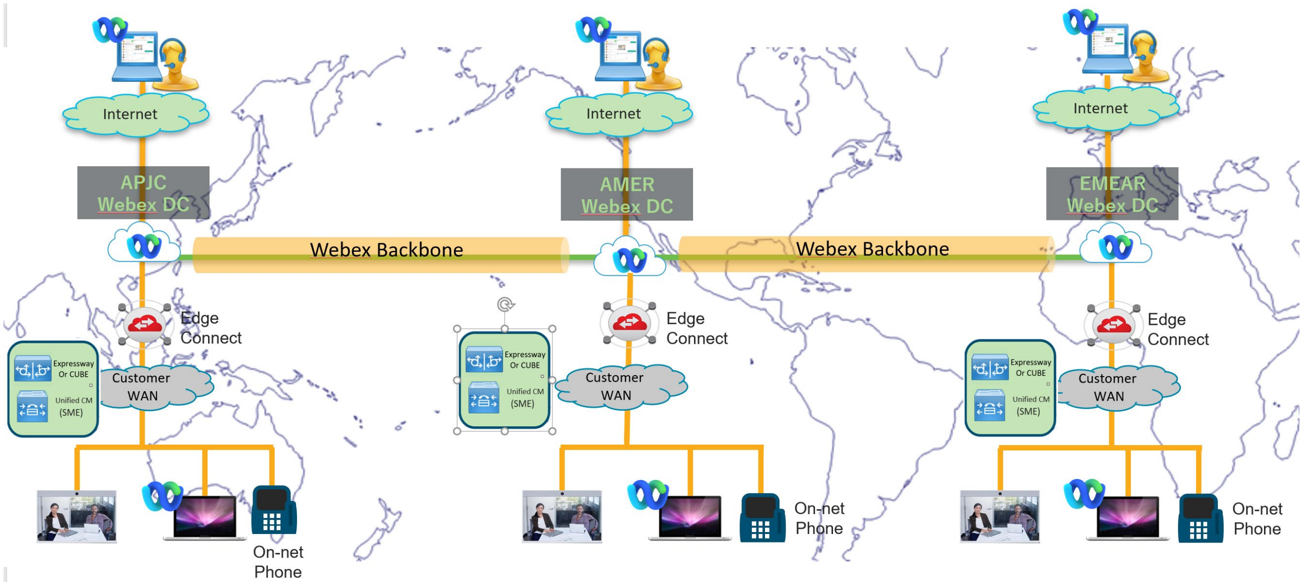
Multisite Centralized Call Processing Model

Cisco recommends that large global deployments take advantage of a centralized Unified CM Session Management Edition (SME) per region. Cisco recommends enterprises with greater than 1,000 concurrent active calls across multiple countries to leverage a geographic distributed Webex Edge architecture. This architecture uses Edge Connect peering and Edge Audio (Expressway, CUBE, or third-party SBCs) deployed at each geographic region as shown in figure 18. The edge architecture in each geographic region leverages the Webex backbone or Global Distributed Media for increased capacity. Figure 18 shows a high-level overview of the recommended Webex architecture for a global customer. This high-level architecture shows the endpoints across a WAN joining a meeting using Webex devices, Webex Meetings app and IP Phones. It also includes centralized call routing, and an Edge Connect private link per region.

Due to the cost and limited bandwidth available across the enterprise WAN, a call admission control mechanism is required to manage the number of calls admitted on any given WAN link. One of the goals of this architecture is to optimize the global call flow to maximize usage of the Webex backbone while minimizing the impact on the customer IP WAN. This is achieved by routing the calls using the IP WAN as close to the final PSTN destination as possible leveraging local rates at a potentially lower cost. Where regulations allow, local PSTN breakout through the remote site gateway or CUBE can be used to enable toll bypass or tail-end hop off (TEHO).

On-net call-in to a Webex meeting with this architecture optimizes the global call flow to maximize usage of the Webex backbone, for example an on-net user in Australia dialing in to a Webex Meeting via the Webex global access number will be routed as a free on-net VoIP call through the regional Edge Connect peering and across the Webex backbone to the meeting.

Figure 18. Global Customer Webex High-Level architecture

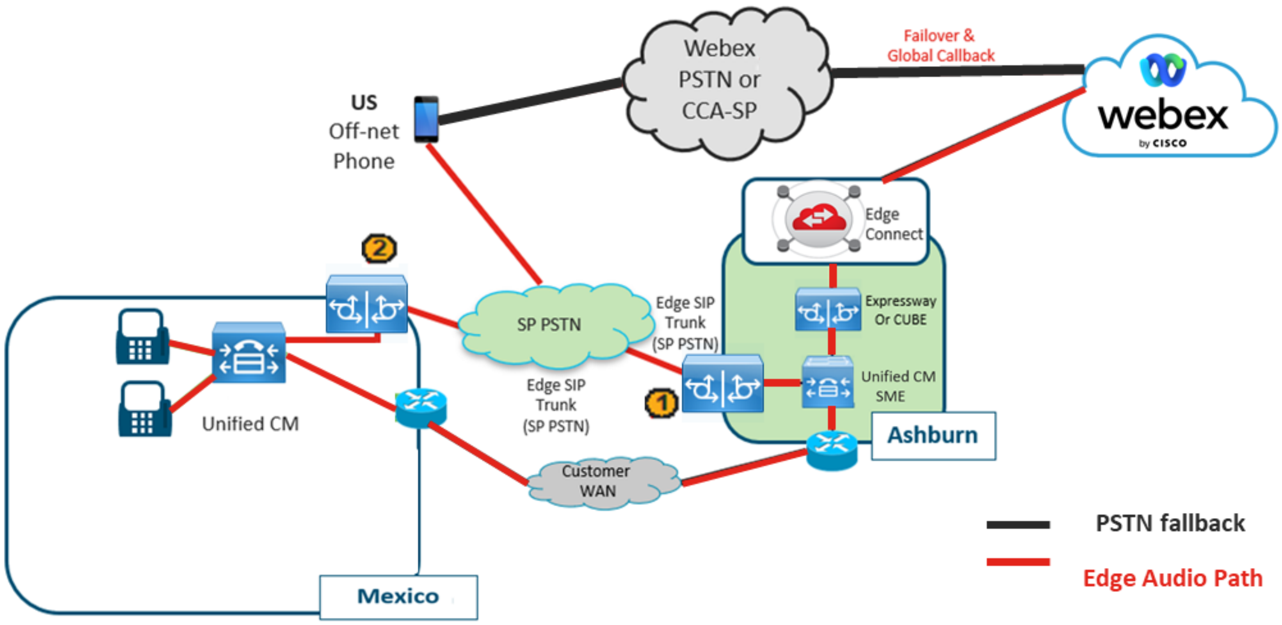


Analyzing just the AMER region of Figure 18, Figure 19 shows a centralized call control and an Expressway or CUBE used for Edge Audio. A Unified CM SME is implemented in this design to centralize the off-net and on-net call routing decisions optimizing WAN consumption because only calls destined to the remote sites use the WAN link.

With the multisite centralized call processing architecture, PSTN routing through both central and remote site gateways or CUBEs is supported.

In Figure 19, the centralized SME in Ashburn receives an off-net Edge Audio callback call destined for Mexico. The routing decision is done by the SME and can either route the call to the Ashburn CUBE (Figure 19 - 1) or send the call to the Mexico CUBE or Voice Gateway (Figure 19 - 2) to take advantage of the local PSTN rates. If the call is rejected by Unified CM SME, the Edge Audio fallback mechanism will route the call out Webex PSTN audio services. As you can see, this architecture enables the Unified CM SME with the flexibility to control the call flow to send the calls to a regional branch to take advantage of lower rates for countries where regulations allow.

Figure 19. Centralized Unified CM SME



Session Refresh Best Practices

When a user places a Webex Edge Audio call to join a Webex meeting, Expressway-E or CUBE sends an INVITE to Webex with a “Supported” SIP header field with the option tag 'timer' indicating support for a session refresh.

For this outgoing invite, Unified CM specifies the *Session-Expires* header field and a *Min-Se* header field into the request and sends the Invite to the Expressway or CUBE.

If the *Session-Expires* interval is too low for Webex, the invite will be rejected with a 422 response. The 422 response contains a *Min-Se* header field identifying the minimum session refresh interval it is willing to support. Expressway-E or CUBE will originate another Invite request including the *Min-Se* header field in the request.

Webex by default uses a minimum session expires timer of 14,400 seconds. Unified CM by default uses 1,800. This can cause the initial Invite to Webex to be rejected with a “422 Session Interval Too Small” error.

Since a Unified CM change is global for all SIP trunks, *Min-SE* changes may affect other SIP flows adversely. Cisco recommends updating the session refresh interval to 14,400 at the edge on the Expressway-E and CUBE.

The administrator can modify the *Session refresh* interval to 14,400 globally in Expressway-E by changing the parameter under Configuration > Protocols > SIP.

The administrator can modify the *Session refresh* interval to 14,400 globally in CUBE by changing the parameter under *voice service voip* > *sip* > *min-se*. This will prevent a 422 response error from Webex.

For additional details on Session Timers in SIP refer to RFC 4028.

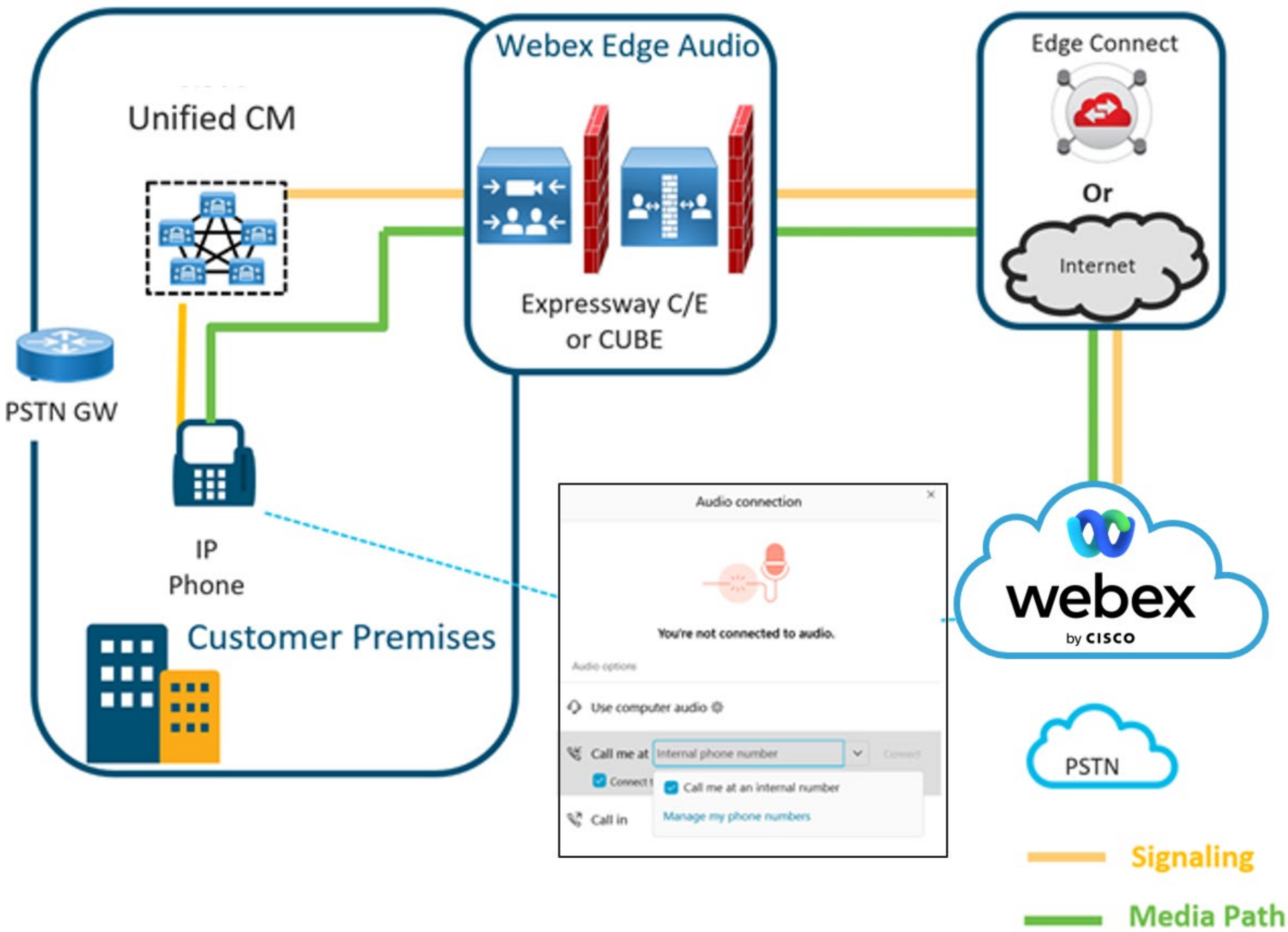
Edge Audio Extension callback

Webex Edge Audio uses an +E.164 numbering plan format for all country callbacks. The administrator can provision the option to allow a shorter number that is easier for the user to enter and remember when connecting to a Webex meeting. This capability is called extension callback. Figure 20 illustrates an extension callback diagram.

When extension callback is enabled in Webex Control Hub, the internal extension call is routed to Unified CM to make the call routing decision. If the extension is a valid extension in Unified CM, the call will ring the device; if not, the call will be rejected.

When configuring extension callback in Webex Control Hub only one SRV record can be used. It is not possible to point the extension to multiple Collaboration Edges. Every extension callback call will take the same destination SRV record.

Figure 20. Extension Callback



Edge Audio PSTN fallback

Edge Audio PSTN fallback has an impact in the number of Webex PSTN minutes consumed by customers, therefore, to reduce PSTN cost it is important to understand how the fallback design works. In the case of a failure due to a connectivity issue Webex can redirect the call to Webex PSTN audio services to connect the call. This feature is called PSTN fallback.

There are many reasons why a call can trigger fallback to Webex PSTN or CCA-SP PSTN. Figure 21 illustrates a fallback due to either "no local PSTN capacity" (Figure 21 - 1) or Unified CM blocking the call (Figure 21 - 2) with possible reasons including dial plan configuration, CAC, or the SIP trunk/route group being unreachable).

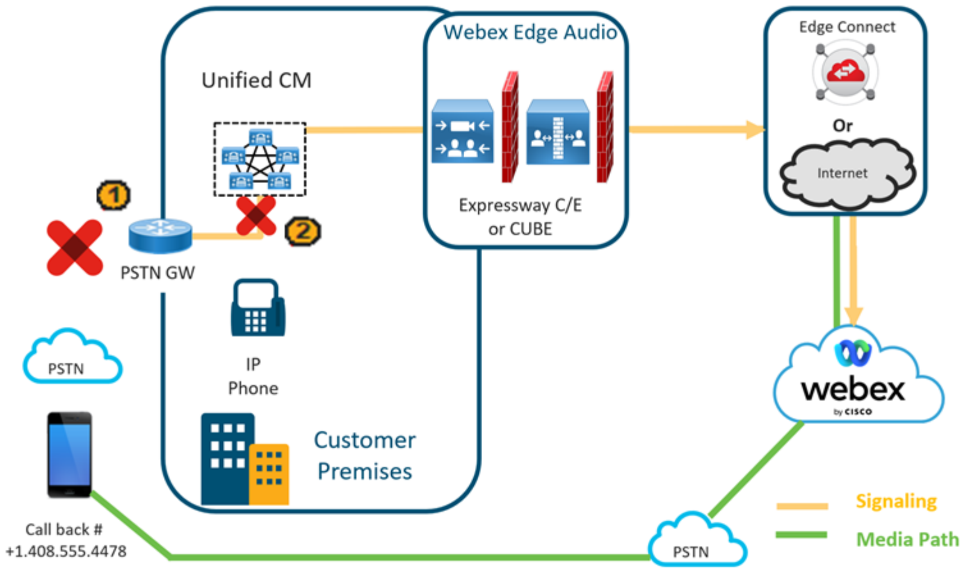
Other possible reasons why PSTN fallback can be triggered are:

- DNS timeouts / failures
- TCP timeouts / failures

- TLS timeouts / handshake failures
- SIP error responses 380 / 4xx / 5xx / 6xx

For DNS timeouts and 503 errors. Webex tries the next A record. If all A records are unavailable, then PSTN fallback is used if enabled.

Figure 21. PSTN fallback errors



PSTN fallback is enable by default, but while enabled it does not support extension callback because there is no way to make a complete +E.164 number for PSTN routing. The Webex administrator has the option to disable PSTN fallback for all Webex Edge Audio calls if they wish to not consume PSTN minutes. The administrator can also monitor the percentage of calls using fallback in Control Hub meeting analytics.

DNS Considerations

Webex leverages DNS for call-in and callback. For call-in, the enterprise edge does a DNS lookup to connect to the correct Webex region. This DNS request goes over the traditional path of the Internet. For callback, the Webex Control Hub uses the SRV record to address callbacks to Webex Edge Audio Expressways or CUBEs. See Webex Edge Audio prerequisites DNS section for more details on SRV record creation.

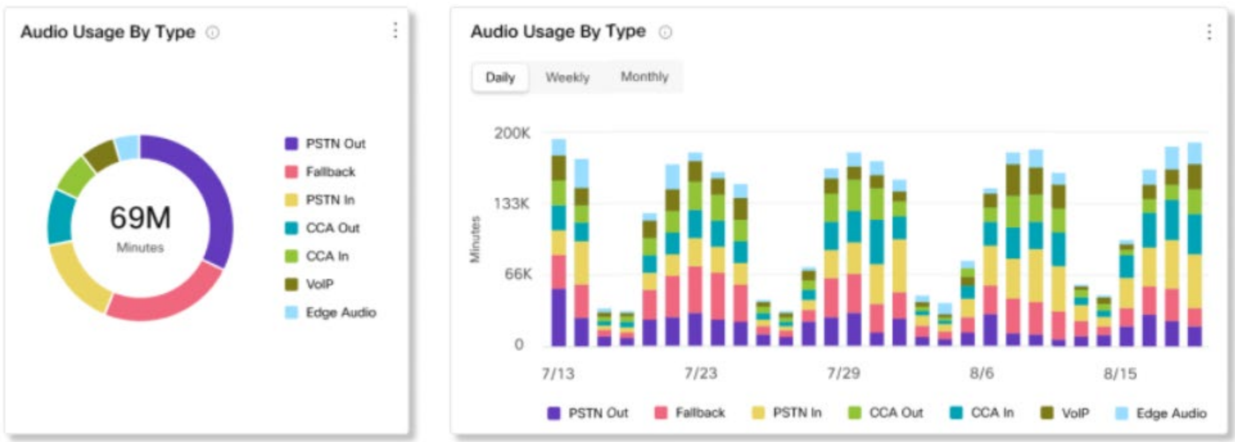
For call-in, when using Expressway-E for the Collaboration Edge, the Webex zone is used to establish communication between Webex and the Expressway-E. The Webex zone is used because a secure mutual TLS connection between Webex and Expressway-E is required to map the appropriate domains. This Expressway zone queries the public DNS for the Webex SRV inside the Lua script; for example, ecccx.amer.pub.webex.com which is used for calls to Webex in North America.

For callback, the hostnames or Fully Qualified Domain Names (FQDNs) in the DNS SRV records must resolve to the Expressway-E cluster's IP addresses, CUBE IP, or 3rd Party SBC through DNS A/AAAA record(s). When setting up the DNS records, do not reuse existing MRA (_collab-edge._tcp), or B2B (_sips._tcp) SRV records because Edge Audio requires that the SRV records resolve to the Expressway-E cluster's mutual TLS port and both mobile remote access (MRA) and business to business calls (B2B) cannot use mutual TLS.

Analytics and Reports

The Meetings Analytics Audio page in Webex Control Hub shows key performance indicators (KPIs) and metrics relevant to Webex Edge Audio including telephony minutes and trending charts with summary statistics. Figure 22 provides an example of the audio usage by type chart in Webex Control Hub. The administrator can also download the Webex Meeting Audio Usage report for audio details.

Figure 22. Audio source chart in Webex Control Hub Analytics



High Availability and Redundancy

High availability and redundancy can be done in several ways. This section will discuss callback with local and site redundancy, call-in with local and site redundancy, and lastly High Availability with a CUBE-HA deployment.

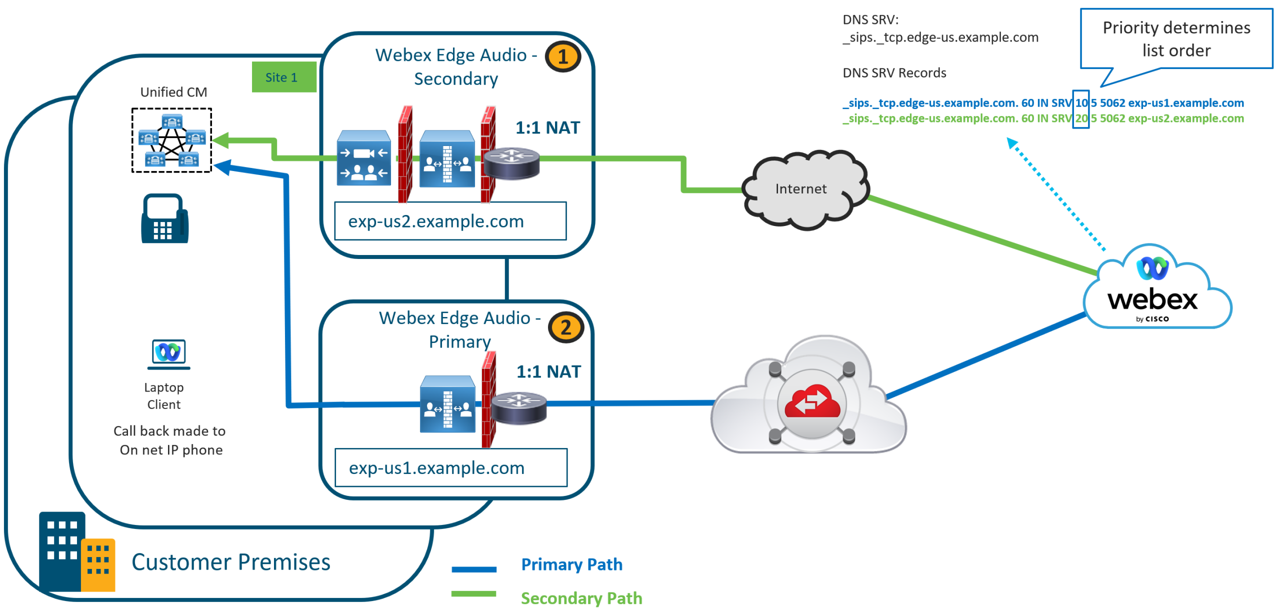
Callback redundancy

Webex Edge Audio uses DNS SRV records (RFC-2782) to provide multiple IP address resolutions for the same hostname. The resolution of the DNS query returns the server selection, and the result considers the priority and weight fields of the SRV record. Webex will attempt to contact the target host with the lowest numbered priority it can reach Figure 23 illustrates using priority to create a Primary and Secondary Edge Audio redundancy plan. In this case exp-us1 is always used as the priority is higher (lower number) than exp-us2. Only if exp-us1 does not respond will xp-us2 be used. This setup is to leverage the edge audio expressway over the Edge Connect link first and only when it's not available use the edge audio Expressway over the internet path. Larger weights have a proportionately higher probability of being selected. Webex cloud contacts the Collaboration Edge dynamically using the information returned by DNS. Redundancy for callback is achieved by the server selection from the SRV query provision under Webex Control Hub for each country or for extension callback. This SRV record can contain site redundancy to achieve a primary and secondary path where the Collaboration Edge is located at a geographically separated site. With separate sites, each site is backing one another up in case of link or site failure. For Expressway clustering ensure that the following network requirements are met:

- Each peer has a different LAN configuration (a different IPv4 address and a different IPv6 address, where enabled).
- Expressway supports a round trip delay of up to 80ms between nodes in a cluster. This means that each Expressway in the cluster must be within 40ms of all other peers in the cluster.
- Each peer in a cluster is directly routable to each other. There must be no NAT between cluster peers – if there is a firewall ensure that the required ports are opened.
- External firewalls are configured to block access to the clustering TLS ports.
- The network connections between the peers must be reliable during cluster forming or changing procedures.

If an Expressway node fails, active calls flowing to that Expressway are dropped and the Webex user must reconnect to audio.

Figure 23. DNS SRV priority and weight for callback



Call-in redundancy

When calling into Webex, Unified CM determines the call path. Using the built-in logic of Unified CM allows for redundancy mechanisms by implementing Route Groups and Route Lists for load balancing when sending calls outbound to the Expressways or CUBEs. The call from Unified CM can be load balanced with local redundancy which consists of having an Expressway Cluster or a CUBE in the same physical location. The call from Unified CM can also be load balanced with site redundancy which consists of having an Expressway cluster or a CUBE located at a geographically separated site. From a sizing perspective each location needs to be able to handle the peak call volume requirements of both sites in case of a failure. As such Expressway or CUBE need to be provisioned accordingly.

Cisco recommends using SIP OPTIONS ping to proactively check the status of the SIP trunks and enable faster selection of an available Expressway or CUBE.

When multiple Expressway-C and Expressway-E pairs are deployed, Unified CM can direct an outbound call to the node that is nearest to the calling endpoint, thus minimizing internal WAN traffic. This can be achieved by using Cisco Unified CM mechanisms such as calling search spaces and partitions. Additionally, when utilizing multiple Expressway clusters, the Expressway-Cs should form a meshed trunk configuration with the Unified CM clusters. This adds more scalability and resiliency by allowing additional outbound traversal paths if the geographically located traversal is full or not available.

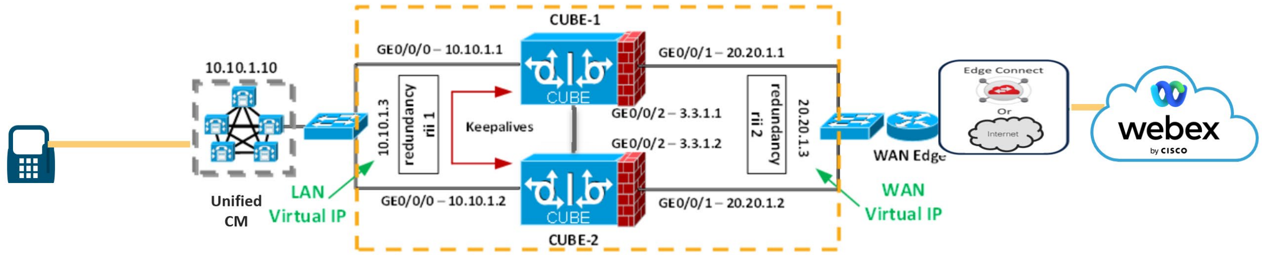
When the customer has multiple Webex sites this will require the configuration of multiple SIP trunks from the regional Unified CMs to the Collaboration Edge. Combining multiple Lua scripts from different Webex sites and applying them to a single SIP trunk is not supported. In an architecture with Unified CM SME, Cisco recommends applying the Lua script on the SME cluster when applicable instead of each leaf Unified CM nodes. Unified CM SME uses a dedicated SIP trunk for Edge Audio towards the Collaboration Edge which avoids having to configure the Lua SIP normalization script in multiple places. With a dedicated SIP trunk per Webex site, the right UUID can be added for Webex to associate the call with its respective site.

CUBE high availability

For all IP-based environments, customers have the option to deploy CUBE high availability (HA) for call preservation. CUBE high availability Layer 2 box-to-box redundancy uses the Redundancy Group (RG) infrastructure protocol to form an active/standby pair of routers. The active/standby pair share the same virtual IP address (VIP) across the respective interfaces and continually exchange status messages. CUBE session information is checkpointed across the active/standby router, enabling the standby router to immediately take over all CUBE call processing responsibilities if the active router should go out of service. This results in stateful preservation of signaling and media.

Refer to figure 24 below which depicts a typical CUBE high availability for Webex Edge Audio.

Figure 24. Webex Edge Audio CUBE HA architecture



Considerations and best practices for CUBE HA include:

- The control link no longer needs to be connected to the same switch.
- Only active calls are checkpointed (Calls connected with 200 OK or ACK transaction completed).
- Upon failover, the previously active CUBE reloads by design.
- Port channels and virtual port channels are recommended to prevent a switch as a single point of failure.

For more information about CUBE HA restrictions and best practices, please refer to the CUBE configuration guide

Conclusion

Three key points to keep in mind when deploying Webex Edge Audio:

- Webex Edge Audio enables both high quality audio and cost savings.
- Consider Webex Edge Connect for the best audio experience.
- The Webex Edge Audio deployment models provide flexibility in the architecture equipment, architecture scale, and cost savings.

Reference Links

- Webex Edge Audio Deployment Options:

  https://help.webex.com/en-us/4pldzd/Cisco-Webex-Edge-Audio-Deployment-Options
- Webex Edge Audio Datasheet:

  https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-edge/data-sheet-c78-741264.html
- Webex Meetings Audio PSTN Coverage for Cisco Collaboration Flex Plan: https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/cisco_webex_gpl_audio.pdf
- Network requirements: https://help.webex.com/en-us/WBX000028782/Network-Requirements-for-Webex-Teams-Services
- Cisco Expressway on Virtual Machine Installation Guide: https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html
- Meeting Flexibility and Improvements within Webex Edge for Meetings - BRKCOL-2050
  - Event: Digital 2021
  - Speaker: Richard Murphy

  https://www.ciscolive.com/global/on-demand-library.html?#/
- Webex Edge Connect preferred architecture https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/EdgeConnect/PA_Edge_Connect_Design.pdf

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.**