White Paper

Cisco WebEx Cloud Connected Audio

Take full advantage of your existing IP telephony infrastructure to help enable a WebEx integrated conferencing experience

Introduction

Cisco® WebEx Cloud Connected Audio (CCA) is an end-to-end audio solution that uses your on-premise IP telephony network to provide an integrated audio experience for your WebEx® meetings. WebEx CCA implements a Session Initiation Protocol (SIP) trunk from your premises into the WebEx data center instead of using a traditional telephony connection. This solution provides the same integrated and intuitive user experience as all other WebEx audio options. However, by directly using your IP telephony network, WebEx CCA can provide more attractive audio pricing.

Cisco has extensive experience in delivering collaboration software as a service (SaaS), as well as in designing and implementing of customer premise equipment (CPE). Together, these experiences help enable us to offer our customers an unparalleled integration between hosted and on-premise telephony solutions through Cloud Connected Audio.

This paper explores the following aspects of WebEx Cloud Connected Audio:

- Benefits
- Architecture Overview
- Architecture Details
- Redundancy
- High Availability
- Security
- Monitoring
- Network Assessment

Benefits

Some of the benefits of WebEx CCA include:

- **Use of existing investment** - Customers can build upon their existing IP telephony infrastructure to create the same integrated, intuitive WebEx conferencing experience.
- **Attractive audio pricing** - Use convenient and flexible concurrent port-base pricing. Predicting the number of concurrent meetings versus how many minutes you use greatly simplifies cost estimates.
- **Global Reach** - Global calls can be carried over the customer's IP network eliminating the need to make calls using global call-in numbers.
- **Scalability** - CCA offers the ability to easily add capacity - with no constraints on available time slots. The solution scales easily and simply as your audio conferencing needs grow.

- **Hosted** - Using solutions delivered over the WebEx Collaboration Cloud simplifies software deployment, administration, upgrades and maintenance.

Architecture Overview

Figure 1 illustrates the traditional deployment model of WebEx audio where all calls go through public switched telephone network (PSTN). For enterprises with large volume of audio conferencing usage, this solution may become cost-prohibitive due to PSTN toll charges.

The conferencing number is owned by Cisco and hosted on Cisco WebEx audio conferencing platform. All calls originated from either within the customer's network or outside of the customer's network flow into WebEx over PSTN. All callbacks coming from WebEx audio are also made through PSTN. Both Cisco and the customer pay their service provider for PSTN access.

Figure 1. Customer Connection to WebEx Audio through PSTN before CCA

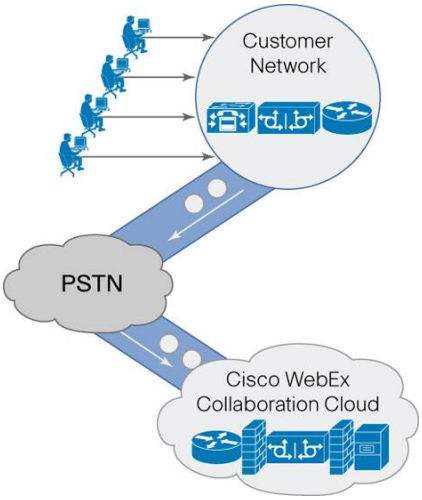
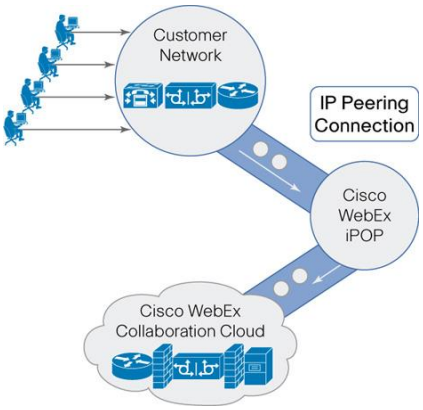


Figure 2 refers to the topology of WebEx CCA. The basic design premise of CCA is to connect the customer's IP PBX to the WebEx audio conferencing platform using an SIP trunk. This architecture eliminates PSTN toll charges for all on-net calls - calls originating from within the customer's network. CCA allows for the more cost-effective audio conferencing solution - especially for customers with large volume of audio conferencing usage.

The SIP connection requires a certified Session Border Controller (SBC) at the customer's premises to connect with WebEx SBCs. All audio conferencing calls are routed by the customer's IP PBX using the customer's SBC into the WebEx cloud over the SIP trunk. All callbacks made from WebEx are made to SBC at the customer's premises as well. The conferencing number is owned by the customer and is hosted on the customer's IP PBX. All conferencing calls originating from the endpoints outside of the customer's network are first established with the customer's IP PBX using the customer's existing PSTN infrastructure and then placed with WebEx audio platform over the SIP trunk.

Figure 2. Customer Connection to WebEx Audio Using CCA



Architecture Details

Following are the main components of the CCA solution:

- Cisco Unified Communications Manager
- Cisco Unified Border Element at customer premises
- IP Peering Connection
- WebEx cloud infrastructure

Cisco Unified Communications Manager (CUCM)

CUCM is an enterprise-class IP communications processing system. It is the certified IP PBX for the WebEx CCA solution. Versions 8.5 and above are recommended.

Cisco Unified Border Element (CUBE) at the customer's premises

CUBE is Cisco's SBC which provides voice connectivity from the customer's IP network to the WebEx cloud over SIP trunks. CUBE is an integrated Cisco IOS® Software application that runs on Cisco Integrated Services Routers (ISRs) and Cisco Aggregation Services Routers (ASRs). Cisco IOS release 15.1 and above on the Cisco ISR 3945 or CUBE version 3.1 on Cisco 1000 Series ASR are recommended for the WebEx CCA solution.

IP Peering Connections

The WebEx CCA requires the customer to connect with WebEx at two separate geographical locations to establish minimum redundancy. Redundant IP links are configured in the active/standby mode, i.e. there is no load balancing across the two IP connections. All conferencing audio traffic must flow over the primary link. Audio traffic fails over only to the secondary link in the event of the primary link going down. The connections into WebEx need to have Ethernet interfaces and could be full or fractional Gigabit Ethernet circuits.

The CCA solution also requires gateway routers capable of Border Gateway Protocol (BGP) and Bidirectional Forwarding Detection (BFD) protocol. BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. The main benefit of implementing BFD for BGP is a significantly faster reconvergence time in the event of network failure.

WebEx Cloud Infrastructure

The CCA solution does not dedicate any equipment or bandwidth to a specific customer's audio traffic. All customer traffic traverses over the shared infrastructure which includes WebEx data center equipment, audio bridge and other servers and all connections between them.

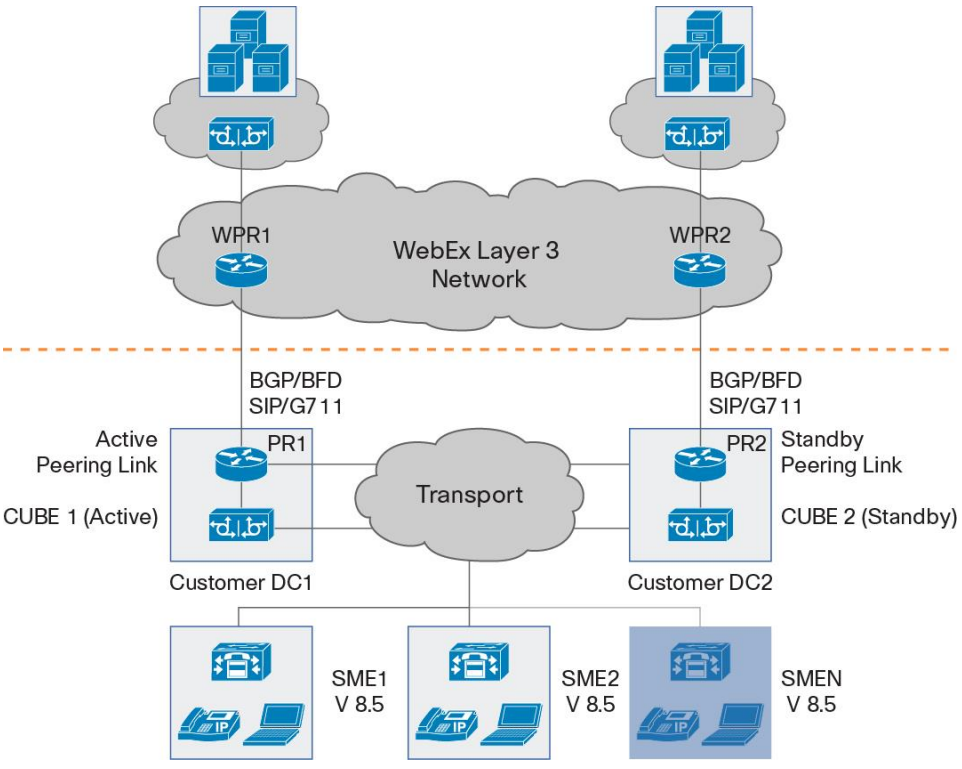
The CCA solution is designed to work only with G. 711µ - the audio compression codec. This solution does not support any other audio codec at this time. The customer is responsible for transcoding any non G. 711µ audio media stream to G. 711µ.

The CCA solution supports only SIP signaling. The customer is responsible for converting any non-SIP signal, such as H.323 signaling, into a SIP signal before sending it to WebEx.

Reference Architecture

The reference architecture locates the equipment in a single data center or separate data centers at the customer premises, providing redundancy via two WAN circuits. This can help achieve hardware and route redundancy in a cost-effective way. Figure 3 shows a detailed diagram of the CCA architecture. Gateways PR1 and PR2 can be consolidated into single Cisco ASR with CUBE combined.

Figure 3. CCA Architecture



Redundancy

The Cloud Connected Audio architecture helps ensure continuous service operation by adhering to the following design guidelines:

Redundant (Active and Standby) Instances of Each Major Component

There are two BGP peering connections handled by two independent pairs of routers, two pairs of CUBEs, and two conferencing bridges. If any of these components fails, its standby counterpart takes over. Best practices call for deployment of redundant components in different geographic areas.

- **Link Failure:** If the peering routers on both sides of the failed link are still operational, each of them withdraws the routes associated with the failed connection from its local network. The network converges on the standby connection. The gateway routers on both sides of the newly activated link start offering routes associated with it to their respective networks. All existing calls continue on with an up to one second interruption of the media flow.
- **CUBE Failure:** The operational state of each CUBE is monitored through the continuous dispatch of out-of-dialog (OOD) options that ping packets by every CUBE or SME to all of its dial peers. Failure to respond to a ping results in removal of the unresponsive element from the dial-peer list of the sender, which commences routing all new calls to the standby CUBE.
- **WebEx Audio Bridge Failure:** All calls associated with the failed WebEx audio bridge instance are terminated. The WebEx meeting server prompts users with a new number to connect to the newly activated (formerly standby) instance of WebEx audio bridge, which also re-dials all system-originated calls (callbacks) from before the failure.

High Availability

To prevent even momentary service interruptions or delays, most of the CCA components can be configured in high-availability mode. In that case the active element of a redundant pair continuously replicates its state to the standby element, allowing for a seamless transition in case of a failure.

WebEx Telephony Platform High Availability

The only failure that results in inevitable disconnection of existing calls is the loss of an audio bridge or its co-located CUBE. Although WebEx audio platform is a highly available, distributed system, the active and standby instances do not share an IP address due to the distance required to achieve geographic diversity. However, the conference state is continuously replicated between the active and standby instances, so meetings resume as soon as calls are reconnected.

Unlike traditional telephony scenarios, re-connecting calls to a WebEx conference is a relatively painless, semi-automatic process. Calls that were originated by WebEx audio bridge will simply be redialed without any user involvement. If the users called into the conference prior to the failure event, they will be automatically prompted to dial the number of the newly activated audio bridge. Once a call is re-connected, it is automatically associated with the other components of the conference (data, video, etc.).

CUBE High Availability

The CUBE servers on the WebEx side (“cloud CUBE”) are running on a Cisco 1006 ASR chassis featuring full in-box redundancy and continuous state replication between redundant pairs of components.

High Availability of Gateway Routers and Peering Link

The failure of a peering link or a gateway router results in a sub-second network convergence as already described. This event is mostly seamless for all network components, with the only ill effect suffered being a sub-second interruption in all media streams.

Security

Since CCA is a fully encapsulated environment, it would be exceedingly difficult to reach it from the Internet, and even more so to perpetrate any kind of an attack. Other tenants are also an unlikely source of malicious traffic, since WebEx's security practices prevent inter-tenant routing. Furthermore, traffic over the peering link is limited to routing protocols between the gateway routers, and to user datagram packets (UDP) with destination ports higher than 1024 between CUBEs. On CUBE level, only traffic from pre-configured dial peers is allowed.

Firewall use is certainly possible, but is not required. The access control list (ACL) in place on the gateway routers already limit traffic to UDP packets on high greater than 1024) ports. A stateful packet inspection firewall would help ensure that traffic is further limited to ports, which have been negotiated for use as RTP destinations in a SIP session between CUBEs on both sides of the peering connection. Such limitation would only be useful if there were services bound to high UDP ports running on either CUBE that could be used as target, but there are none. A denial of service (DoS) attack is unlikely in this environment, because it would have to originate from WebEx, and would be thwarted by the "only traffic from pre-configured dial peers" rule on quantum processor level. Therefore, a firewall would add to the cost and complexity of the solution without making it appreciably more secure.

In an effort to reduce overhead and maximize throughput of the network components, the traffic is not encrypted, nor is SIP digest authentication used. The rationale is that the peering link is not unlike a time-division multiplexing (TDM) trunk between two companies, where none of these measures are present and expectations of security are covered by the private nature of the connection.

Concerning privacy, the use of the SIP normalization and topology hiding features of CUBE is recommended. The replacement of the originating endpoint's telephone number with a generic one may not be a good idea, because it would hinder troubleshooting and debugging effort if there is a quality or network problem with a call.

In conclusion, WebEx CCA offers strong security and reasonable privacy without introducing unnecessary overhead to the traffic or encumbering the design with marginally useful network security elements.

Monitoring

WebEx continuously monitors the state of all WebEx cloud infrastructure and evaluates capacity for all large implementations. Additional services can be procured with Cisco Managed Services to actively monitor the on-premise collaboration components.

Network Assessment

To help ensure adequate voice quality, customers must assess their network for available bandwidth and latency for carrying the voice traffic for CCA. Customers may need a network assessment performed by Cisco Advanced Services or other certified organizations. Such a service will be able to determine network readiness for CCA service.

Conclusion

For enterprises that use millions of minutes of WebEx meetings, the telephony costs can be variable and difficult to control. Migrating to WebEx CCA and taking full advantage of the enterprise IP PBX infrastructure not only helps enable the integrated WebEx conferencing experience but can also help reduce telephony costs for meetings, provide scalability, and achieve rapid ROI for required equipment.

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.**

Printed in USA C11-690048-00 11/12