



You make **possible**



Cisco Webex Edge for Meetings

Webex Edge Audio, Connect and Video Mesh

Richard Murphy

BRKCOL-2120

CISCO *Live!*

Barcelona | January 27-31, 2020



August 5, 2019

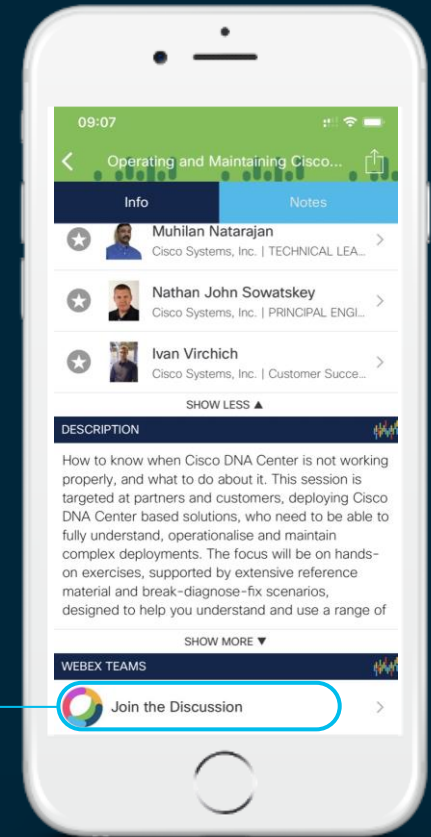
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space



Abstract

Cisco Webex is a constantly evolving cloud platform with innovation happening all the time such as the Webex Edge for Meetings service. What is it? If this question is something you are asking yourself, then this session is right for you. This session is designed to be an introductory session and will cover the three different services of Webex Edge Connect, Webex Edge Audio, and Webex Edge Video Mesh that make up the Webex Edge for Meetings service. The attendees will understand the differences of each service, the configuration requirements, and common deployment scenarios. A general knowledge of Cisco UC products such as Expressway and Cisco UCM is required. Cisco Expressways and Cisco UCM will not be discussed in detail except where they are relevant to the Webex Edge for Meetings service.

Agenda

- Webex Edge Connect
 - Overview
- Webex Edge Audio
 - Design and Implementation
- Webex Edge Video Mesh
 - Design and Implementation
- Conclusion

Components of Webex Edge for Meetings



Webex Edge for Meetings

1 Connect

Direct Connection to the Webex Datacenter

2 Audio

Webex Meeting Audio via the Internet or Edge Connect

3 Video Mesh

Meeting Resources on premises

Webex Edge Connect

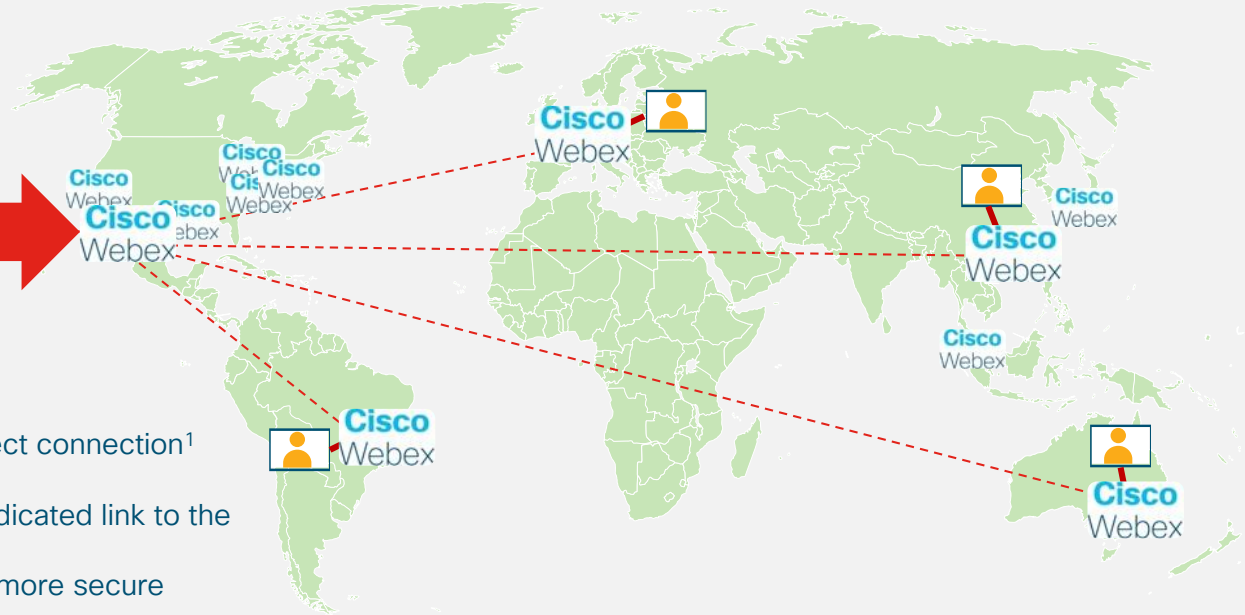
Webex Edge Connect

Brings the power of the Webex backbone directly to your data centre



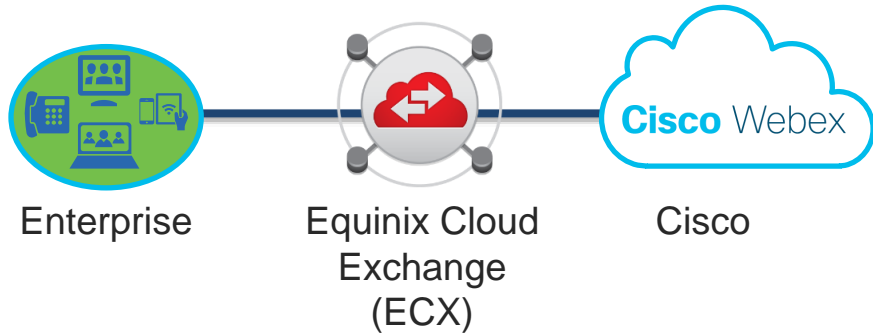
Webex Edge Connect

- A direct peering at Equinix data centers
- Bypasses the Internet by providing a direct connection¹ to the Webex data center
- All Webex media traffic traverses the dedicated link to the meeting. (VoIP, video, content sharing)
- When used with Video Mesh provides a more secure end-to-end experience



Overview

Peering connection with Cisco Webex



Benefits

- Private circuit (not over Internet)
- Deterministic network path
- Predictable and stable latency and jitter
- Guaranteed bandwidth
- Speed options: 500M, 1G, 5G, 10G

Available Services

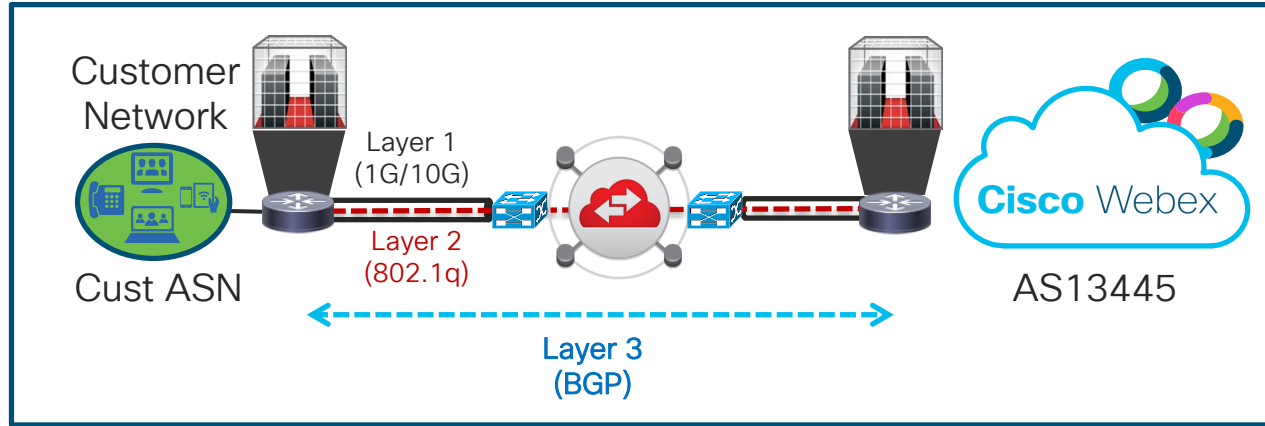
- Webex Meetings
- Webex Teams Media *
- Video Device-Enabled Webex Meetings (CMR)
- Webex Edge Audio

* Webex Teams, Board, Cloud Registered Endpoints and Video Mesh require Internet access for signaling




Webex Edge Connect Benefits

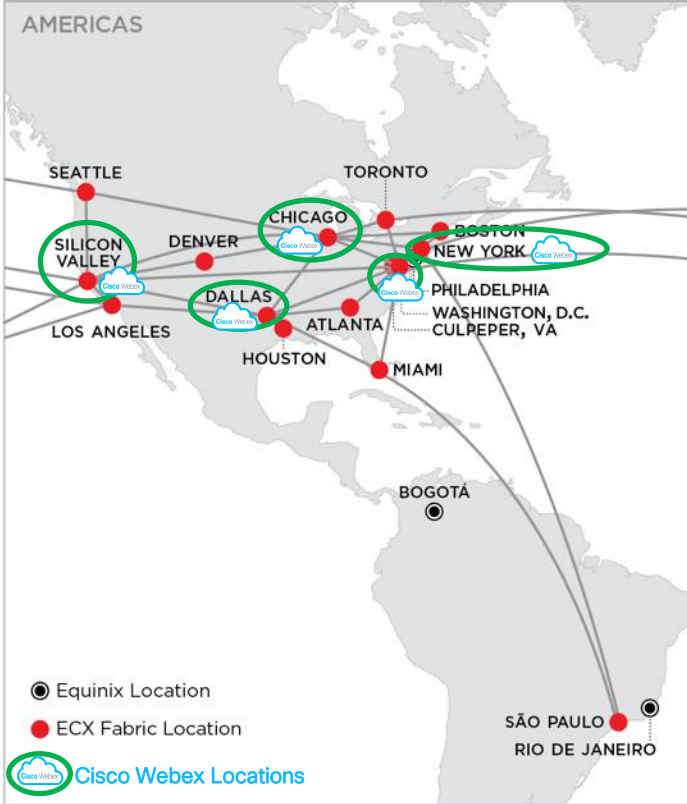
- Enhanced Meeting Quality - Your day-day core business conducted over the internet does not interfere with meetings and vice-versa. This means you can be assured of a consistent, reliable, cost effective, and secure meeting experience for all
- Added Security - Webex Edge Connect direct peering insulates your meetings from the variability of the Internet and provides protection from the public Internet and the potential threats and attacks.

Equinix Cloud Exchange



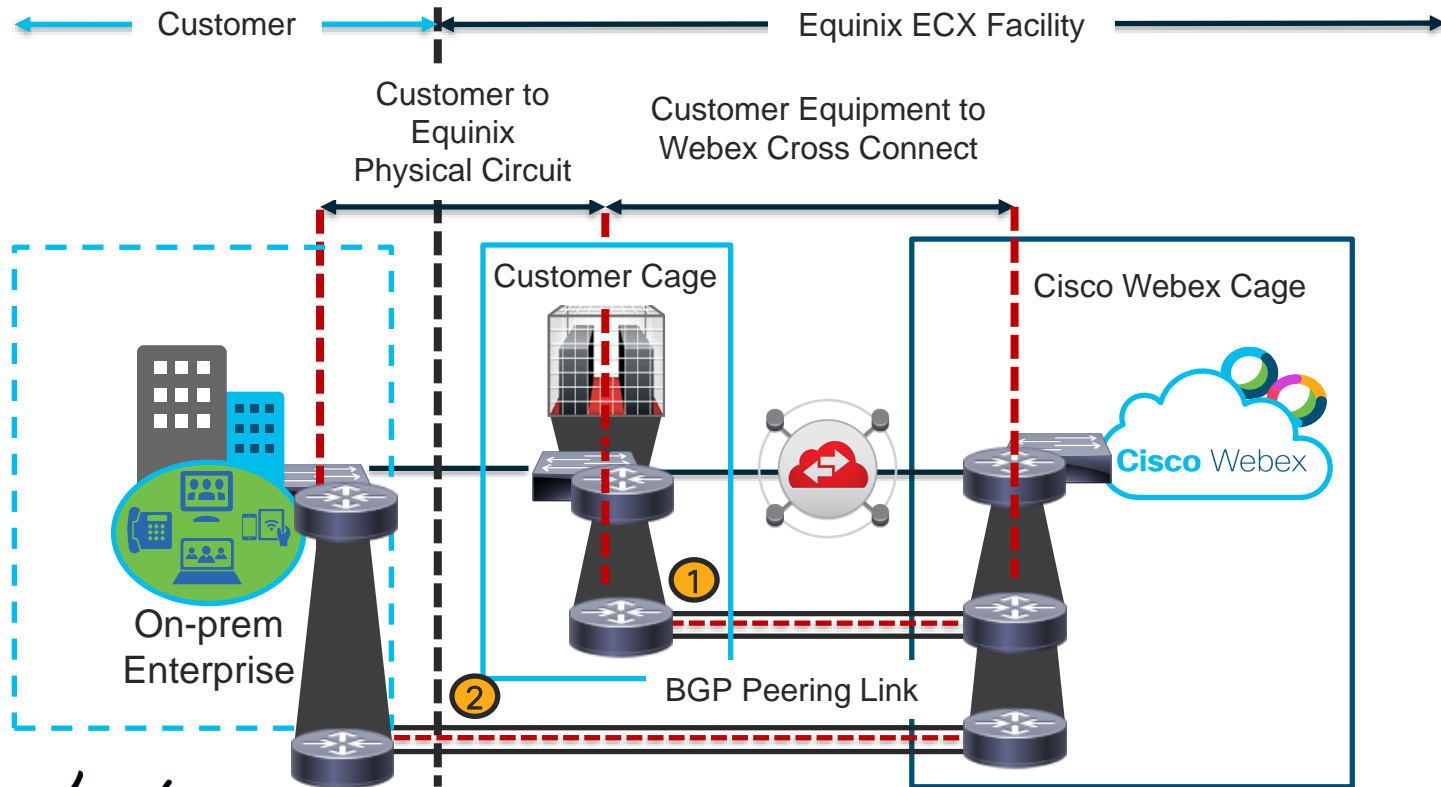
IMPORTANT ROLES AND RESPONSIBILITIES

- | | | |
|---|------------------------------------|--|
|  | 1. Layer 1 – Physical Connectivity | } Equinix responsibility:
✓ Physical link provisioning (cross connects)
✓ Virtual circuit monitoring reports & support |
|  | 2. Layer 2 – Ethernet Connectivity | |
| <hr/> | | |
|  | 3. Layer 3 – IP connectivity | } Cisco responsibility
✓ peering provisioning and support |

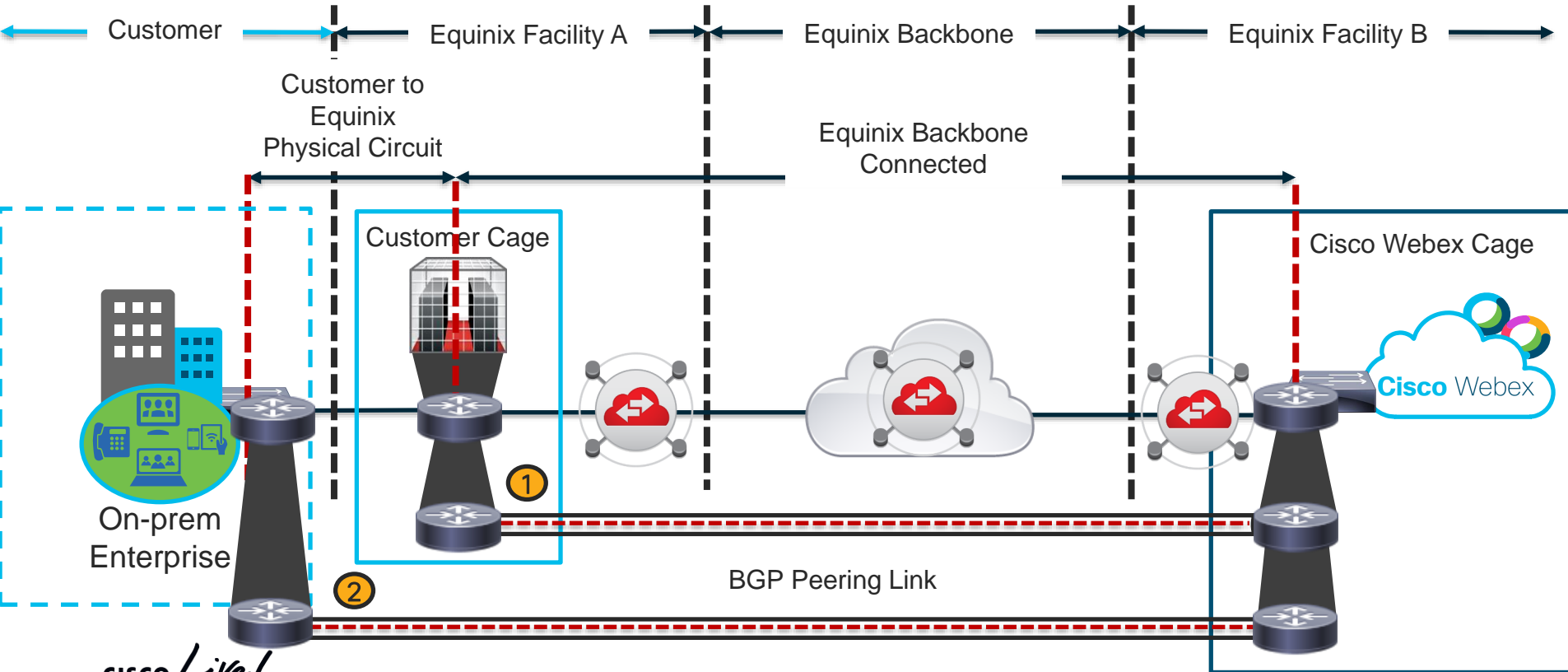


cisco *Live!*

Option 1: Equinix Cloud Exchange (ECX) Direct Peering via Customer Cage

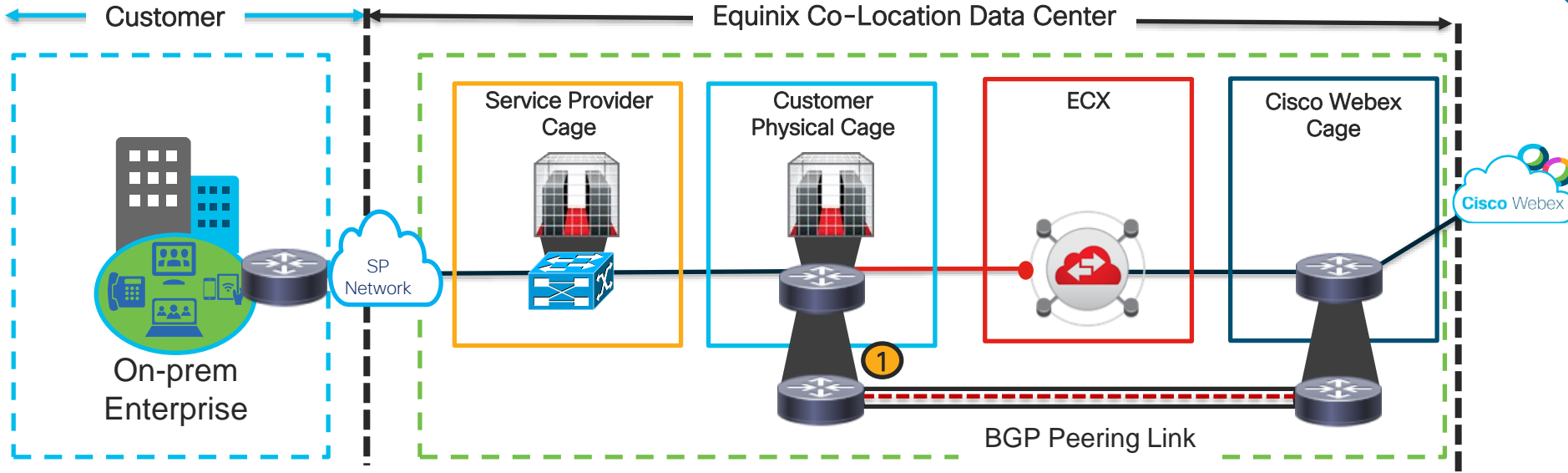


Option 1: Equinix Cloud Exchange (ECX) Direct Peering via Customer Cage 'Remote Port'



Option 2: ECX Direct Peering via Customer Cage cross connected to SP Cage

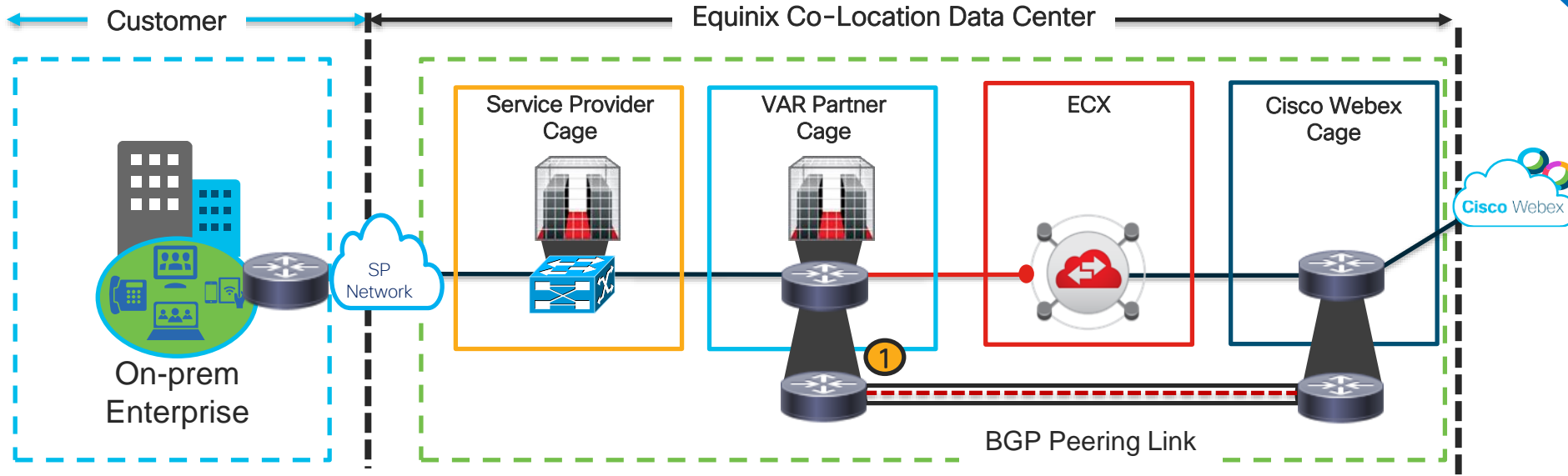
IN EFT TRIALS



When a customer has a cage within Equinix DC, the ECX virtual circuit will be considered '**Local Port & Local Connection**' with lower monthly fee from Equinix.

Option 3: Equinix Cloud Exchange Direct Peering via VAR Partner Cage

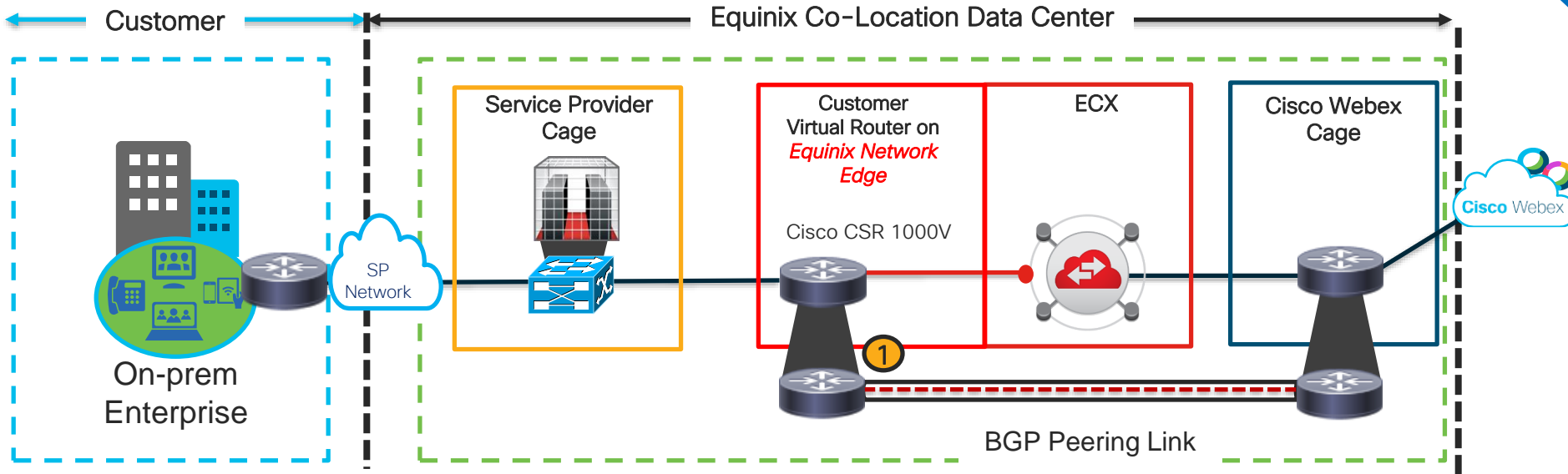
IN EFT TRIALS



In this option, VAR Partner has established a cage with Equinix and manages the equipment, ECX ports, and billing from Equinix. VAR Partner can manage virtual connections on customer's behalf or assign ECX portal permissions for customer to manage virtual connections. The VAR partner is the Equinix customer of record with a local Cage thus Local Port pricing applies.

Option 4: Equinix Cloud Exchange Direct Peering via *Network Edge*

IN EFT TRIALS



When a customer does not have a cage in Equinix DC, they can consider the new Equinix 'Network Edge' option; however, the the ECX connection will be considered a 'Remote Port' with additional monthly fees from Equinix.

Customer Requirements - Core

- Equinix Cloud Exchange (ECX) Account and Rackspace in ECX
- BGP and Dot1Q Tagging Capable Router with L3 Connectivity to the Enterprise
- Physical port [1G/10G typical] available for connecting to ECX Fabric
- Public BGP Autonomous System Number (ASN)
- An IP space that is public and provider-independent
 - Edge Connect does not accept private IP advertisements like RFC1918
- An IT team knowledgeable of BGP and peering principles

Customer Requirements – IP Routing

- IP Addressing

- Public IP - /30 or /31 supported
- Max length prefix that Webex advertises is /24
- The maximum length prefix that Webex accepts is /29
- The maximum number of routes Webex accepts is 100
- We recommend that customers allow 50 routes from Webex on the BGP peering as the number of routes that Webex advertises may change over time
- Bidirectional-Forwarding Detection (BFD) is supported and enabled with a default value of 300 ms x 3 on the Webex Edge routers
- Customer owned IP Addresses



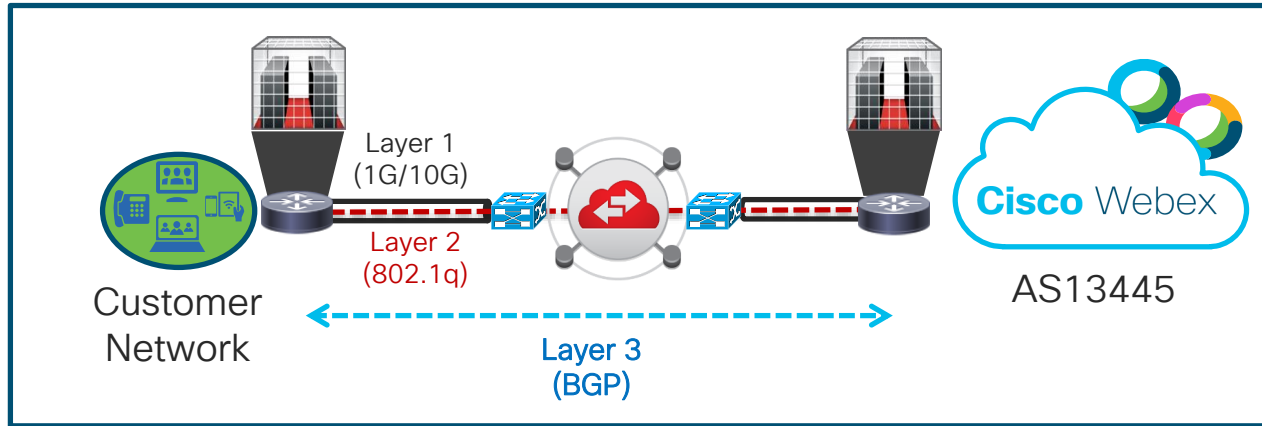
Ordering Process

- Purchase link/space in Equinix Cloud Exchange (ECX)
- Cisco Commerce Workspace (CCW): Cisco Order # used in ECX Portal
- ECX Portal to Request Port Connection
 - VLAN ID (customer side locally significant for Equinix only)
 - Purchase Order (PO) Number (From CCW order)
 - Public IP Range (/30 or /31) for BGP Peering (BYoIP - Customer and Webex side)
 - Subnets to Advertise to Webex (max /29 - max 100 subnets)
 - Public AS + password (32 bit supported)
 - Tech contact (i.e. admin group alias + phone number)
 - Link speed to provision: 200mb, 500mb, 1gb, 5gb, 10gb or increments thereof!
- Peering Provisioning Completion Email
 - L3 should be up and running

How do I
Connect?

Connectivity – Key Components




Equinix Cloud Exchange



Order Process

1. Order physical circuit to ECX fabric
2. Provision virtual circuit to Cisco Webex using Equinix self-service portal
3. Cisco enables BGP connection to the Enterprise to establish connectivity

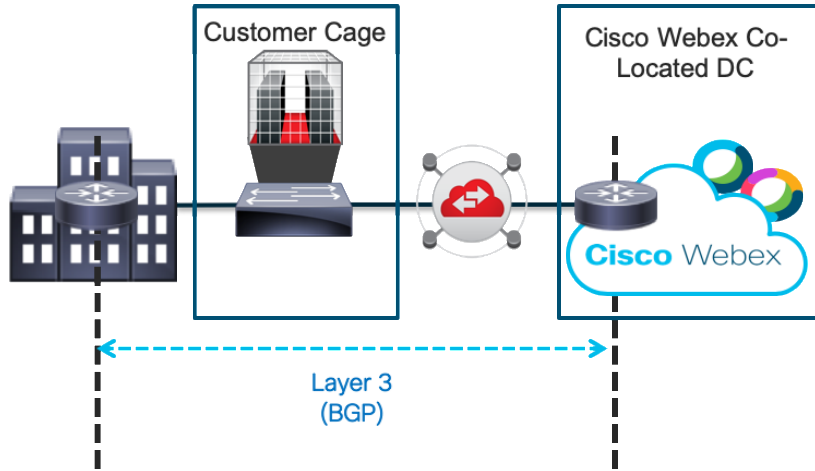
IMPORTANT ROLES AND RESPONSIBILITIES

- | | | |
|--|------------------------------------|--|
|  | 1. Layer 1 – Physical Connectivity | } Equinix responsibility:
✓ Physical link provisioning (cross connects)
✓ Virtual circuit monitoring reports & support |
|  | 2. Layer 2 – Ethernet Connectivity | |
| <hr/> | | |
|  | 3. Layer 3 – IP connectivity | } Cisco responsibility
✓ peering provisioning and support |

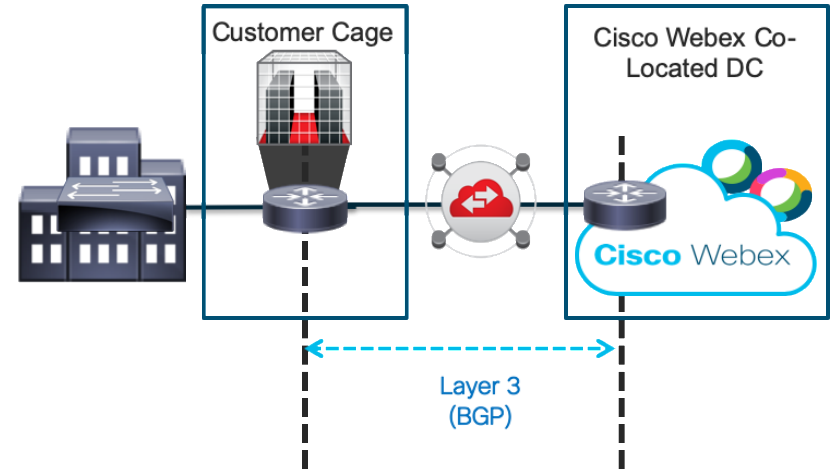
CISCO *Live!*

Equinix Cloud Exchange Connectivity

BGP Peering Router Location



BGP peering from the router in the Enterprise



BGP peering from the router in the Equinix Cage

BGP Peering Configuration – high level

Customer

- /30 or /31 IP subnet supported
- Customer public IP block – Bring your own IP (BYOIP)

(IOS-XE)

```
interface GigabitEthernet0/1/1
ip address 192.0.2.2 255.255.255.252
encapsulation dot1q 10
```

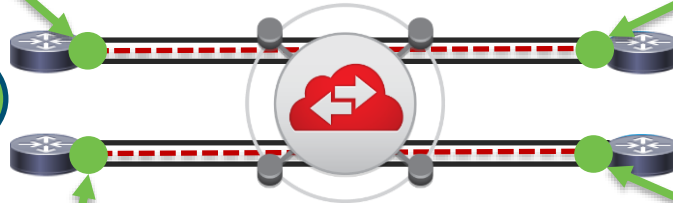
Cisco Webex

IP address is provided by customer
Gig interfaces: Webex network uses LAG bundles to support 10 Gig

(IOS-XR)

```
interface Bundle-Ether10000.2
ipv4 address 192.0.2.1/30
encapsulation dot1q 11
```

Customer Network



Cisco
Recommends
Dual peering
links for high
availability

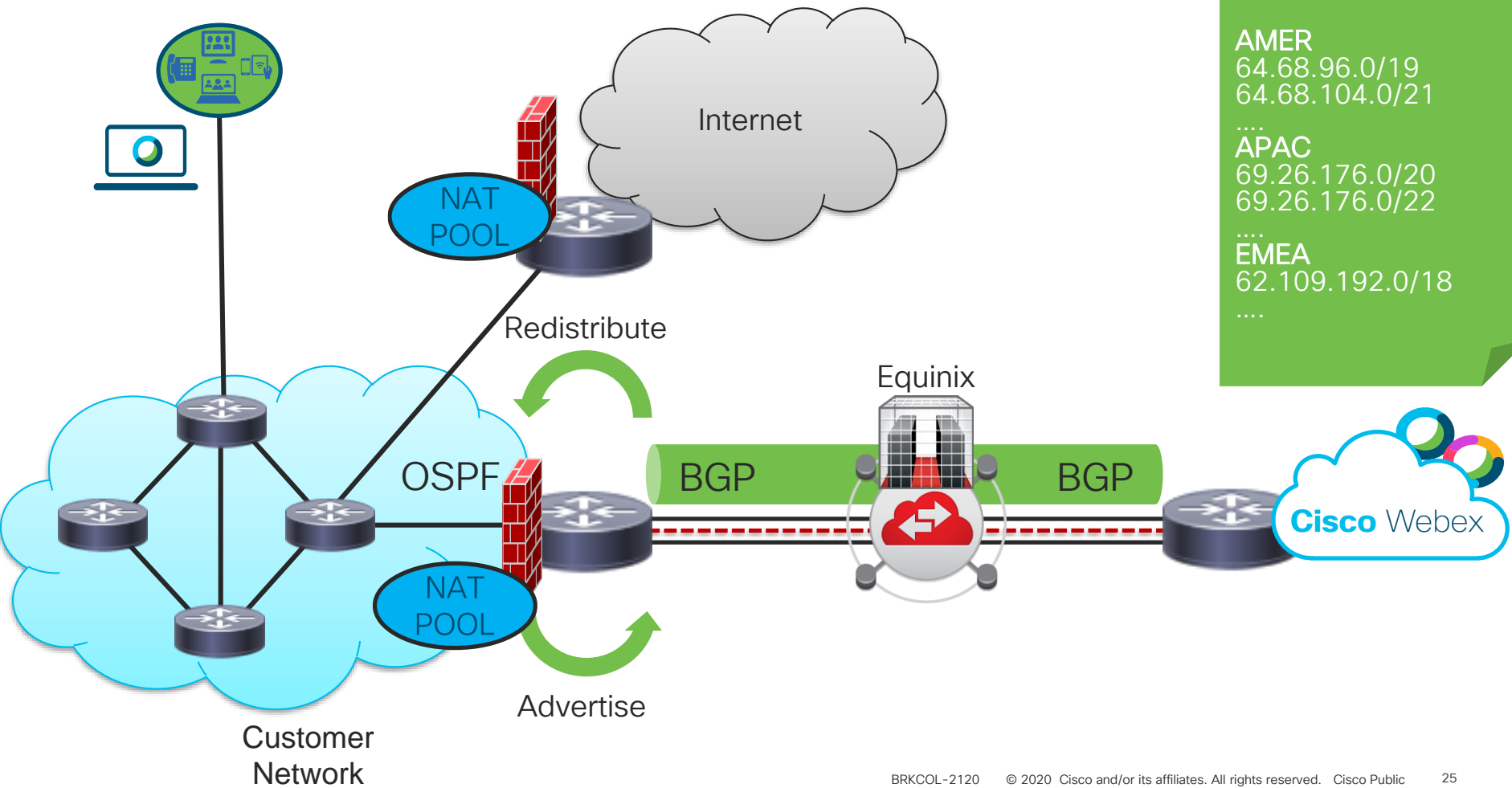
(IOS-XE)

```
interface GigabitEthernet0/1/1
ip address 192.0.2.6 255.255.255.252
encapsulation dot1q 20
```

(IOS-XR)

```
interface Bundle-Ether10000.2
ipv4 address 192.0.2.5/30
encapsulation dot1q 12
```

Note - VLAN assignment is locally significant due to ECX QinQ tagging and does not need to match on Webex & Customer sides



Webex Routes

- AMER
64.68.96.0/19
64.68.104.0/21
- ...
- APAC
69.26.176.0/20
69.26.176.0/22
- ...
- EMEA
62.109.192.0/18
- ...

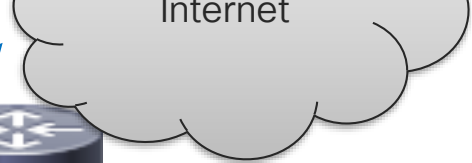
Connect to webex.com



64.68.96.55

DNS Lookup

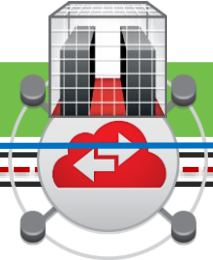
DNS Server



DNS Server



Equinix

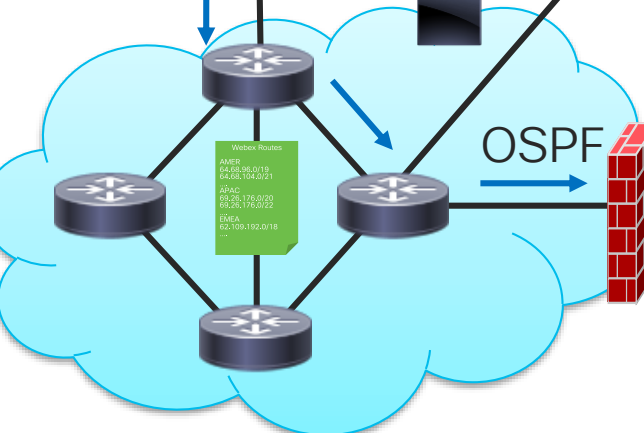


BGP

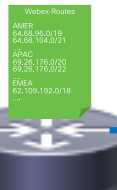
BGP



OSPF



Customer Network



Webex Routers
AMER: 64.68.96.0/18
98.25.176.0/22
APAC: 64.68.96.0/18
98.25.176.0/22
EMEA: 64.68.96.0/18
98.25.176.0/22

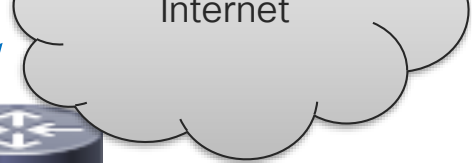
Connect to webex.com



64.68.96.55

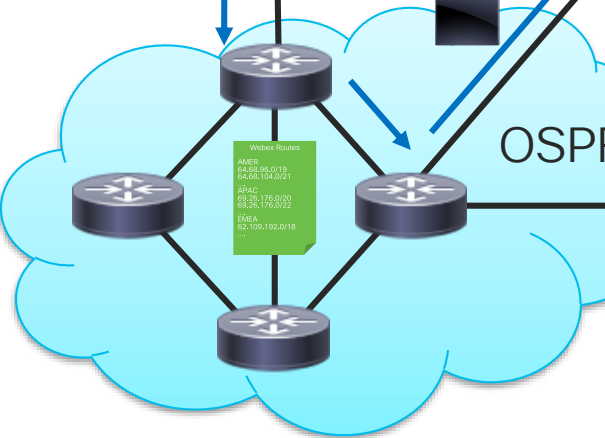
DNS Lookup

DNS Server



Internet

DNS Server



Customer Network

OSPF



Webex Routers

AMER: 64.68.96.0/18
EMEA: 62.709.192.0/18



BGP

Equinix



BGP



BGP Peering

Webex Edge Connect

Customer Requirements

- ✓ Enterprises are responsible for their network architecture
 - Avoid asymmetric routing
 - Avoid suboptimal network paths
- ✓ A connection to the Equinix Cloud Exchange
- ✓ Knowledge of BGP Routing
- ✓ Public BGP Autonomous System Number
- ✓ Public provider independent IP block
 - ✓ No RFC1918 addressing (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

Don't have the networking expertise internally?
Consider enlisting a partner or Cisco Advanced Services to ensure a successful deployment.

BGP Traffic Engineering – Customer Controlled

- All global routes are advertised by Webex Edge Connect
- We recommend using IP prefix lists to manage route advertisements
- Filter ONLY on subnet groups by Theater: North America, EMEA, AsiaPac
- No static routing – Dynamic routing routing is required
- Route advertisements may change over time so customers should accept all Webex routes with prefix length that is less than or equal to /24

BGP Traffic Engineering – Customer Controlled

Multiple options to influence traffic flow

Option 1 – BGP Community local preference tagging

- Highest level of control and routing influence
- Advanced customer configuration

Option 2 – AS-Path prepending

- Simple

Option 3 – Unique NAT Pools per peering session

- Simple
- Disruptive Fail-over



Traffic Engineering Communities

Link Priority

- **None** – Default (least desirable path)
- **13445:200** – Local Preference 200
- **13445:300** – Local Preference 300
- **13445:400** – Local Preference 400
- **13445:500** – Local Preference 500
- **13445:600** – Local Preference 600
- **13445:700** – Local Preference 700
- **13445:800** – Local Preference 800
- **13445:900** – Local Preference 900 (Most desirable path)

Webex Prefix BGP Origin communities

- **13445:10000** – AMER
- **13445:10010** – EMEA
- **13445:10020** – APAC

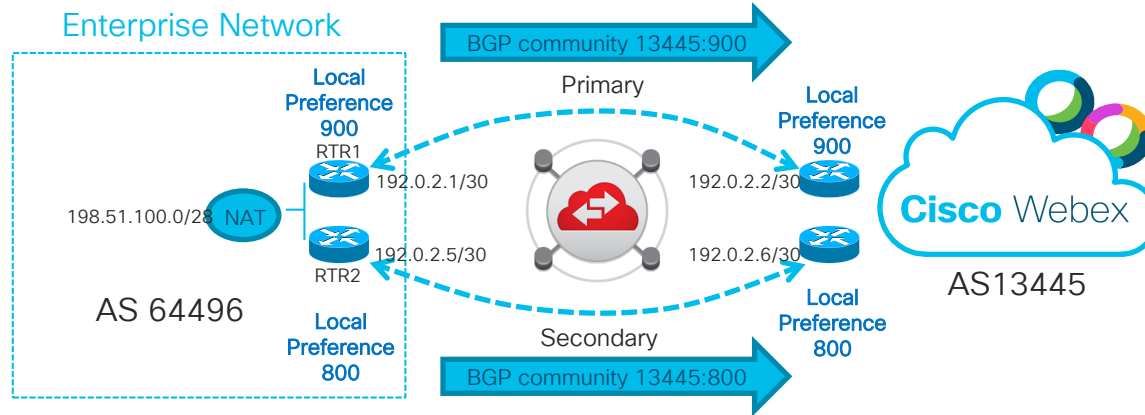
Customer Prefix propagation scoping communities

- **None** – Default permit global reachability
- **13445:677** – Permit local theater reachability

Example: Community Route Policy

IOS XE

The following diagram is an example of a typical active/standby topology. Router 1 (RTR1) is the primary path and Router 2 (RTR2) is the backup.



RTR1 Example BGP Configuration

```
router bgp 64496
neighbor 192.0.2.2 remote-as 13445
!
address-family ipv4
neighbor 192.0.2.2 activate
neighbor 192.0.2.2 send-community both
neighbor 192.0.2.2 route-map PRIMARY-OUT out
neighbor 192.0.2.2 route-map PRIMARY-IN in
exit-address-family
!
ip prefix-list ADVERTISE-TO-WEBEX seq 5 permit 198.51.100.0/28
!
route-map PRIMARY-OUT permit 10
match ip address prefix-list ADVERTISE-TO-WEBEX
set community 13445:900
!
route-map PRIMARY-IN permit 10
set local-preference 900
!
```

RTR2 Example BGP Configuration

```
router bgp 64496
neighbor 192.0.2.6 remote-as 13445
!
address-family ipv4
neighbor 192.0.2.6 activate
neighbor 192.0.2.6 send-community both
neighbor 192.0.2.6 route-map SECONDARY-OUT out
neighbor 192.0.2.6 route-map SECONDARY-IN in
exit-address-family
!
ip prefix-list ADVERTISE-TO-WEBEX seq 5 permit 198.51.100.0/28
!
route-map SECONDARY-OUT permit 10
match ip address prefix-list ADVERTISE-TO-WEBEX
set community 13445:800
!
route-map SECONDARY-IN permit 10
set local-preference 800
!
```

Webex to Enterprise network path selection:

RTR1 applies the BGP community 13445:900 and RTR2 applies the community 13445:800 to the enterprise prefix 198.51.100.0/28. The Webex cloud selects the RTR1 path because it is advertising the most desirable link priority community.

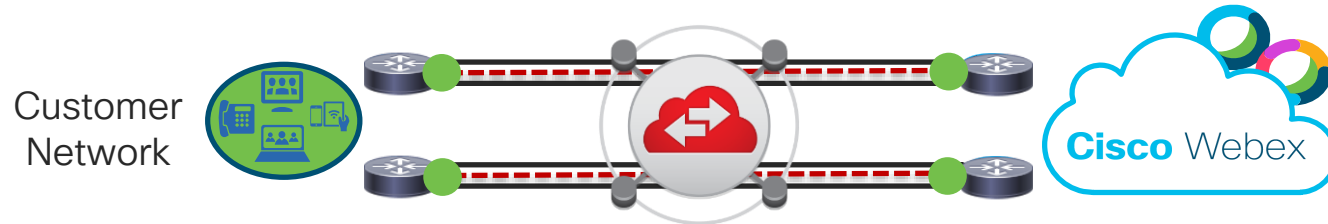
Enterprise to Webex Network path selection:

RTR1 applies a local preference of 900 and RTR2 applies a local preference of 800 to the Webex prefixes. The best path to reach the Webex cloud is RTR1 because it has assigned the highest local preference.

Webex Prefix BGP Origin communities

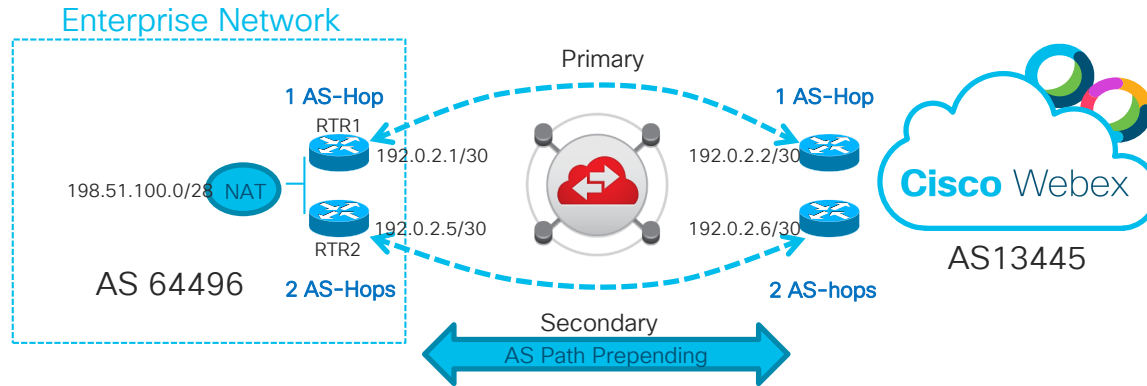
Filter routes by Origin Community (per Theater)

- 13445:10000 - AMER
- 13445:10010 - EMEA
- 13445:10020 - APAC



Example: AS-Path Prepending Route Policy

The following diagram is an example of a typical active/standby topology. Router 1 (RTR1) is the primary path and Router 2 (RTR2) is the backup.



Webex to Enterprise network path selection:

RTR2 applies AS path prepending 64496 to the enterprise prefix 198.51.100.0/28. The Webex cloud selects the RTR1 path because it is advertising the shortest AS Path.

Enterprise to Webex Network path selection:

RTR2 applies AS path prepending 13445 to the Webex prefixes. The best path to reach the Webex cloud is RTR1 because it has the shortest AS Path.

IOS XE

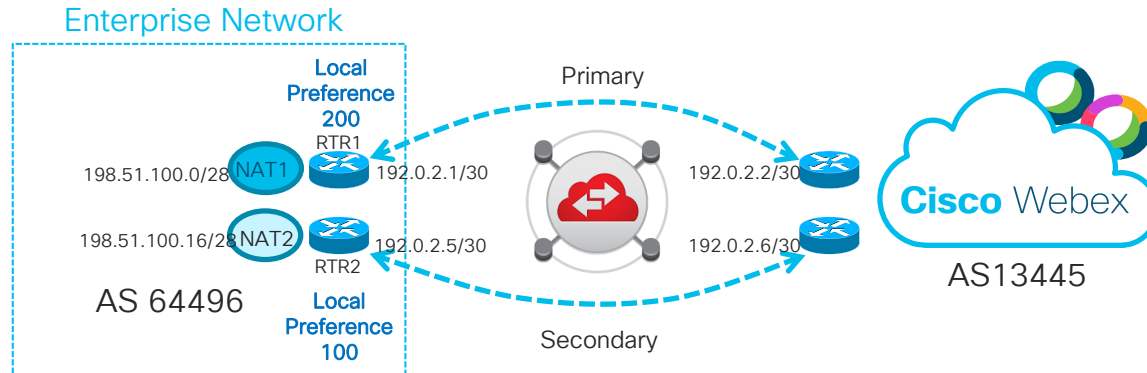
RTR2 Example BGP Configuration

```
router bgp 64496
neighbor 192.0.2.6 remote-as 13445
!
address-family ipv4
neighbor 192.0.2.6 activate
neighbor 192.0.2.6 send-community both
neighbor 192.0.2.6 route-map SECONDARY-OUT out
neighbor 192.0.2.6 route-map SECONDARY-IN in
exit-address-family
!
ip prefix-list ADVERTISE-TO-WEBEX seq 5 permit 198.51.100.0/28
!
route-map SECONDARY-OUT permit 10
match ip address prefix-list ADVERTISE-TO-WEBEX
set as-path prepend 64496
!
route-map SECONDARY-IN permit 10
set as-path prepend 13445
```

Example: Unique NAT per peering Route Policy

IOS XE

The following diagram is an example of a typical active/standby topology. Router 1 (RTR1) is the primary path and Router 2 (RTR2) is the backup.



RTR1 Example BGP Configuration

```
router bgp 64496
neighbor 192.0.2.2 remote-as 13445
!
address-family ipv4
neighbor 192.0.2.2 activate
neighbor 192.0.2.2 send-community both
neighbor 192.0.2.2 route-map PRIMARY-OUT out
neighbor 192.0.2.2 route-map PRIMARY-IN in
exit-address-family
!
ip prefix-list ADVERTISE-NAT1-TO-WEBEX seq 5 permit 198.51.100.0/28
!
route-map PRIMARY-OUT permit 10
match ip address prefix-list ADVERTISE-NAT1-TO-WEBEX
!
route-map PRIMARY-IN permit 10
set local-preference 200
```

RTR2 Example BGP Configuration

```
router bgp 64496
neighbor 192.0.2.6 remote-as 13445
!
address-family ipv4
neighbor 192.0.2.6 activate
neighbor 192.0.2.6 send-community both
neighbor 192.0.2.6 route-map SECONDARY-OUT out
neighbor 192.0.2.6 route-map SECONDARY-IN in
exit-address-family
!
ip prefix-list ADVERTISE-NAT2-TO-WEBEX seq 5 permit 198.51.100.16/28
!
route-map SECONDARY-OUT permit 10
match ip address prefix-list ADVERTISE-NAT2-TO-WEBEX
!
route-map SECONDARY-IN permit 10
set local-preference 100
```

Webex to Enterprise network path selection:

RTR1 and RTR2 are advertising unique prefixes. The Webex network will respond to the router performing the NAT.

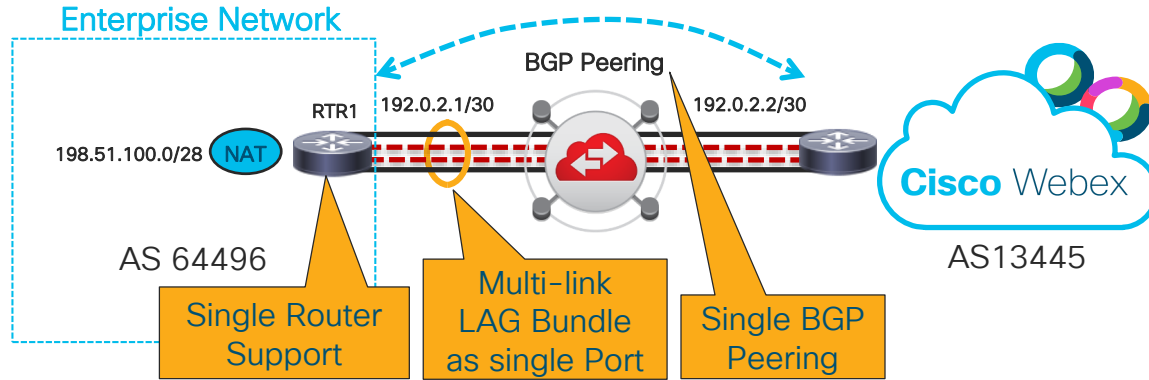
Enterprise to Webex Network path selection:

RTR1 applies a local preference of 200 to make it the most desirable path towards the Webex network.

CISCO Live!

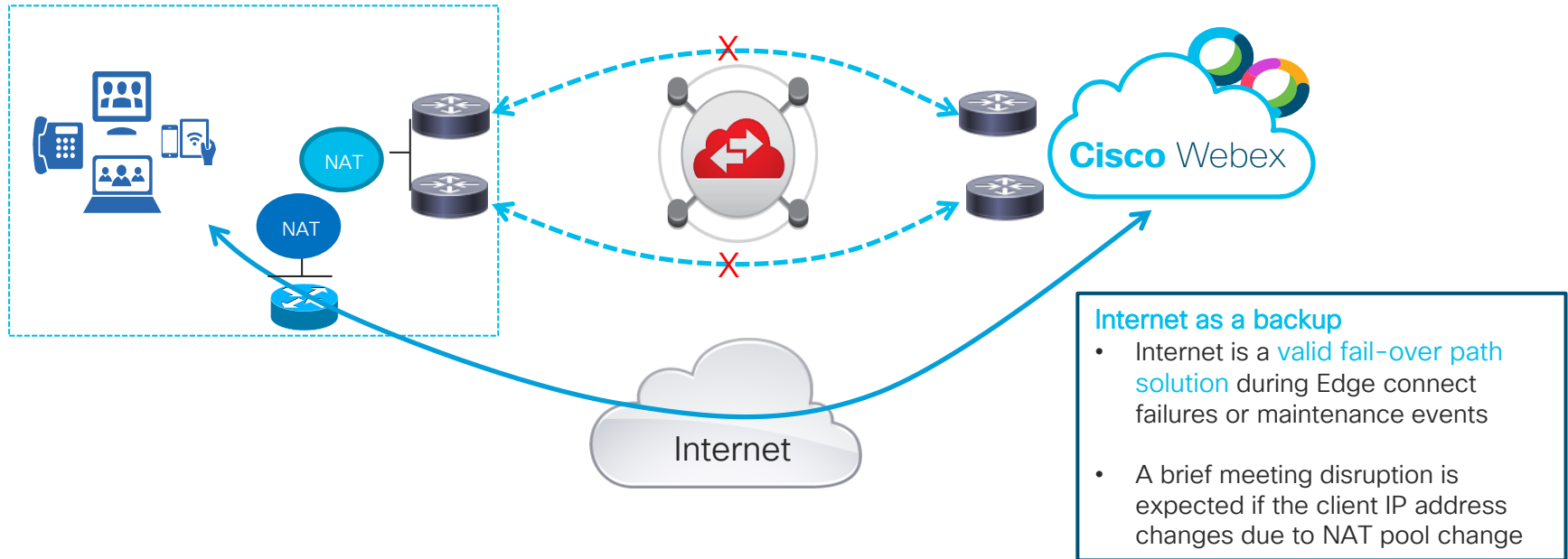
High Availability and Redundancy

Equinix Circuit



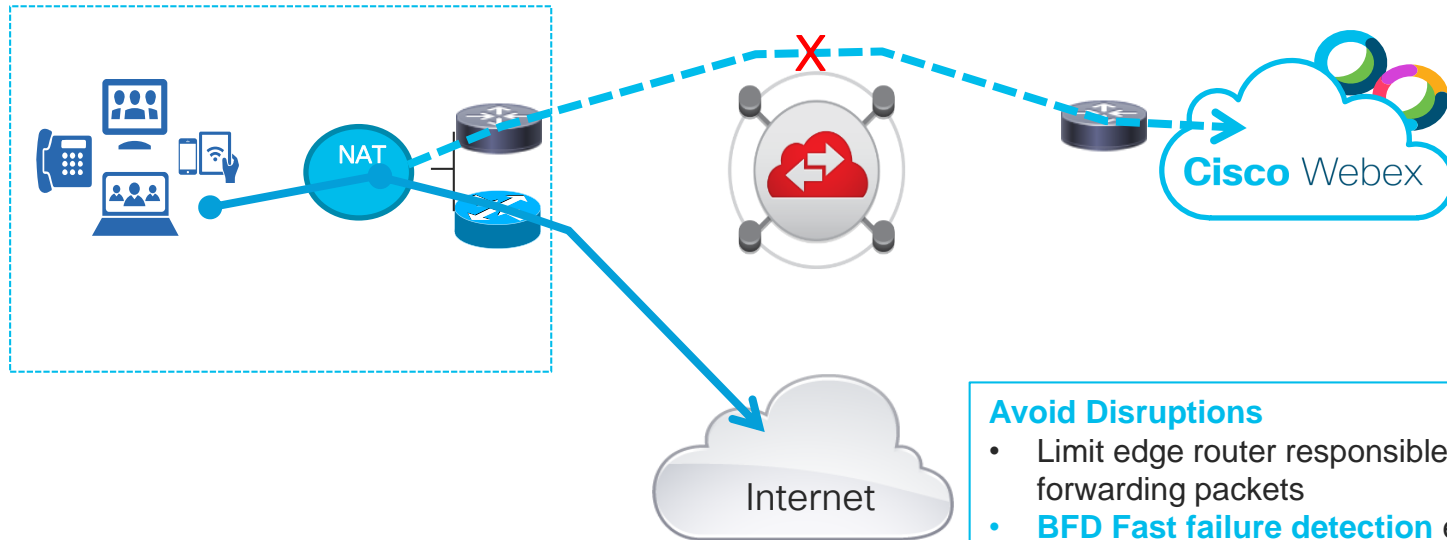
Internet as a backup

Enterprise Network



Internet as a backup

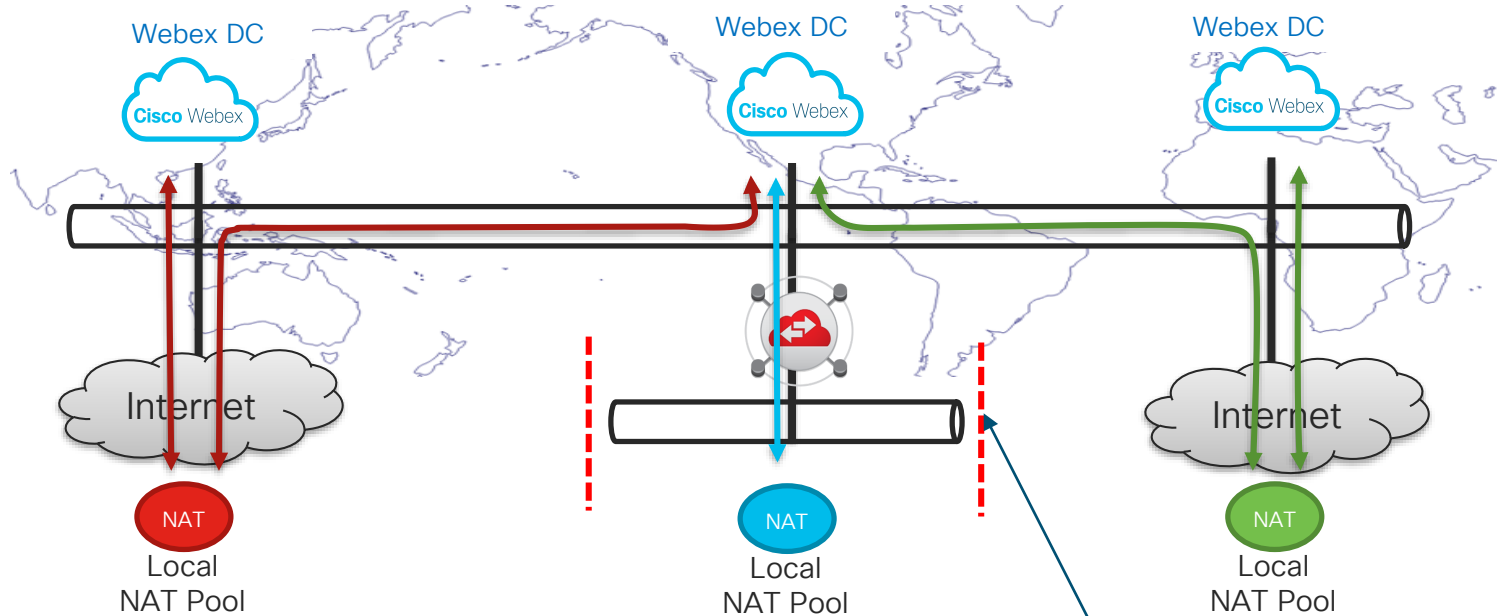
Enterprise Network



Avoid Disruptions

- Limit edge router responsible to routing and forwarding packets
- **BFD Fast failure detection** ensures meeting traffic is redirected over alternative available links to prevents meeting disruptions
- **Perform NAT on a device inside network**

Hybrid Peering: Edge Connect and Direct Internet Access

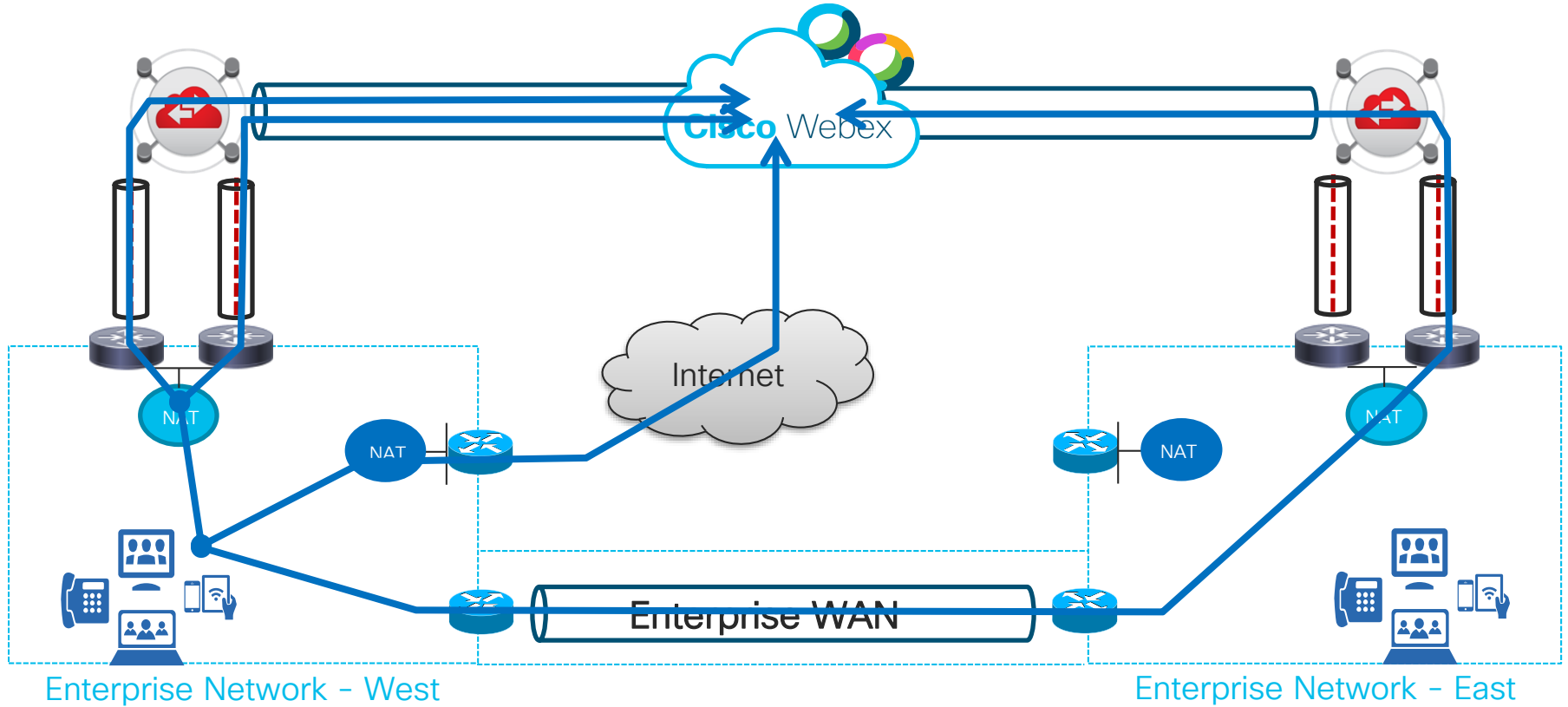


Enterprise Network

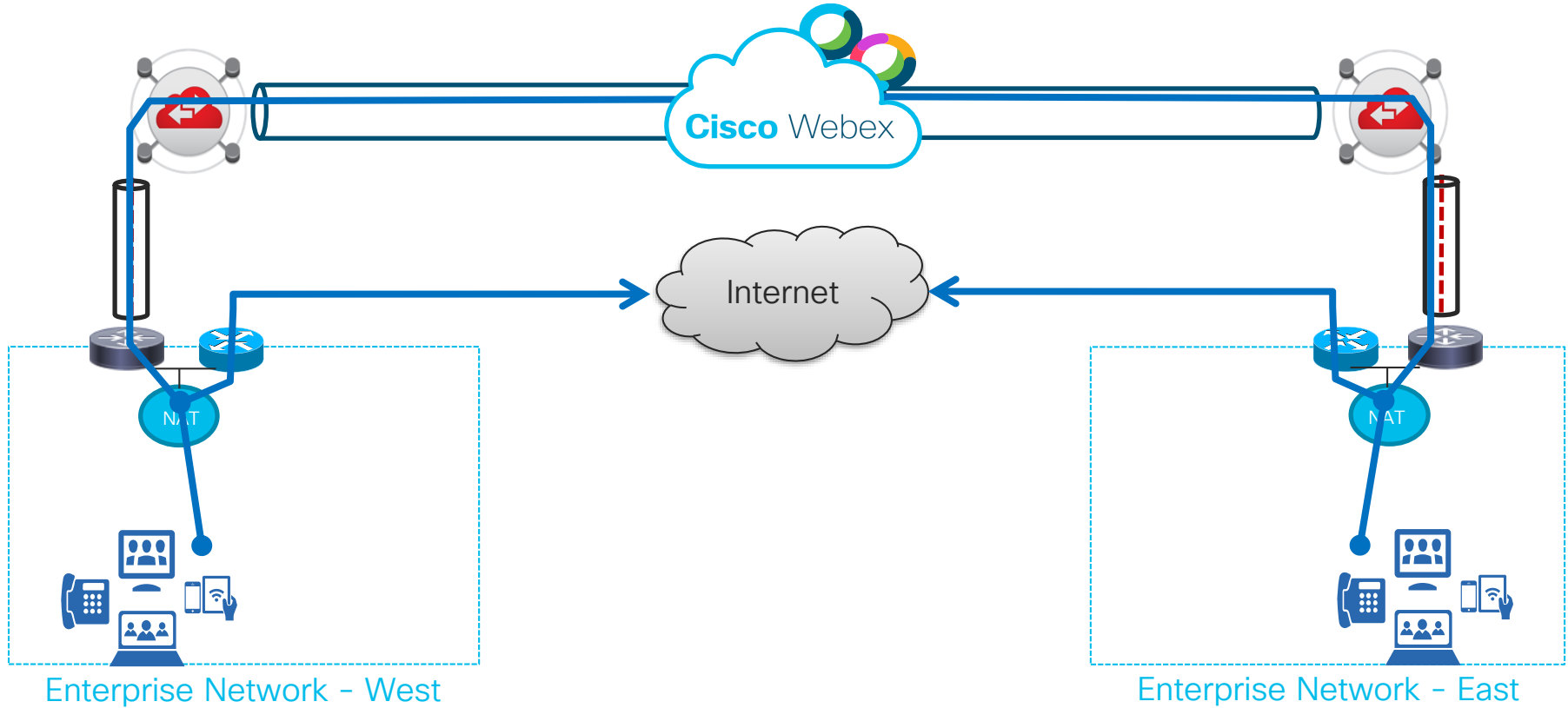


Enterprises will need to limit route leaking across their WAN to ensure remote offices utilize local Internet paths

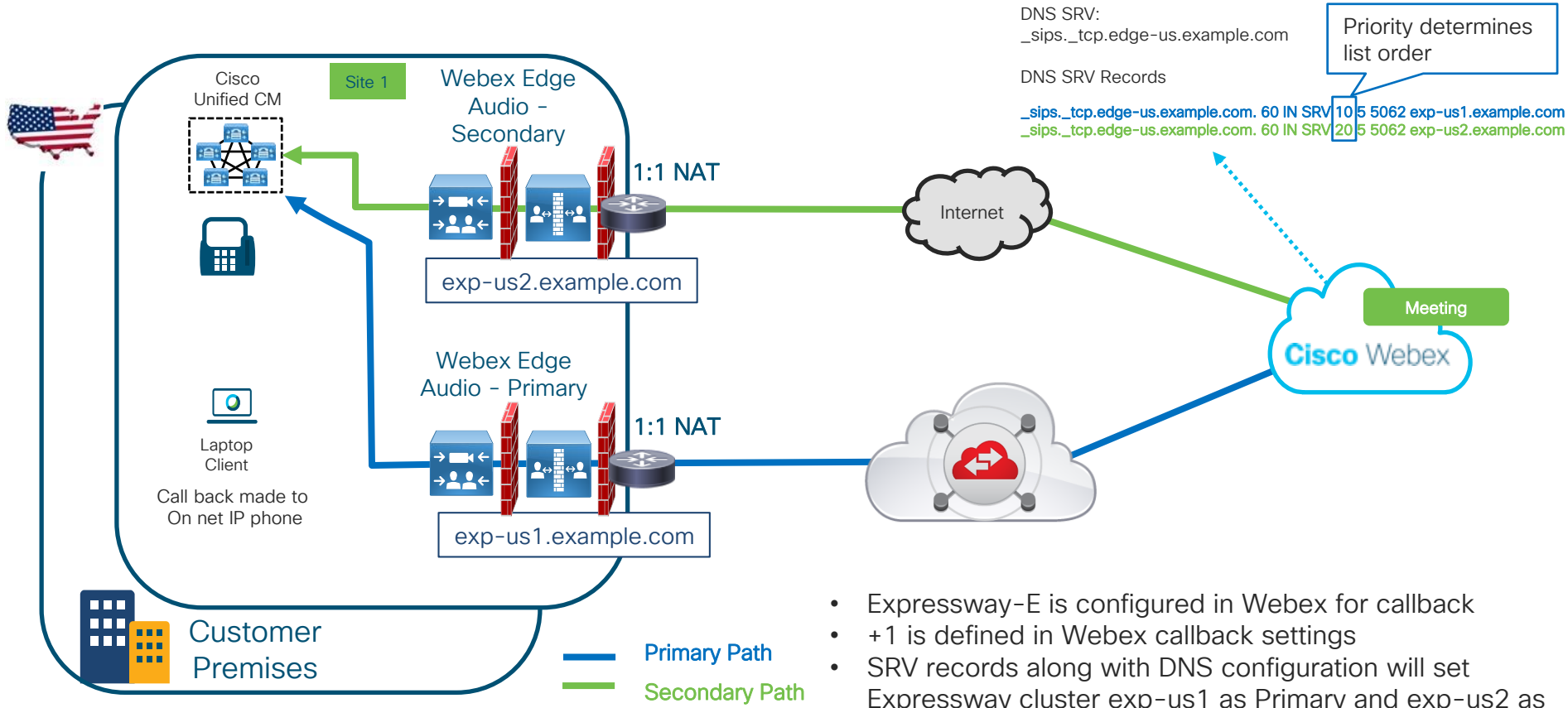
Link Redundancy and Site Redundancy



Link Redundancy and Site Redundancy



Edge Audio w/ Edge Connect using Internet as Backup



- Expressway-E is configured in Webex for callback
- +1 is defined in Webex callback settings
- SRV records along with DNS configuration will set Expressway cluster exp-us1 as Primary and exp-us2 as Secondary



What level of redundancy is desired?

Link Level Redundancy?

- Cost vs other redundancy options
- Expressway solution considerations
- Seamless recovery

Site to Site redundancy?

- Can the MAN/WAN support the traffic load?
- Changing NAT pools can cause service disruption

Failover to Direct Internet Access (DIA)?

- Use your DIA link as a redundant option
- Changing NAT pools can cause service disruption

Webex Traffic Flows over Edge Connect

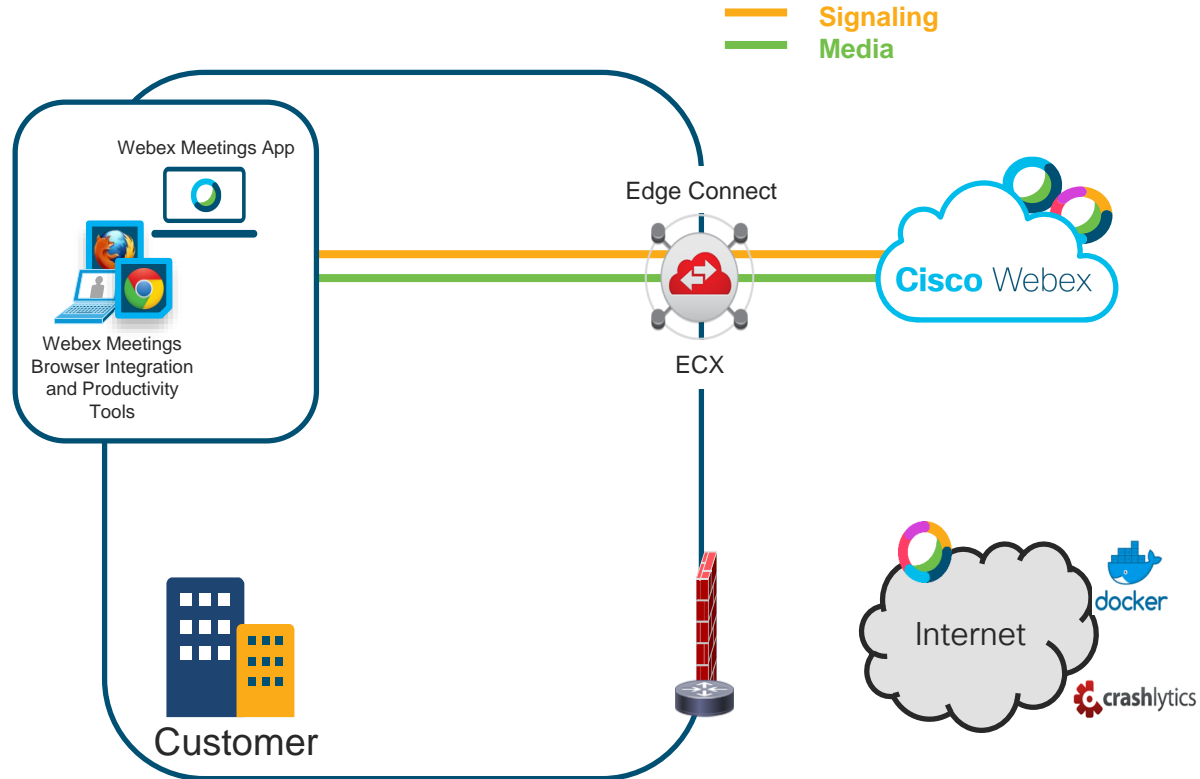
Webex Edge Connect - Traffic

Signaling and Media

Edge Connect Peering Link

Webex Meetings App **Signaling** and **Media**

Public Internet



Webex Edge Connect - Traffic

Signaling and Media

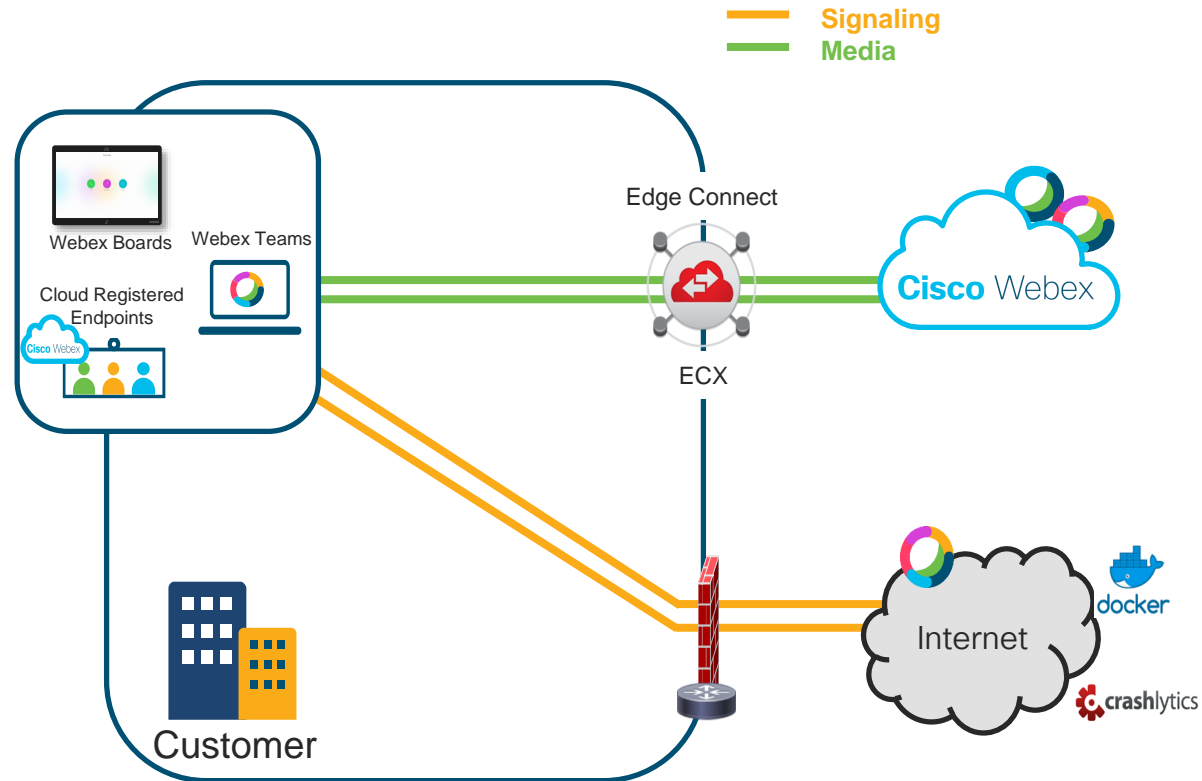
Edge Connect Peering Link

Webex Meetings App **Signaling** and **Media**

Webex Teams, Board and Endpoint's **Media**

Public Internet

Webex Teams, Board and Endpoint's **Signaling**



Webex Edge Connect - Traffic

Signaling and Media

Edge Connect Peering Link

Webex Meetings App **Signaling** and **Media**

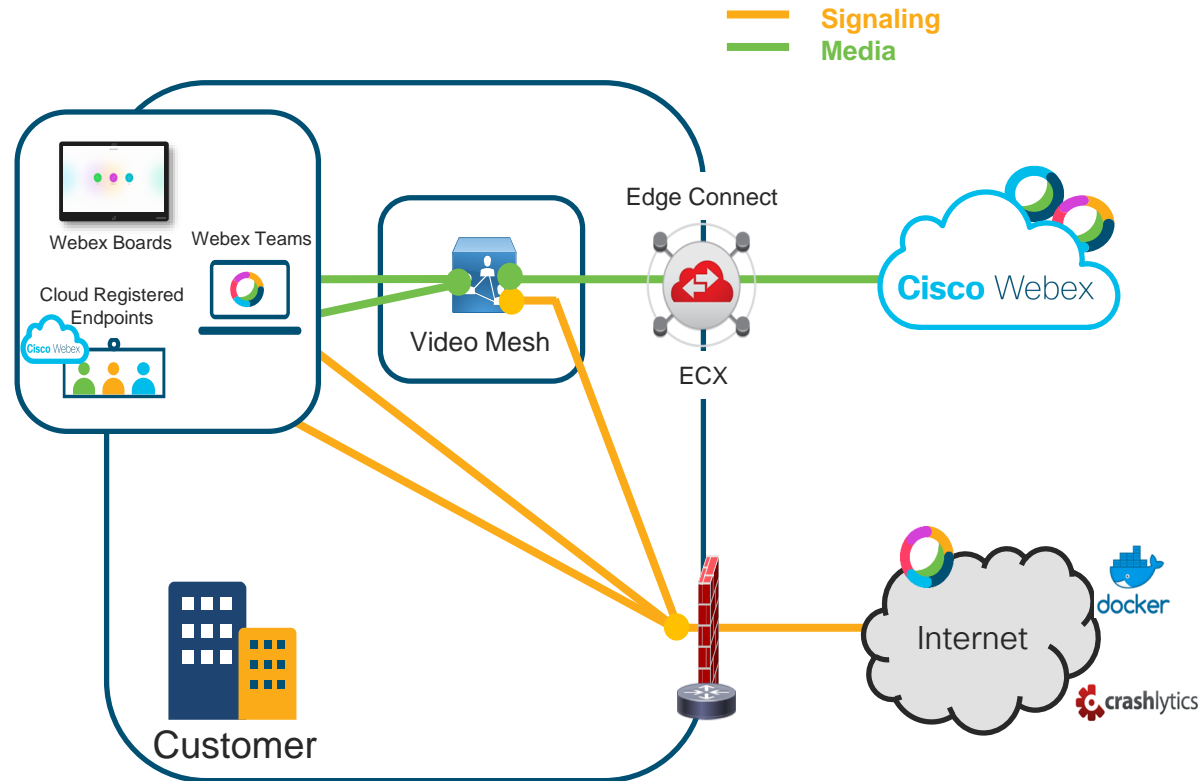
Webex Teams, Board and Endpoint's **Media**

Video Mesh Cascade **Media**

Public Internet

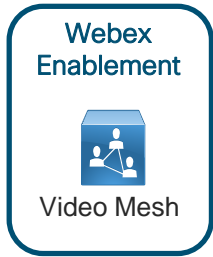
Webex Teams, Board and Endpoint's **Signaling**

Video Mesh **Signaling**



Unified CM integration – Video Mesh

Signaling and Media



Edge Connect Peering Link

Webex Meetings App **Signaling** and **Media**

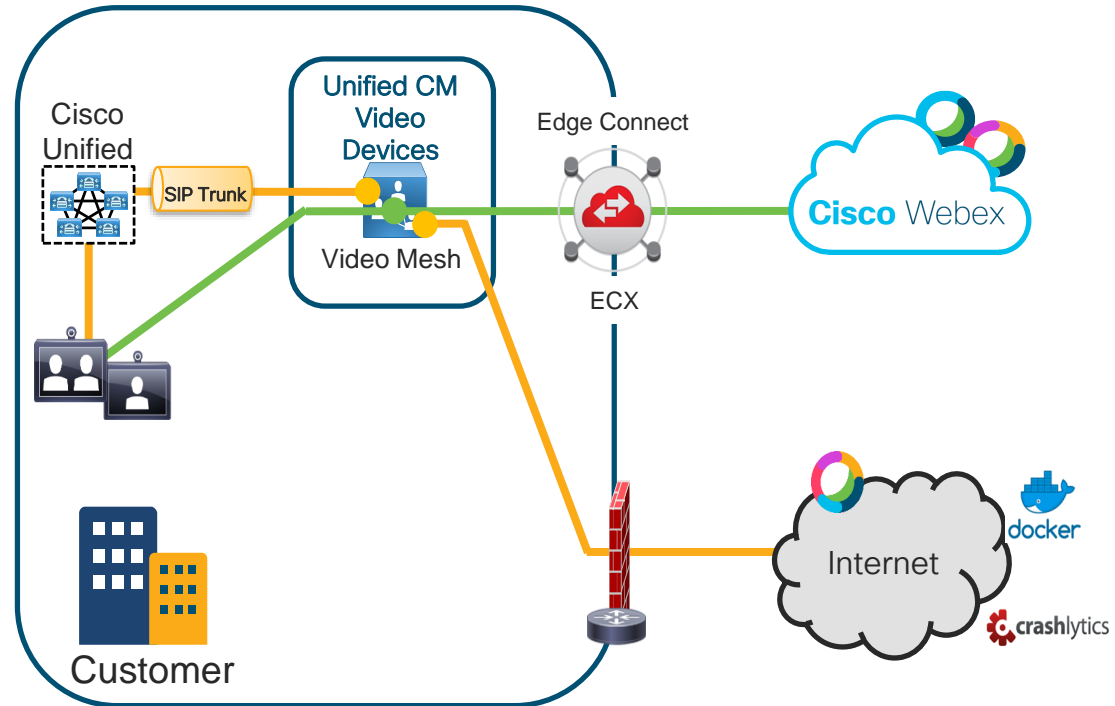
Webex Teams, Board and Endpoint's **Media**

Video Mesh Cascade **Media**

Public Internet

Webex Teams, Board and Endpoint's **Signaling**

Video Mesh **Signaling**



Unified CM Integration – Video Device-Enabled Cisco Webex Meetings

Signaling and Media

Edge Connect Peering Link

Webex Meetings App **Signaling** and **Media**

Webex Teams, Board and Endpoint's **Media**

Video Mesh Cascade **Media**

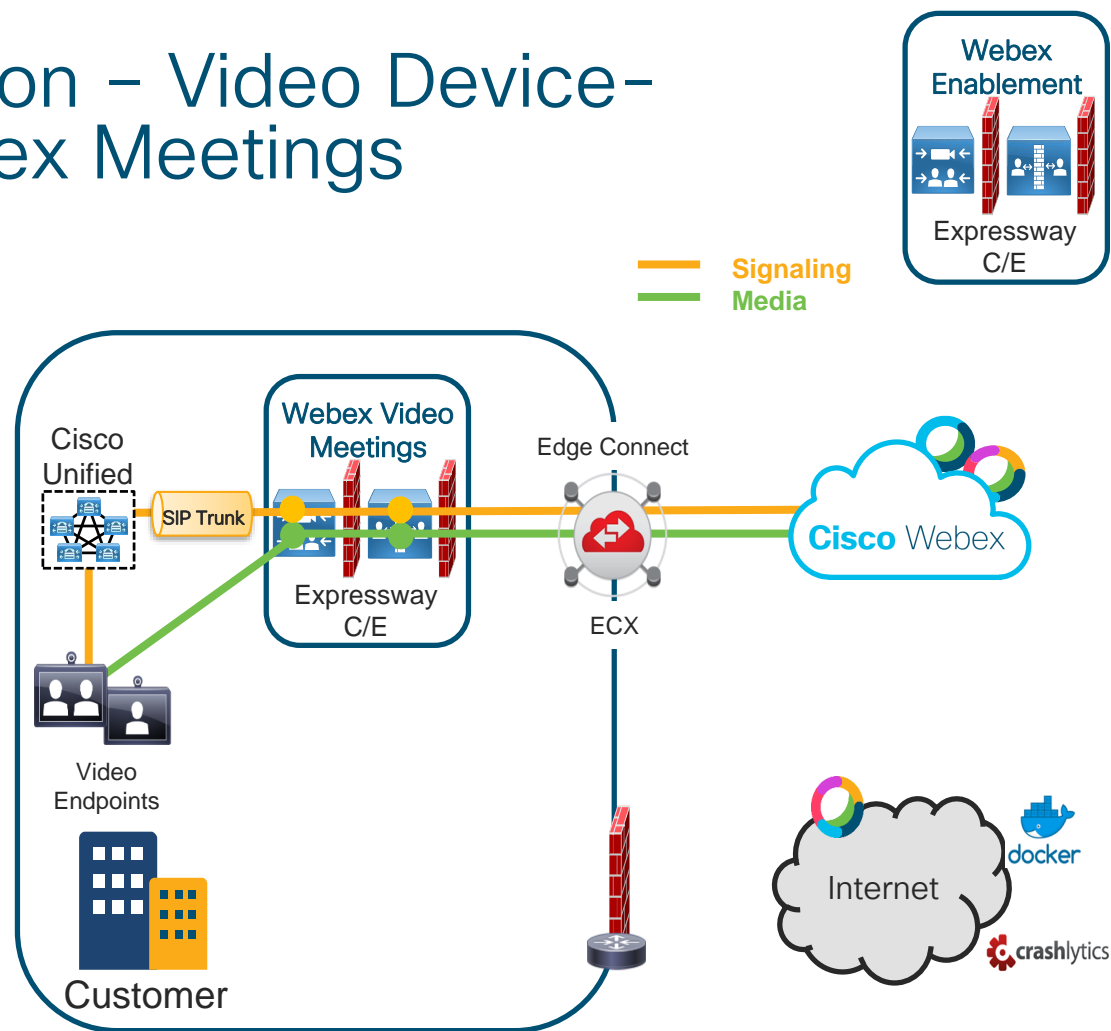
Expressway **Signaling** and **Media**

Public Internet

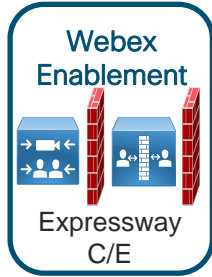
Webex Teams, Board and Endpoint's **Signaling**

Video Mesh **Signaling**

cisco *Live!*



Unified CM Integration – Webex Edge Audio



Edge Connect Peering Link

Webex Meetings App **Signaling** and **Media**

Webex Teams, Board and Endpoint's **Media**

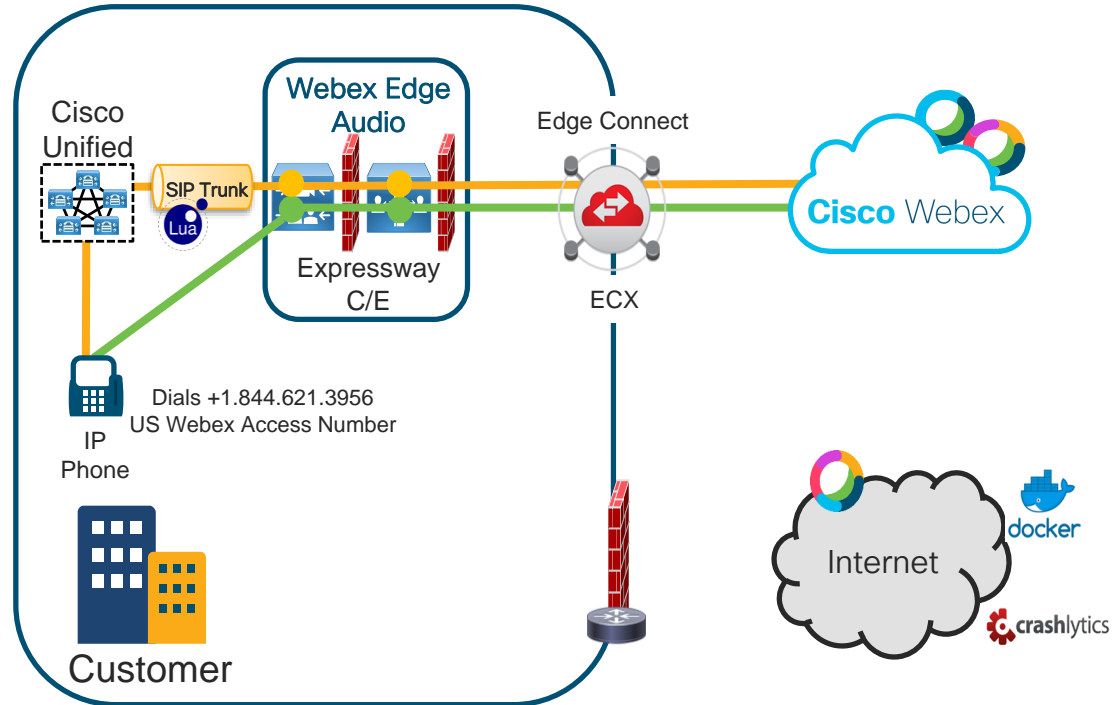
Video Mesh Cascade **Media**

Expressway **Signaling** and **Media**

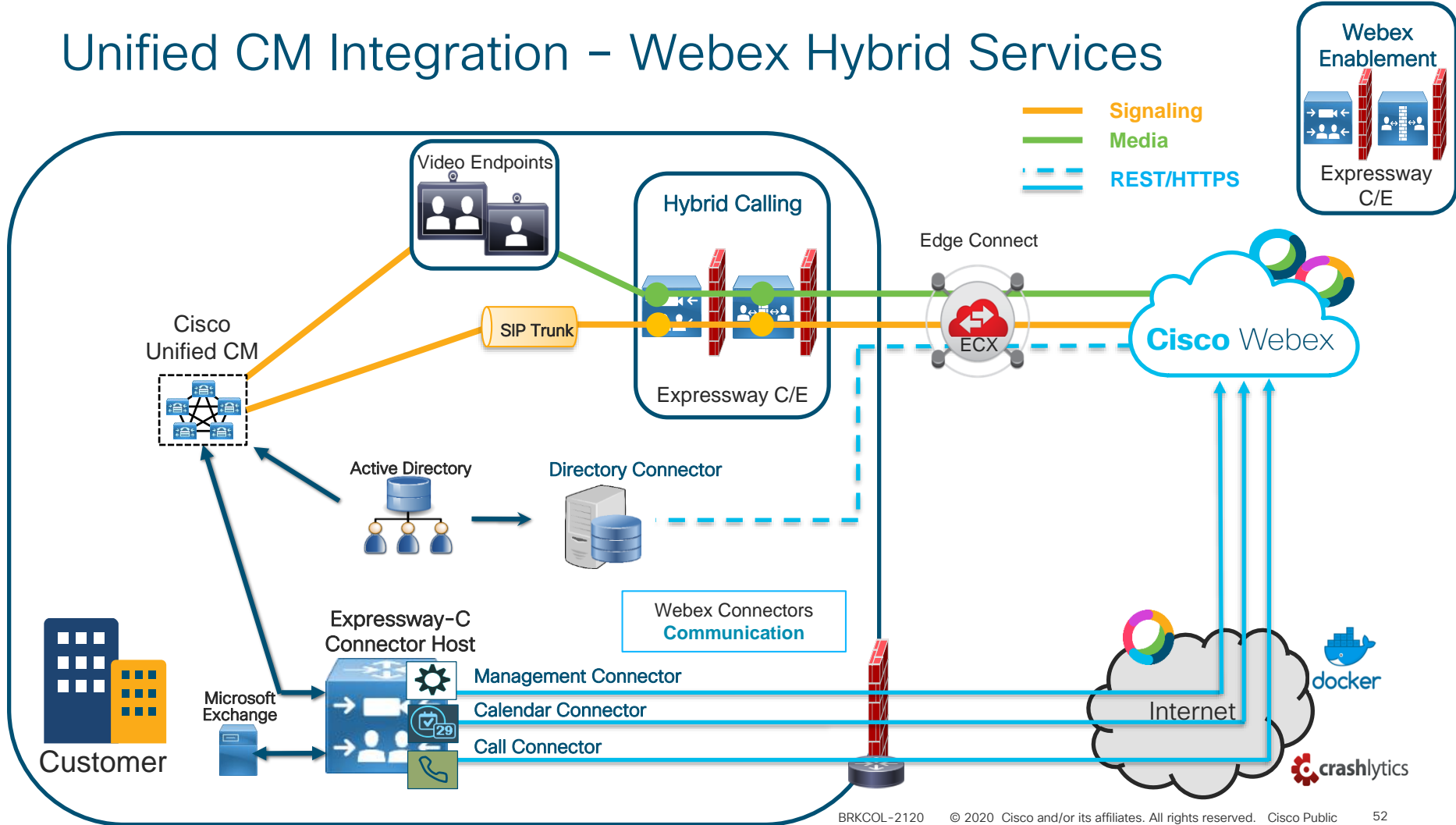
Public Internet

Webex Teams, Board and Endpoint's **Signaling**

Video Mesh **Signaling**



Unified CM Integration - Webex Hybrid Services



Connect to webex.com



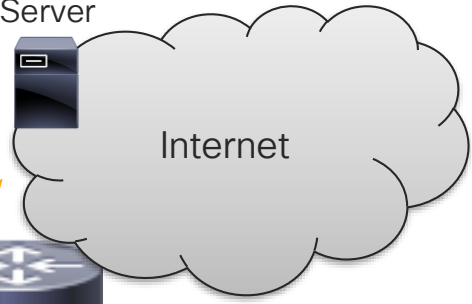
64.68.96.55

Signaling

Media

DNS Server

DNS Lookup

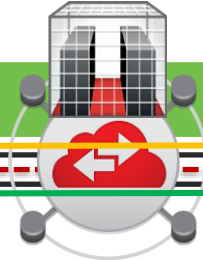


Internet

DNS Server



Equinix



BGP

BGP

Cisco Webex

Webex Routes
AMER
64.68.96.0/19
64.68.104.0/21
...
APAC
69.26.176.0/20
69.26.176.0/22
...
EMEA
62.109.192.0/18
...

OSPF



Customer Network

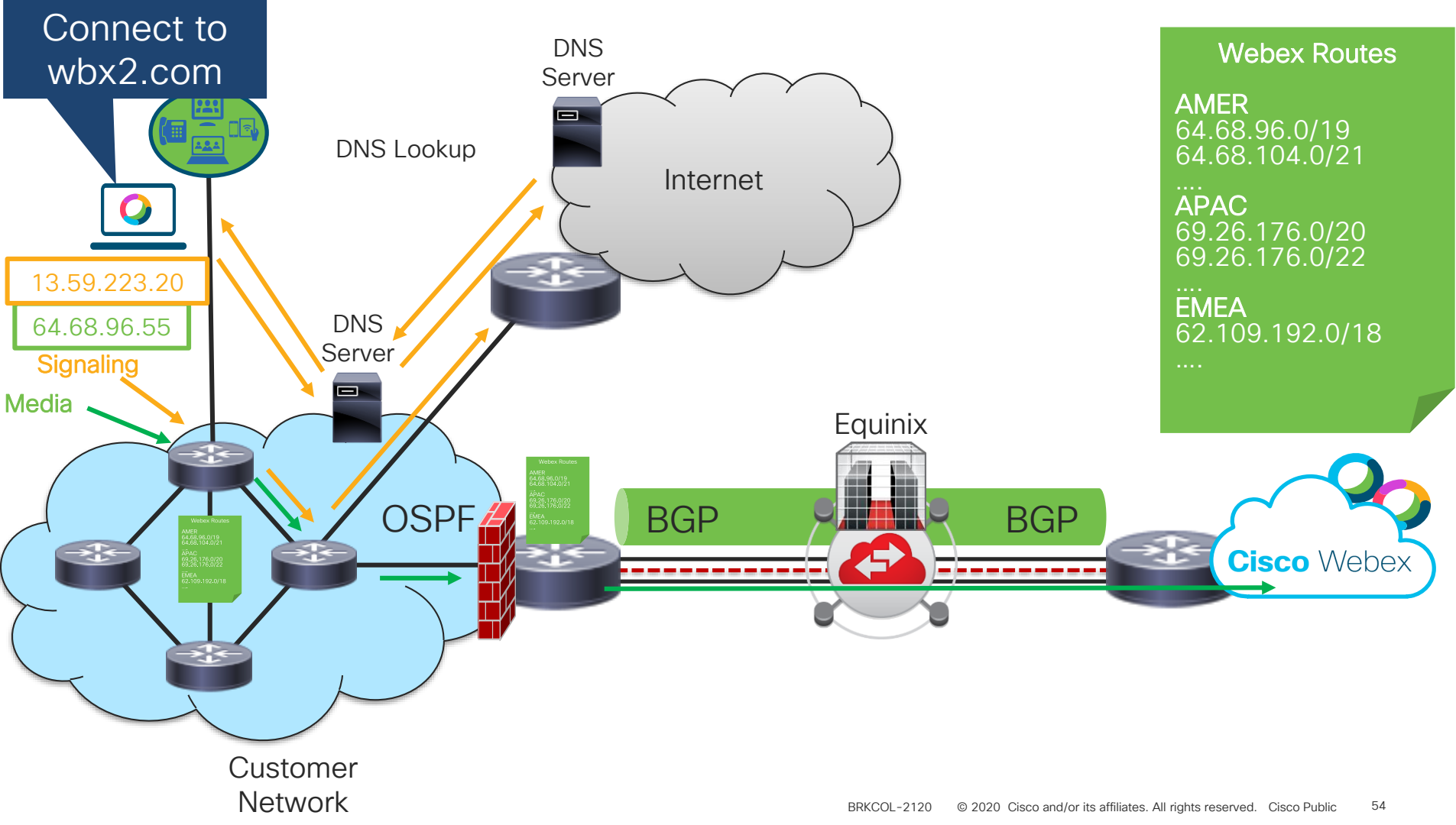
Webex Routes

AMER
64.68.96.0/19
64.68.104.0/21
...

APAC
69.26.176.0/20
69.26.176.0/22
...

EMEA
62.109.192.0/18
...

Connect to wbx2.com



Webex Routes

- AMER
64.68.96.0/19
64.68.104.0/21
- ...
- APAC
69.26.176.0/20
69.26.176.0/22
- ...
- EMEA
62.109.192.0/18
- ...

13.59.223.20

64.68.96.55

Signaling

Media

DNS Lookup

DNS Server

Internet

DNS Server

Equinix

BGP

BGP

Cisco Webex

Webex Routes

- AMER
64.68.96.0/19
64.68.104.0/21
- APAC
69.26.176.0/20
69.26.176.0/22
- EMEA
62.109.192.0/18
- ...

Webex Routes

- AMER
64.68.96.0/19
64.68.104.0/21
- APAC
69.26.176.0/20
69.26.176.0/22
- EMEA
62.109.192.0/18
- ...

Customer Network

Connecting to Webex through Enterprise Firewalls: Webex Teams Apps and Devices

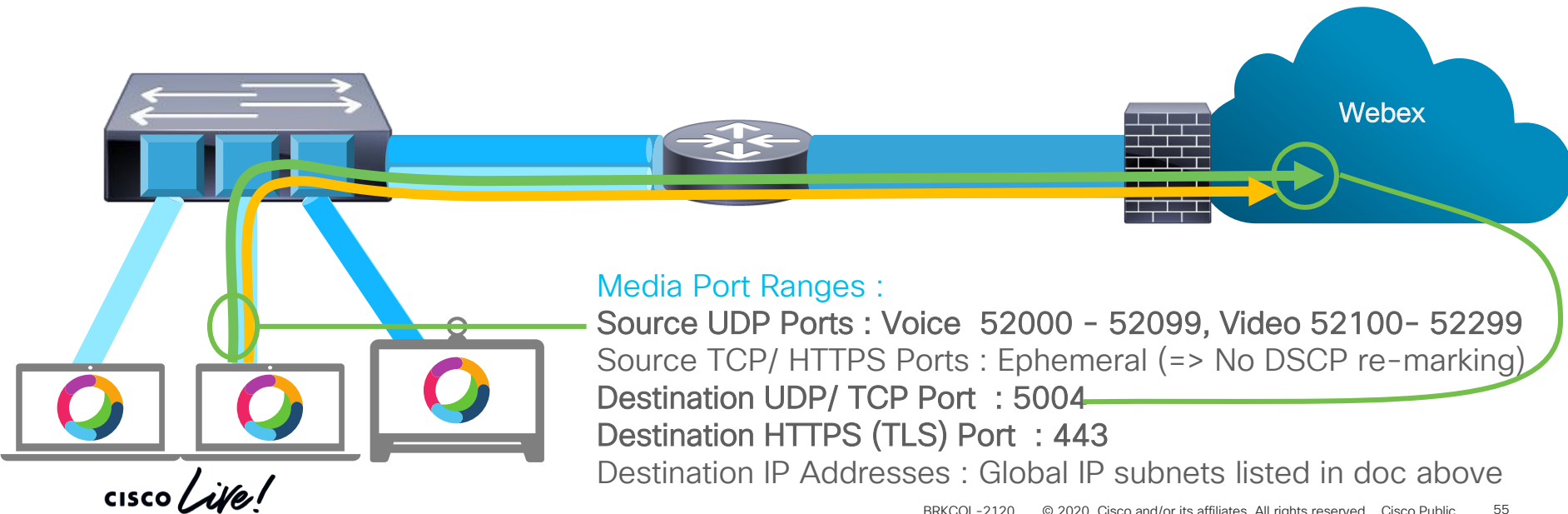
— Signalling
— UDP Media

Firewalls : Whitelisting Ports and Destinations

You will need to allow Webex Teams media and signaling traffic to pass through your Enterprise Firewall – For white listing details refer to :

Webex Teams Network Requirements doc :

<https://collaborationhelp.cisco.com/article/en-us/WBX000028782>



Media Port Ranges :

Source UDP Ports : Voice 52000 - 52099, Video 52100- 52299

Source TCP/ HTTPS Ports : Ephemeral (=> No DSCP re-marking)

Destination UDP/ TCP Port : 5004

Destination HTTPS (TLS) Port : 443

Destination IP Addresses : Global IP subnets listed in doc above

Firewall rules continued

Webex Teams, Board and Registered Video Endpoints

Include all rules outlined in the following documents:

Webex Meetings: <https://collaborationhelp.cisco.com/article/en-us/WBX264>

Webex Teams & Boards: <https://collaborationhelp.cisco.com/article/en-us/WBX000028782>

Note - Teams, Board and Registered Video Endpoints signaling service and messaging requires [Internet access](#).

Internet
access
required

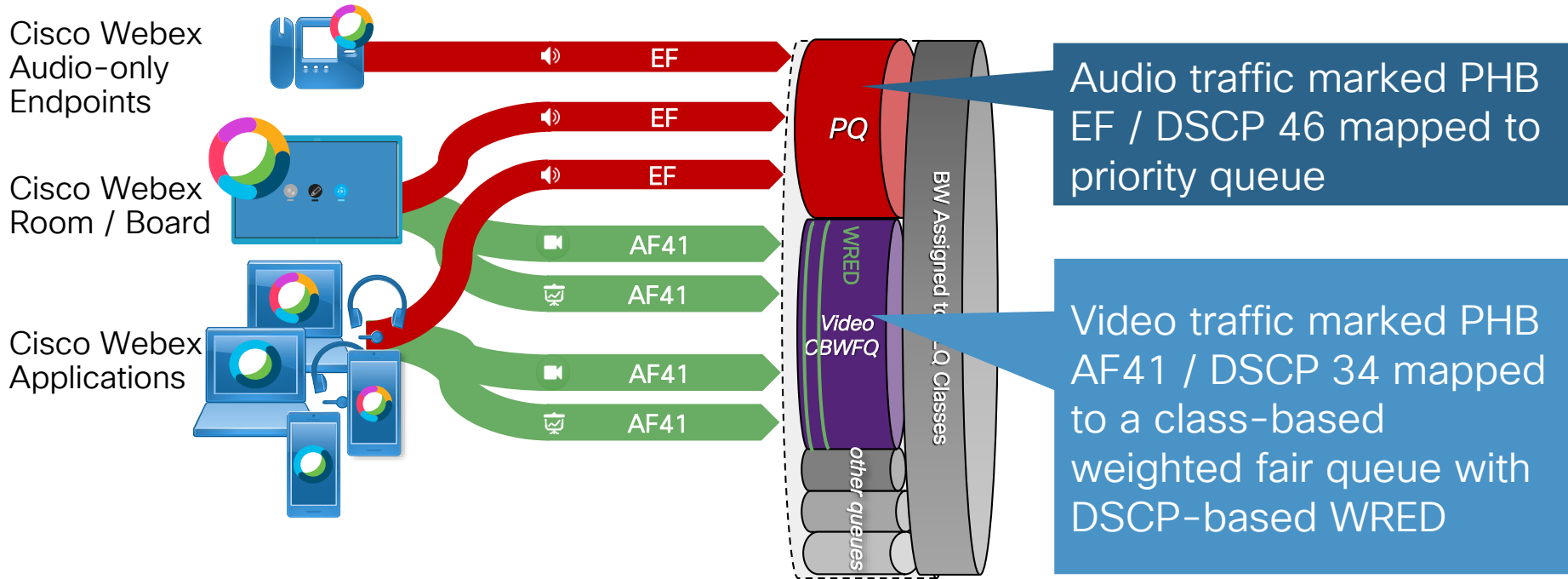
Source IP	Destination IP	Destination Port	Protocol	Description	Devices using this rule
Your networks	ANY	443	TLS	HTTPS and WSS for signalling and messaging. If your firewall supports DNS resolution, or you are using a proxy; use these Webex Teams URLs to white list access to Webex Teams services.	All
Video Mesh Node	ANY	444	TCP	Cascade Signalling	Video Mesh Node cascade signalling to Webex Cloud
Video Mesh Node	ANY	123	UDP	Network Time Protocol	Video Mesh Node NTP
Video Mesh Node	ANY	53	TCP/UDP	Domain Name System	Video Mesh Node DNS
Your Networks	Webex Collaboration Cloud 5004 (1)		UDP SRTP	Secure audio, video. Content sharing on Webex Teams devices	All
Your Networks	Webex Collaboration Cloud 5004		TCP SRTP	Used for secure content sharing on Webex Teams desktop and mobile apps. Also serves as a fallback transport for audio and video if UDP cannot be used.	All except Webex Board
Your Networks	Webex Collaboration Cloud 443		TLS/HTTPS SRTP	Used as a fallback transport for audio, video and content sharing if UDP and TCP cannot be used.	Webex Teams desktop and mobile apps
Video Mesh Nodes in your networks	Webex Collaboration Cloud 5004		UDP SRTP	Secure audio, video & content sharing media from Video Mesh Node to the Webex Cloud (TCP also supported, but not recommended)	Video Mesh Node Cascade connections
Your Networks	Webex Collaboration Cloud 33434-33598		UDP SRTP	Secure audio, video & content sharing media	SIP calls to or from Webex Teams, including Hybrid Call Service Connect



S Marking for
Webex Media

Cisco Webex Teams Media

Assigning Cisco Webex Teams Media Traffic To Queues



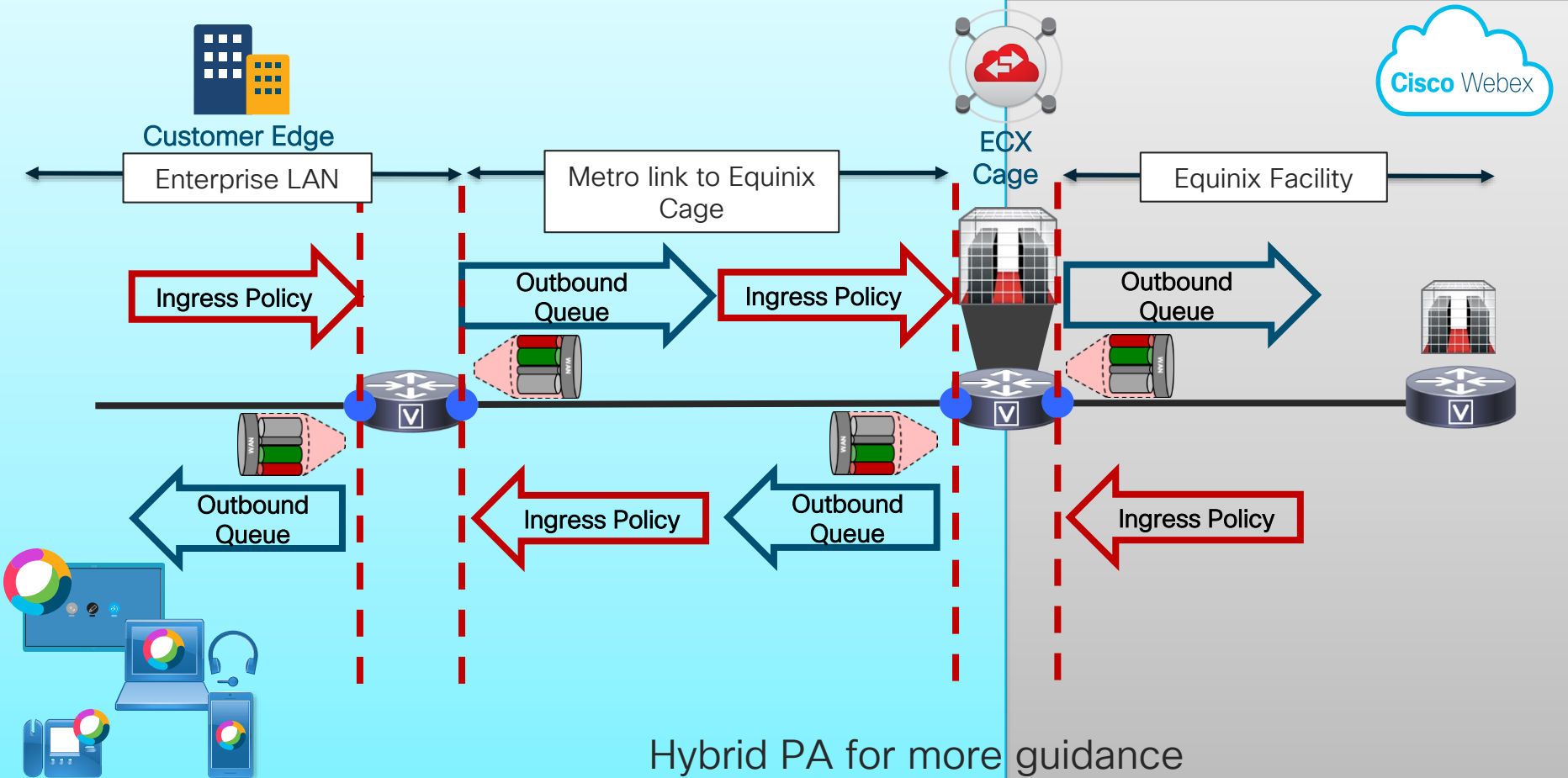
Cisco Webex Teams Media

Webex Teams Endpoint and Applications Native Marking

Traffic Type	PHB; DSCP (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
Other traffic	Best Effort; 0	0	Includes messaging, file transfer, configuration, call and meeting setup

Microsoft Windows does not allow applications to mark DSCP natively. Group Policy Objects (GPO) can be used to instruct the operating system to classify traffic from the application based on specific **port ranges**; however, we recommend following a network-based classification scheme.

Webex Edge Connect – Where to mark/queue



Media Signatures for Cisco Webex Teams and Cloud Registered Endpoints

Client to Cloud (Reverse for Cloud to Client)

Source IP	Destination IP	Source UDP Ports	Destination UDP Ports	Recommended DSCP	Media Type
Webex Teams application or endpoint	Webex cloud and Video Mesh Media Services	52000 to 52099	5004	EF	Audio
Webex Teams application or endpoint	Webex cloud and Video Mesh Media Services	52100 to 52299	5004	AF41	Video
Video Mesh Node	Webex Cloud Media Services	52500 to 62999	5004	EF	Audio
Video Mesh Node	Webex cloud Media Services	63000 to 65500	5004	AF41	Video
Video Mesh Node	Video Mesh Node	52500 to 62999	5004	EF	Audio
Video Mesh Node	Video Mesh Node	63000 to 65500	5004	AF41	Video

Media Signatures for Cisco Webex Meetings Application

Client to Cloud (Reverse for Cloud to Client)

Source IP	Destination IP	Source UDP Ports	Destination UDP Ports	Recommended DSCP	Media Type
Cisco Webex Meetings Application	Webex Cloud	Ephemeral	9000	AF41	Audio / Video

Webex Meetings App

webex-audio = Webex audio streaming

webex-video = Webex video streaming

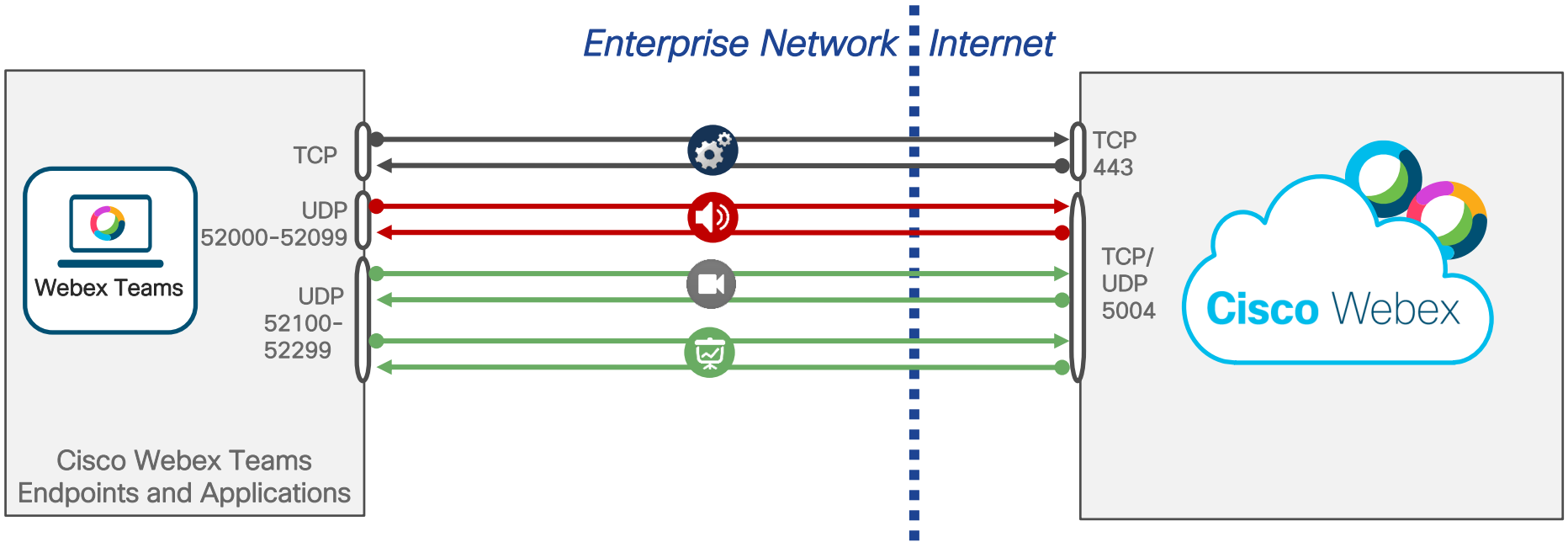
webex-app-sharing = Webex app sharing traffic

webex-meeting = Webex Signaling Traffic - (non-media – not port based)

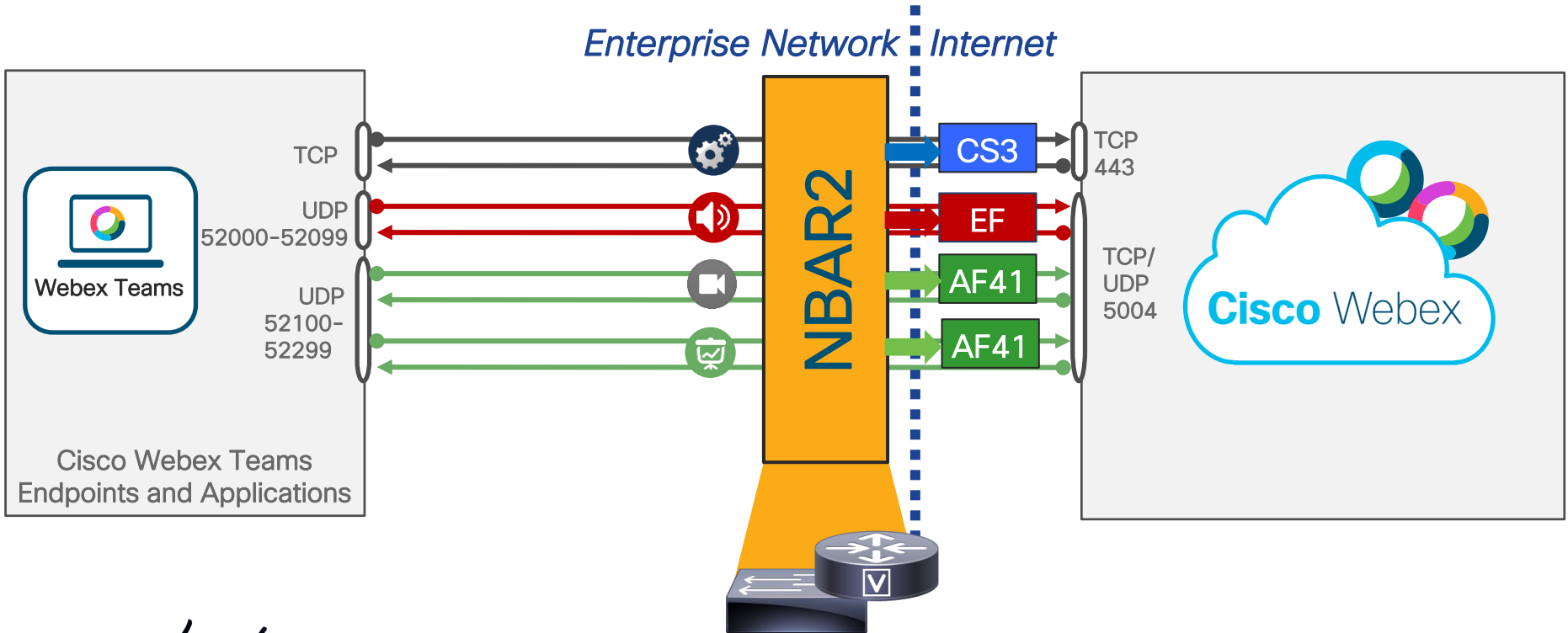
NBAR2



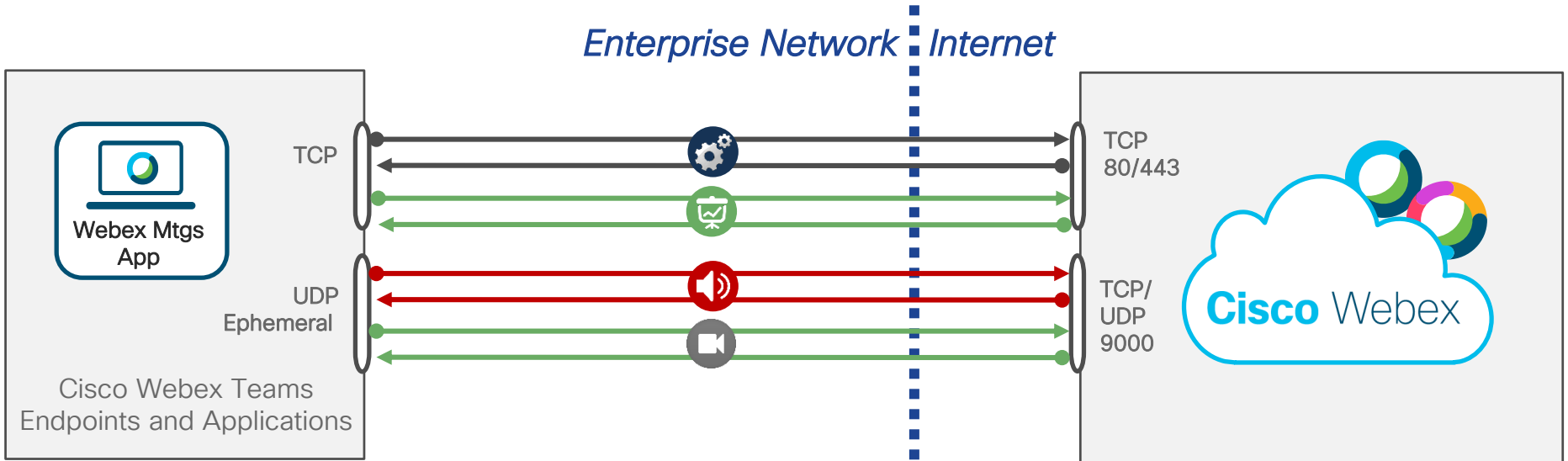
Port Usage Today – Webex Teams



Port Usage Today – Webex Teams

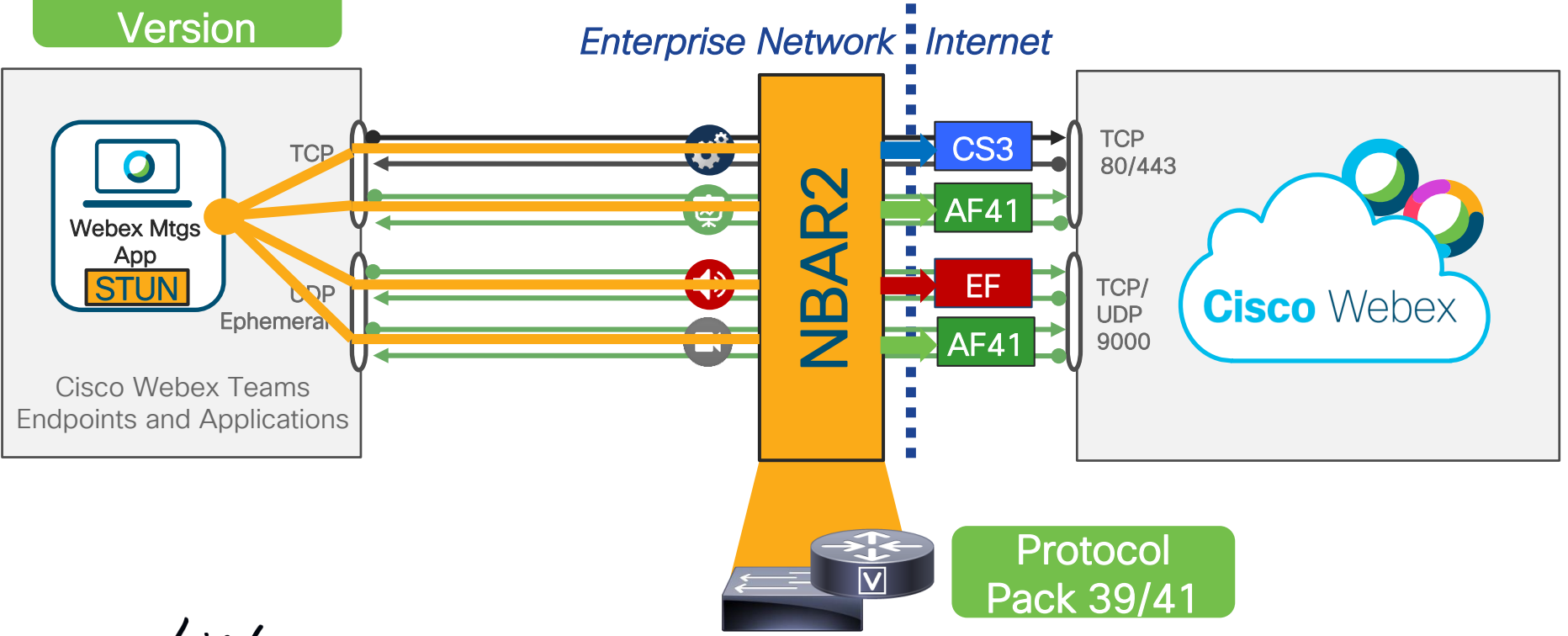


Port Usage Today – Webex Meetings App



Port Usage Today – Webex Meetings App

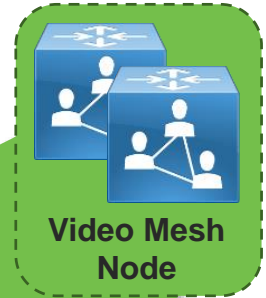
Latest Webex Version



Video Mesh Node – Ports

- Webex Control Hub Services > Video Mesh
- QoS (Enabled by Default)
- Enables Cascade Port Ranges and Native Marking
 - Audio 52500-62999 (EF)*
 - Video 63000-65500 (AF41)*

Video Mesh Cluster



Service Configuration

QoS

Quality of Service ⓘ

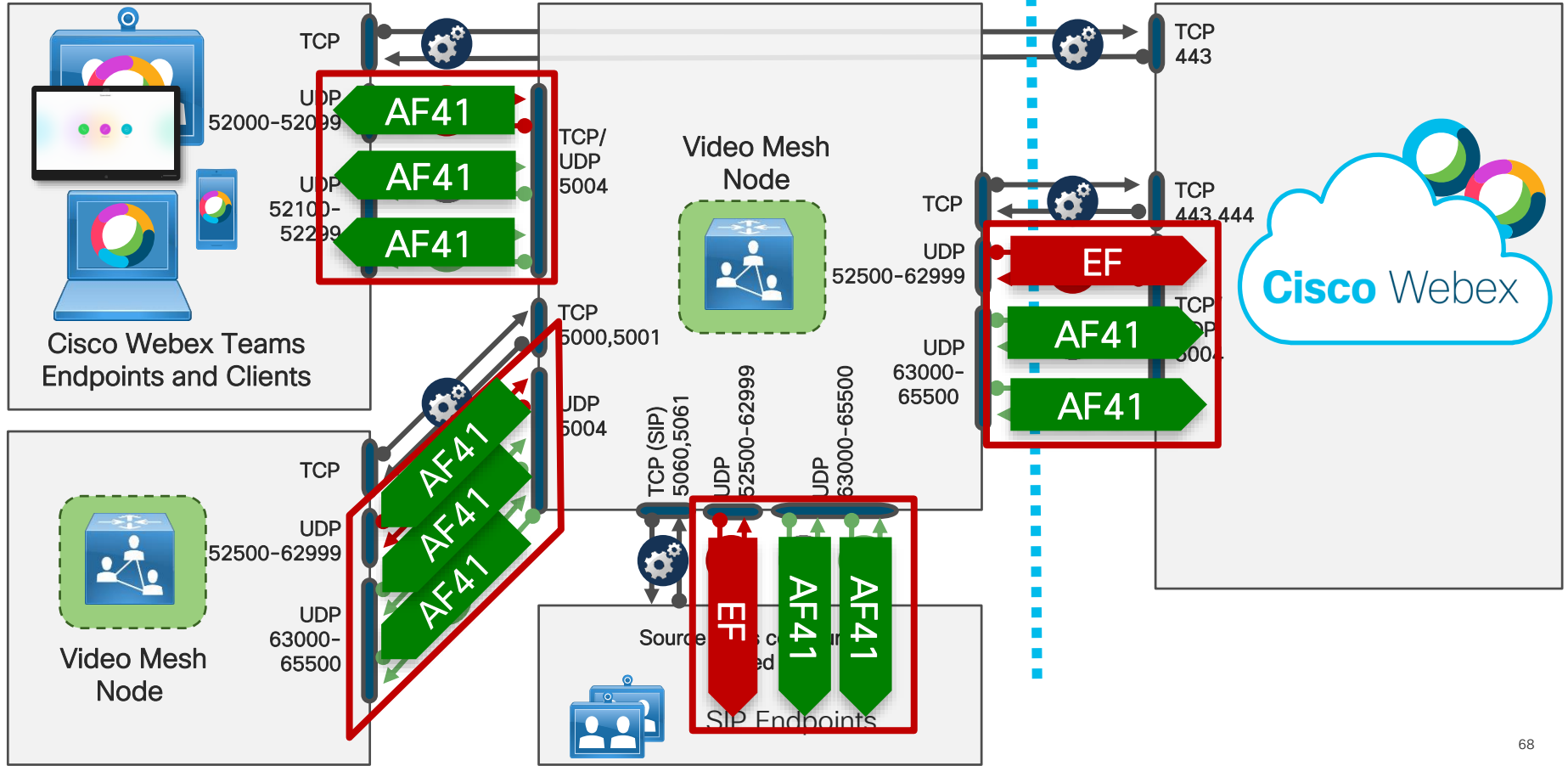
Enabling this setting modifies the UDP port range for Video Mesh cascade media and the Quality of Service (QoS) markings for both Video Mesh cascade and SIP client media. See the [Ports and Protocols documentation](#) for guidance.



* When disabled changes the source ports that are used for audio, video, and content sharing from the Video Mesh node to the range 34000 to 34999

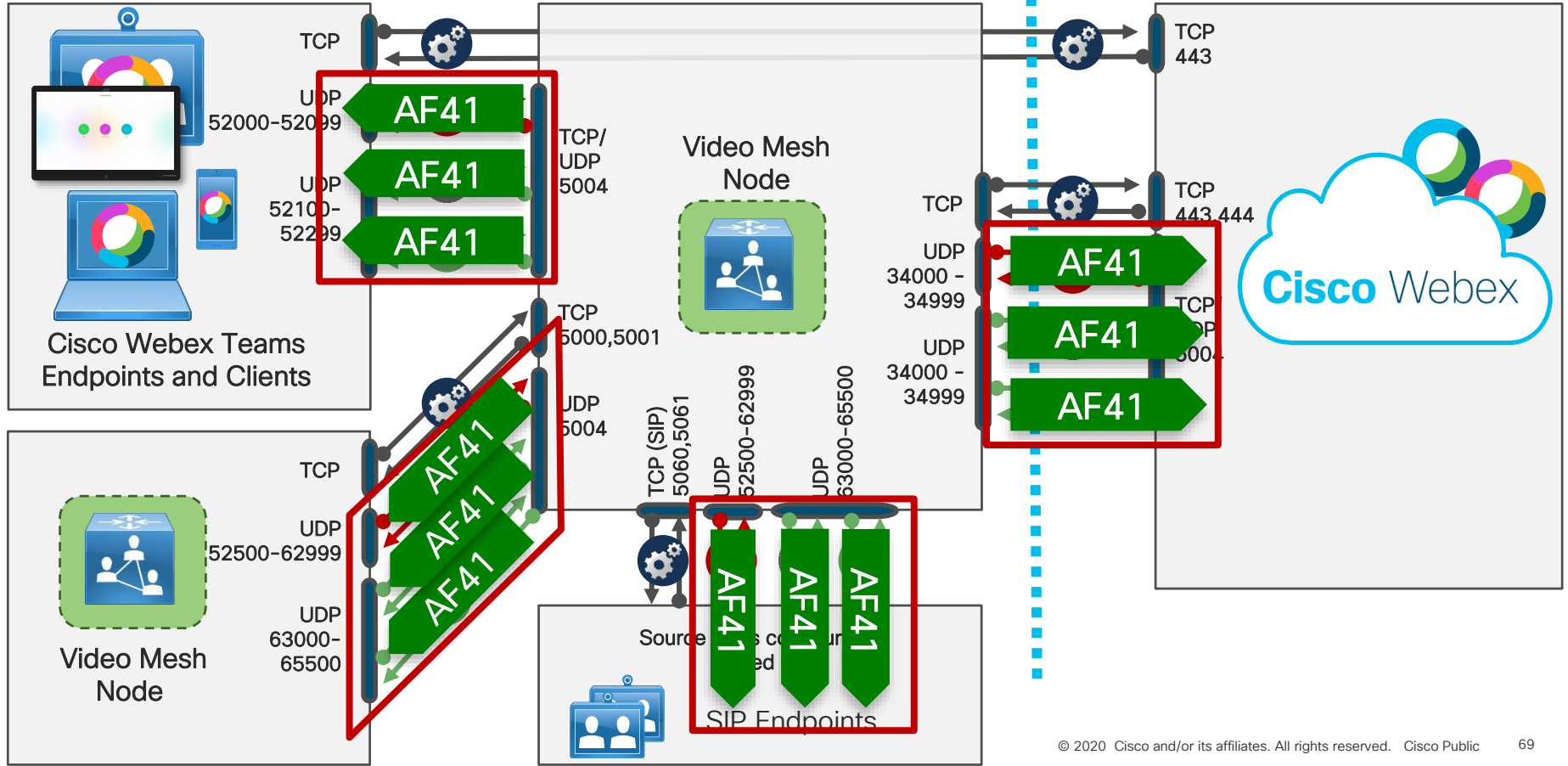
Video Mesh - Native Marking QoS Enabled

Enterprise Network Internet



Video Mesh - Native Marking QoS Disabled

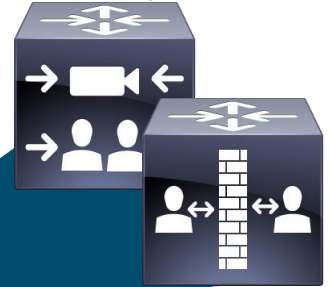
Enterprise Network Internet



Expressway

- System → Quality of Service
 - DSCP Signaling value 24 (Default) → CS3
 - DSCP Audio value 46 (Default) → EF
 - DSCP Video value 34 (Default) → AF41
 - DSCP XMPP value 24 (Default) → CS3

Cisco Expressway Core
(C) and Edge (E)



Status **System** Configuration Applications Users Maintenance

Quality of Service You are here: [System](#) ▶ Quality of Service

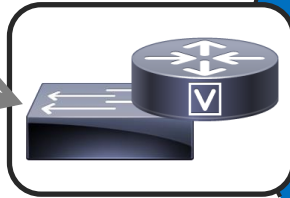
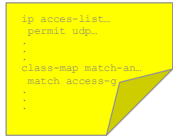
Tagging

DSCP Signaling value	* 24	i
DSCP Audio value	* 46	i
DSCP Video value	* 34	i
DSCP XMPP value	* 24	i

Webex Ingress QoS Policy



Update QoS configuration



Webex Meetings App

- webex-audio** = Webex audio streaming
- webex-video** = Webex video streaming
- webex-app-sharing** = Webex app sharing traffic
- webex-meeting** = Webex Signaling Traffic - (non-media, not port based)

NBAR2

```
ip access-list extended QOS_VOICE
 permit udp any range 17000 17999 any dscp ef
ip access-list extended QOS_PRIORITIZED_VIDEO
 permit udp any range 17000 17999 any dscp af41
```

```
ip access-list extended QOS_WEBEX_TEAMS_AUDIO
 permit udp any range 52000 52099 any any
 permit udp any eq 5004 any range 52000 52099
ip access-list extended QOS_WEBEX_TEAMS_VIDEO
 permit udp any range 52100 52299 any any
 permit udp any eq 5004 any range 52100 52299
```

```
class-map match-any VOICE
```

```
 match access-group name QOS_VOICE QOS_VOICE
```

```
 match access-group name QOS_WEBEX_TEAMS_AUDIO
```

```
class-map match-any PRIORITIZED_VIDEO
```

```
 match access-group name QOS_PRIORITIZED_VIDEO QOS_PRIORITIZED_VIDEO
```

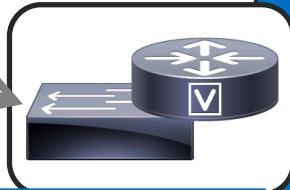
```
 match access-group name QOS_WEBEX_TEAMS_VIDEO QOS_WEBEX_TEAMS_VIDEO
```

Webex Ingress QoS Policy



Update QoS configuration

```
ip access-list
permit udp
...
class-map match-any
match access-g
```



Webex Teams

- cisco-spark-audio** = Teams audio streaming
- cisco-spark-video** = Teams video streaming
- cisco-spark-media** = Outdated: Will match if Audio and Video are not matched
- cisco-spark** = Teams Signaling (login, chat, keep-alive, etc...)

NBAR2

```
ip access-list extended QOS_VOICE
  permit udp any range 17000 17999 any dscp ef
ip access-list extended QOS_PRIORITIZED_VIDEO
  permit udp any range 17000 17999 any dscp af41
```

```
ip access-list extended QOS_WEBEX_TEAMS_AUDIO
  permit udp any range 52000 52099 any any
  permit udp any eq 5004 any range 52000 52099
ip access-list extended QOS_WEBEX_TEAMS_VIDEO
  permit udp any range 52100 52299 any any
  permit udp any eq 5004 any range 52100 52299
```

```
class-map match-any VOICE
```

```
  match access-group name QOS_VOICE
```

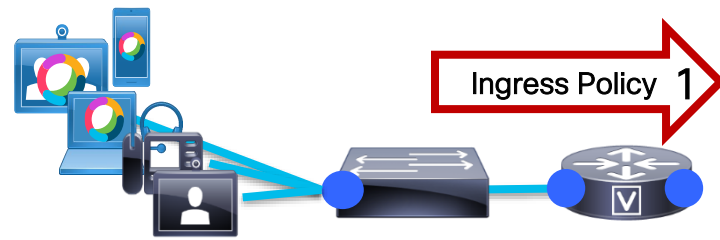
```
  match access-group name QOS_WEBEX_TEAMS_AUDIO
```

```
class-map match-any PRIORITIZED_VIDEO
```

```
  match access-group name QOS_PRIORITIZED_VIDEO
```

```
  match access-group name QOS_WEBEX_TEAMS_VIDEO
```


WAN Ingress QoS Marking Policy



Reference



! This section applies the policy-map to the Interface
Router(config-if)# service-policy input **INGRESS-MARKING**
! Attaches service policy to interface



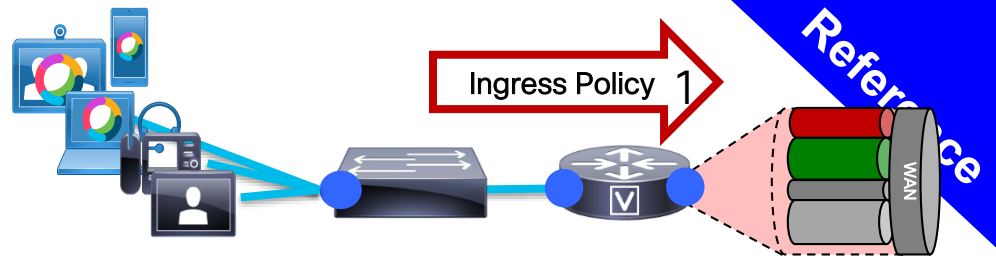
! This section configures the policy-map to set DSCP for Trusted and Untrusted Voice, Video and SIP Signaling on ingress

```
policy-map INGRESS-MARKING  
class VOICE  
    set dscp ef  
class PRIORITIZED-VIDEO  
    set dscp af41  
class OPPORTUNISTIC-VIDEO  
    set dscp af42  
class SIGNALING  
    set dscp cs3  
class class-default
```

! This section configures the classes

```
class-map match-any VOICE  
    match webex-audio  
    match access-group QOS_WEBEX_TEAMS_AUDIO  
class-map match-any PRIORITIZED-VIDEO  
    match webex-video  
    match access-group QOS_WEBEX_TEAMS_VIDEO  
class-map match-any SIGNALING  
    match webex-meeting  
    match cisco-spark  
    match access-group QOS_SIGNALING
```





! This section configures the classes

```
class-map match-any VOICE
```

```
match webex-audio
```

```
match access-group QOS_WEBEX_TEAMS_AUDIO
```

```
class-map match-any PRIORITIZED-VIDEO
```

```
match webex-video
```

```
match access-group QOS_WEBEX_TEAMS_VIDEO
```

```
class-map match-any SIGNALING
```

```
match webex-meeting
```

```
match cisco-spark
```

```
match access-group QOS_SIGNALING
```

4

! This section configures the policy-map to set DSCP for Trusted and Untrusted Voice, Video and SIP Signaling on ingress

```
policy-map INGRESS-MARKING
```

```
class VOICE
```

```
set dscp ef
```

```
class PRIORITIZED-VIDEO
```

```
set dscp af41
```

```
class OPPORTUNISTIC-VIDEO
```

```
set dscp af42
```

```
class SIGNALING
```

```
set dscp cs3
```

```
class class-default
```

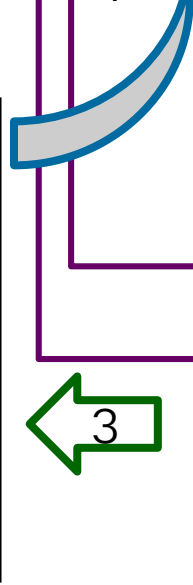
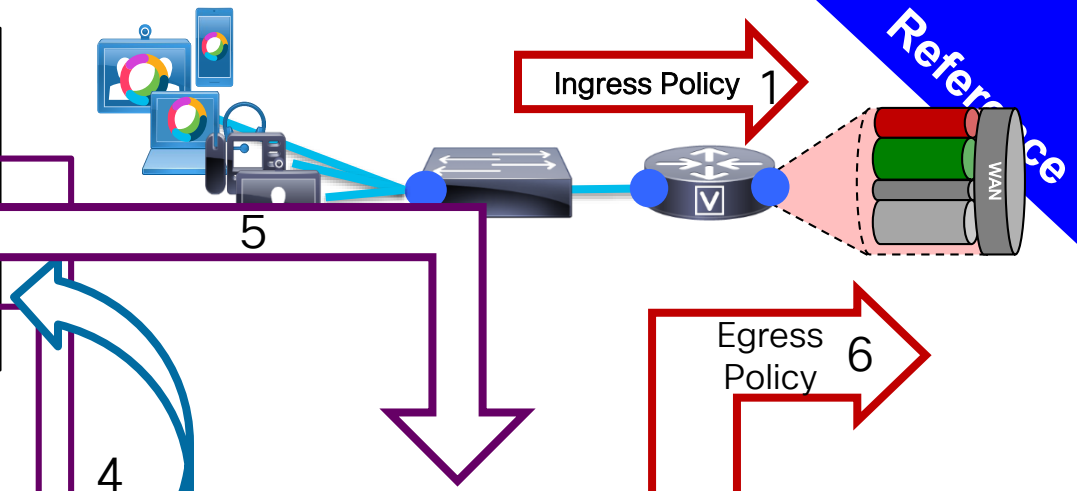
3

```
! This section configures the ACL's
ip access-list extended QOS_WEBEX_TEAMS_AUDIO
 permit udp any range 52000 to 52099 any 5004
 permit udp eq 5004 any range 52000 to 52099
ip access-list extended QOS_WEBEX_TEAMS_VIDEO
 permit udp any range 52100 52299 any 5004
 permit udp eq 5004 any range 52100 52299
```

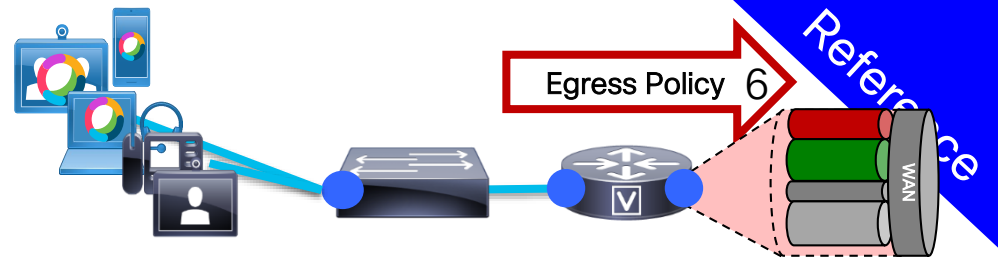
```
! This section configures the classes
class-map match-any VOICE
 match webex-audio
 match access-group QOS_WEBEX_TEAMS_AUDIO
class-map match-any PRIORITIZED-VIDEO
 match webex-video
 match access-group QOS_WEBEX_TEAMS_VIDEO
class-map match-any SIGNALING
 match webex-meeting
 match cisco-spark
 match access-group QOS_SIGNALING
```

```
! This section configures the policy-map to set DSCP
for Trusted and Untrusted Voice, Video and SIP
Signaling on ingress

policy-map INGRESS-MARKING
 class VOICE
  set dscp ef
 class PRIORITIZED-VIDEO
  set dscp af41
 class OPPORTUNISTIC-VIDEO
  set dscp af42
 class SIGNALING
  set dscp cs3
 class class-default
```



Egress Classification and Queuing



6.1

! This section applies the policy-map to the Interface
Router (config-if)# service-policy output EGRESS-QUEUING
! Attaches service policy to interface

! This section configures the bandwidth for all collab traffic

```
policy-map EGRESS-QUEUING
class VOICE
  priority percent 10
! Provisions 10% LLQ to VOICE class
class VIDEO
  bandwidth percent 30
! Provisions 30% CBWFQ to VIDEO class
class SIGNALING
  bandwidth percent 2
! Provisions 2% CBWFQ to SIGNALING class
```

6.2

! This section applies the policy-map

```
class-map match-all VOICE
  match dscp ef
class-map match-any VIDEO
  match dscp af41
  match dscp af42
class-map match-all SIGNALING
  match dscp cs3
```

6.3

QoS Marking and Traffic Queuing

Key Takeaways

- Simplified Ingress Remarking Policy
- Egress Queuing Policy (recommended)
 - Single video queue for AF class traffic model is recommended
- All Webex media traffic can be differentiated and marked
- QoS should be set prior to arriving at Edge Connect
- Webex Edge Connect over Equinix does not modify the QoS marking applied but does not use it either. It will only be used for your outbound queueing (If configured)
- A QoS policy is required for traffic coming from Webex to remark it prior to entering the Enterprise.

Common Questions and Answers

Q: Does Edge Connect support IPv6

A: No

Q: Will Edge Connect support a private BGP AS

A: Yes, contact your account team to request

Q: Will Edge Connect support private IP Addressing

A: No

Q: Does Edge Connect support 4 byte ASN

A: Yes

Reference Links

Tutorial Videos

- ECX Portal Tutorials: <https://ecxfabric-documentation.equinix.com/hc/en-us/articles/360013215672-Video-tutorials>
- ECX Portal Edge Connect Ordering Tutorial: <https://www.youtube.com/watch?v=WhRHgbUXGns>

Cisco Webex Edge Connect Documentation

- <https://collaborationhelp.cisco.com/article/en-us/n68tcpb>

Equinix Cloud Exchange Portal

- <https://cloudexchangeportal.equinix.com>

Network requirements for Webex Services

- Webex Meetings: <https://collaborationhelp.cisco.com/article/en-us/WBX264>
- Teams & Boards: <https://collaborationhelp.cisco.com/article/en-us/WBX000028782>

Network connectivity test

- <https://mediatest.webex.com>

AS13445 Looking Glass

- <http://lg.webex.com/lg/>

Webex Edge Audio

Components of Webex Edge for Meetings



Webex Edge for Meetings

1 Connect

Direct Connection to the
Webex Datacenter

2 Audio

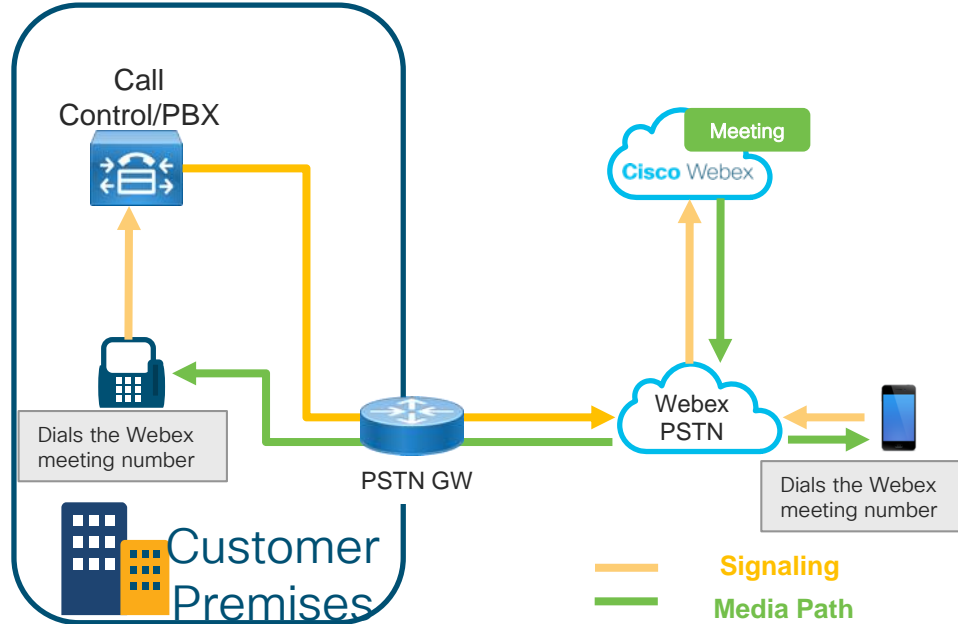
Webex Meeting Audio via the
Internet or Edge Connect

3 Video Mesh

Meeting Resources on
premises

Cisco Webex PSTN Audio

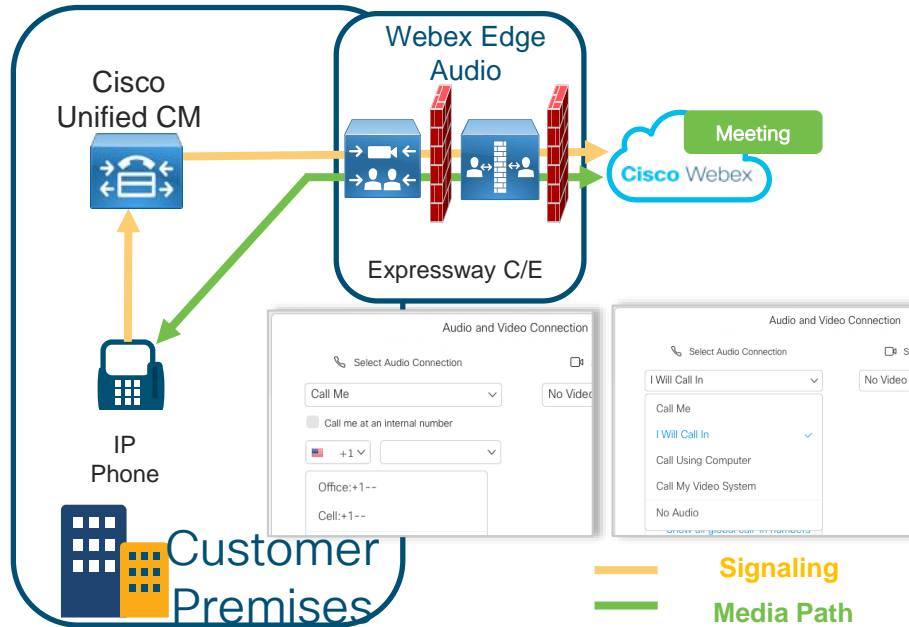
High level overview



1. On-premises telephone or cell phone dials the Webex meeting number to get connected by audio into the meeting.
2. Signaling is routed via the on-premises call control device/PBX or by the cell phone network to Webex Meetings audio service.
3. Audio media (the sound) is connected via the Webex PSTN connection between the Webex meeting and the on-premises phone or cell phone.

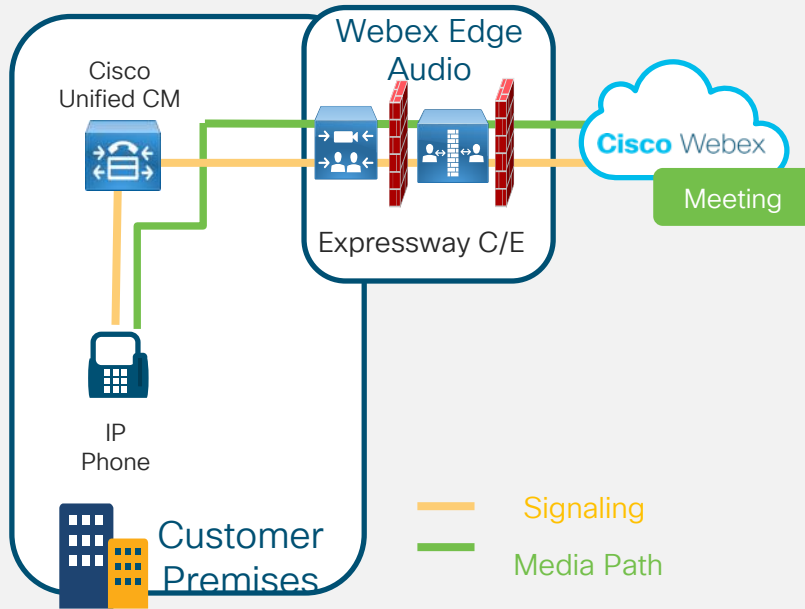
Cisco Webex Edge Audio

High level overview



1. On-premises telephone dials the Webex meeting number or gets a call back from the Webex meeting to get connected by audio into the meeting.
2. Signaling is routed via the on-premises call control device (Unified CM) through the Expressway C and E to Webex Meetings audio service.
3. Audio media (the sound) is routed from the Webex meeting to the Expressway E and C and then to the on-premises phone for callback and the reverse for call in.

Cisco Webex Edge Audio

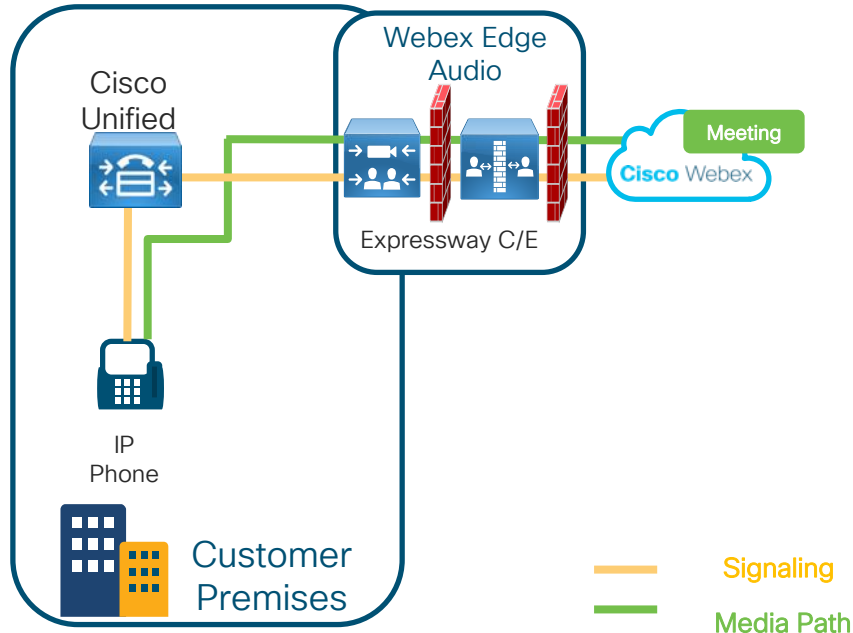


- Intelligent audio routing: integrating Webex with Unified CM
 - Creates end-to-end VoIP path for Unified CM registered devices (callback and dial-in)
 - Uses company's own PSTN for any other device (callback savings)
 - No SIP trunks or peering arrangements required
- Geo-country code configurable
- Included in Collaboration Flex Plan – no extra charge. No port charges on Expressway
- Supports Webex Meetings, Events, Training

No user training, no change in user behavior, easy for IT

Cisco Webex Edge Audio

Architecture requirements



Unified CM support only

- 10.5 or later

Cisco UCM registered IP phones

- Supporting G.711 or G.722

Expressway support only

- X8.10 or later
- Can use existing Expressway C/E deployment
- Audio scale dependent on Expressway deployment and services enabled.

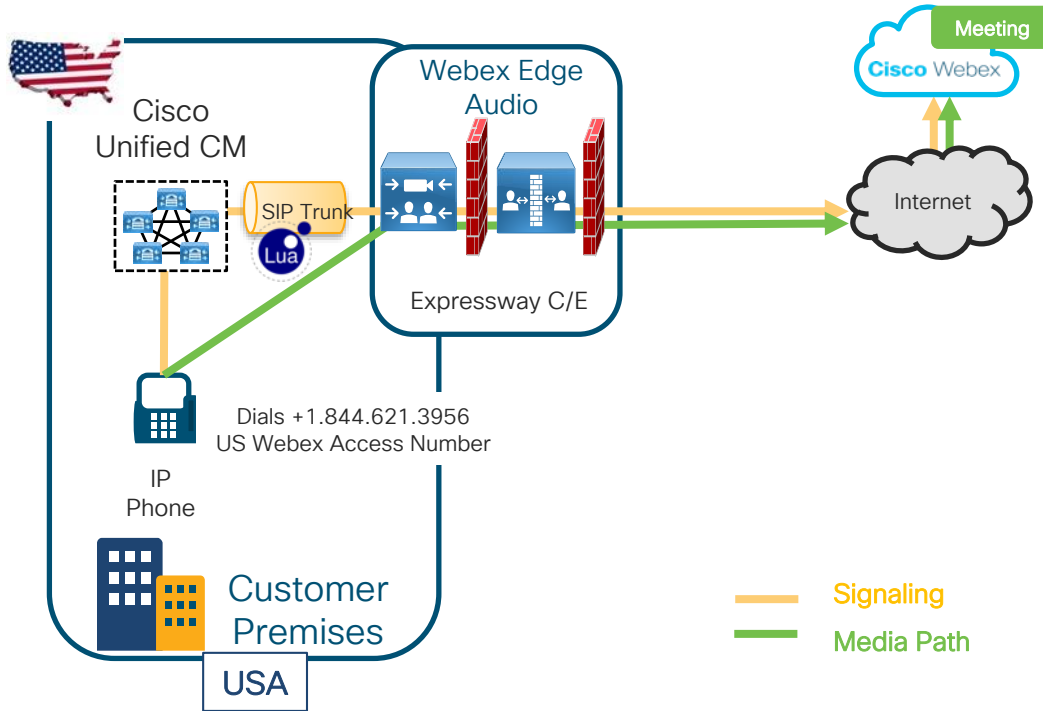
Webex site

- WBS 33.x or higher
- Included in Flex, A-WBX and A-SPK SKU need the Webex Edge Audio package
- Not available on CCA-ENT or TSP sites.
- Requires migration to Webex Audio Site

Requires a signed certification from a Cisco trusted Certificate Authority (CA)

Configuration Steps

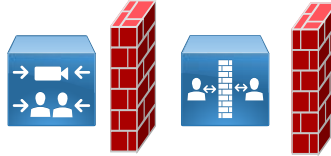
Best Practice



1. Make a new SIP trunk from CUCM to Expressway – C, **do not** use an existing trunk.
2. Create a new dedicated traversal zone between Expressway C and E for Edge Audio only, **do not** use an existing zone.
3. MRA and Edge Audio can co-reside on the same Expressway C/E pair.
4. Edge Audio is based on +E.164 numbers for dialing.
5. Recommend a dedicated Expressway C & E pair for environments that require high volume webex audio calling support.

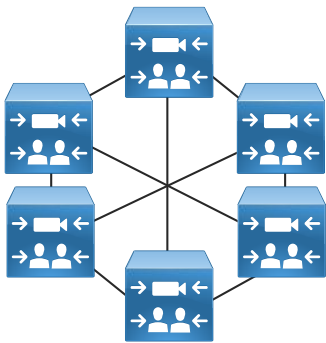
Expressway sizing

Expressway - C + E
1 node cluster

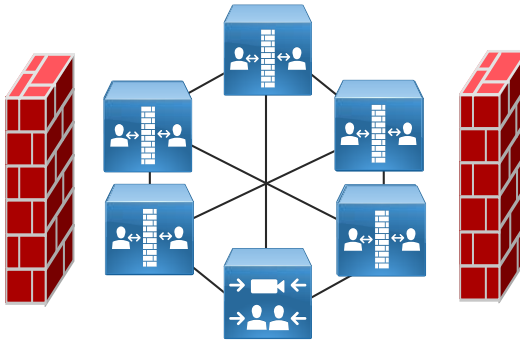


Single Expressway C + E pair

- Supports up to **1000** audio calls



Expressway - C
6 node cluster

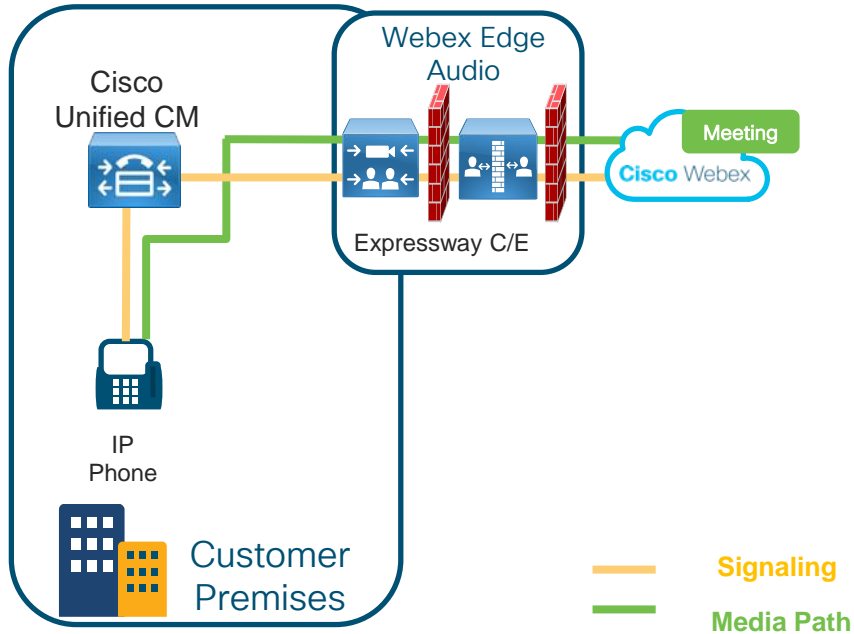


Expressway - E
6 node cluster

- Size the Expressway clusters based on peak load and regional traffic
- Each Expressway cluster supports up to **4000** peak audio calls with full active-active redundancy
- Each Expressway 6 node cluster supports up to 16 calls per sec.
- Recommend **dedicating** Expressway C and E pairs for Edge audio only calls to Webex for large peak loads

Cisco Webex Edge Audio

Overview Architecture configuration

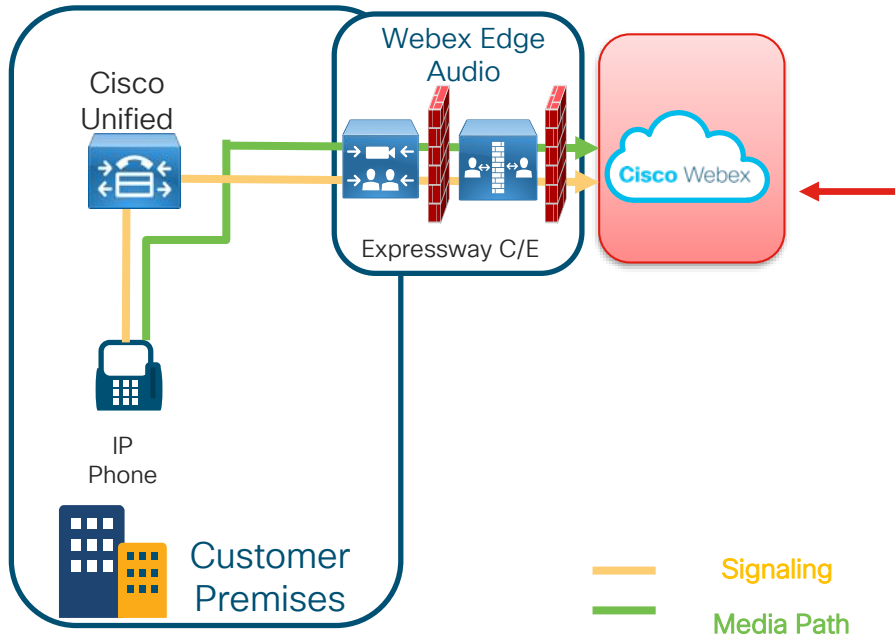


Overview of Webex Edge Audio Configuration Steps:

1. Obtain dial-in numbers and Lua script from Control Hub
2. Configure Unified CM
3. Set Up Expressway-C
4. Set Up Expressway-E
5. Open Firewall ports
6. Apply Signed Certificate From Trusted Certificate Authority
7. Apply Edge Audio Callback Settings

Cisco Webex Edge Audio

Architecture configuration – Dial in

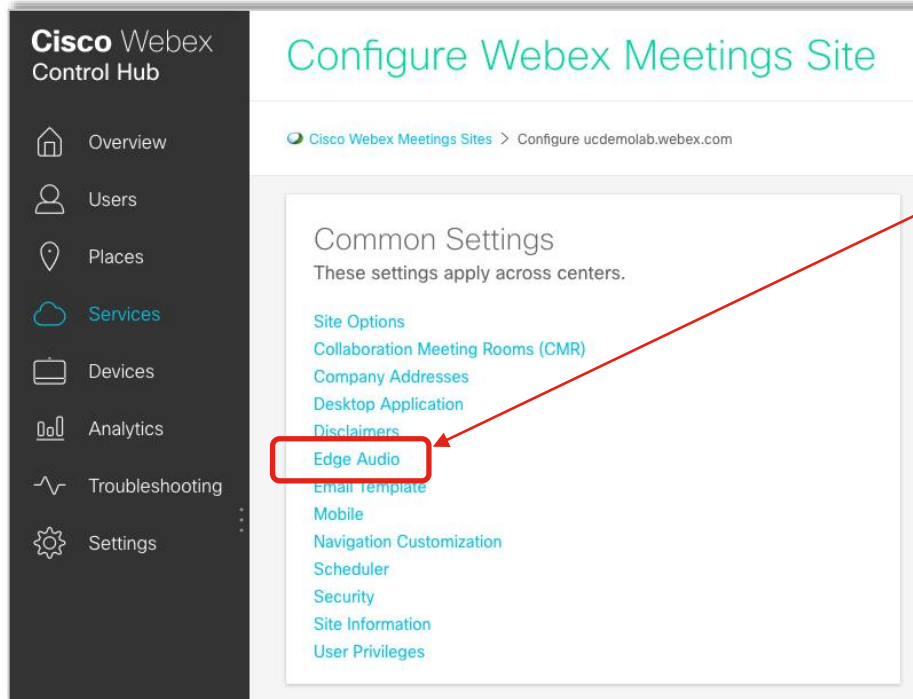


Overview of Webex Edge Audio Configuration Steps:

1. Obtain dial-in numbers and Lua script from Control Hub
2. Configure Unified CM
3. Set Up Expressway-C
4. Set Up Expressway-E
5. Open Firewall ports
6. Apply Signed Certificate From Trusted Certificate Authority
7. Apply Edge Audio Callback Settings

Cisco Webex Edge Audio

Architecture configuration – Dial in



Webex Edge Audio Call-in Set Up Steps:

1. Obtain dial-in numbers and Lua script from Webex Control Hub.

Cisco Webex Edge Audio

Architecture configuration – Dial in

Cisco Webex Control Hub

Webex Edge Audio

Cisco Webex Meetings Sites > Configure ucdemolab.webex.com > Webex Edge Audio

Webex On-net Audio allows you to leverage the internet to route dial-in and callback audio from the Webex Meetings application, and phones and video devices through a Cisco Unified Communication Manager and Cisco Expressway solution. Follow these instructions to configure Webex On-net Audio.

Dial-in Settings

Click Generate Lua Script to save the Lua Script to your computer. Then apply the Lua script to your CUCM in order to update its configuration to allow for appropriate routing of dial-in calls to the cloud. [Click here](#) to view the list of phone numbers allowed under this setting.

[Generate Lua Script](#)

Callback Settings

Country/Region:

Country/Region	Expressway DNS SRV	Connectivity Check Status	Action
		<input type="checkbox"/>	

Settings last updated on - are in effect [Details](#)

UC Demo Lab

Webex Edge Audio Call-in Set Up Steps:

1. Obtain dial-in numbers and Lua script from Webex Control Hub.

Dial-in Settings

Click Generate Lua Script to save the Lua Script to your computer. Then apply the Lua script to your CUCM in order to update its configuration to allow for appropriate routing of dial-in calls to the cloud. [Click here](#) to view the list of phone numbers allowed under this setting.

Webex On-net Audio DNS: `_sips._tcp.ecccx.amer.pub.webex.com` [Hide call-in numbers](#)

Phone Label	Phone Number
Argentina Toll	+54-11-5984-2766
Argentina Toll Free	0800-8000-182
Australia Toll	+61-28317-5553
Australia Toll Free	1-800-820-385
Austria Toll	+43-720-815317
Austria Toll Free	0800-29-8494
Bahrain Toll Free	8000-6014
Belarus Toll Free	882-00011-0840

Cisco Webex Edge Audio

Architecture configuration – Dial in

Cisco Webex Control Hub

Webex Edge Audio

Cisco Webex Meetings Sites > Configure ucdemolab.webex.com > Webex Edge Audio

Webex On-net Audio allows you to leverage the internet to route dial-in and callback audio from the Webex Meetings application, and phones and video devices through a Cisco Unified Communication Manager and Cisco Expressway solution. Follow these

```
M={}

function M.outbound_INVITE(msg)
  --[[
    This function does all required Webex Express translations
    This will change outgoing INVITE RequestURI and To header.
    RequestURI will be changed to have
    1. Webex Express DNS SRV for a Webex region
    2. x-cisco-site-uuid parameter
    To header will be changed to have
    1. Access number
  --]]
end
```

[How to apply Lua script to Cisco Unified Communication Manager](#)

[Customer Configuration Guide](#)

Export Copy Close

Generate Lua Script

Apply Settings

Webex Edge Audio Call-in Set Up Steps:

1. Obtain dial-in numbers and Lua script from Webex Control Hub

Lua Script

Changes outgoing INVITE RequestURI and To header

RequestURI will be changed to have

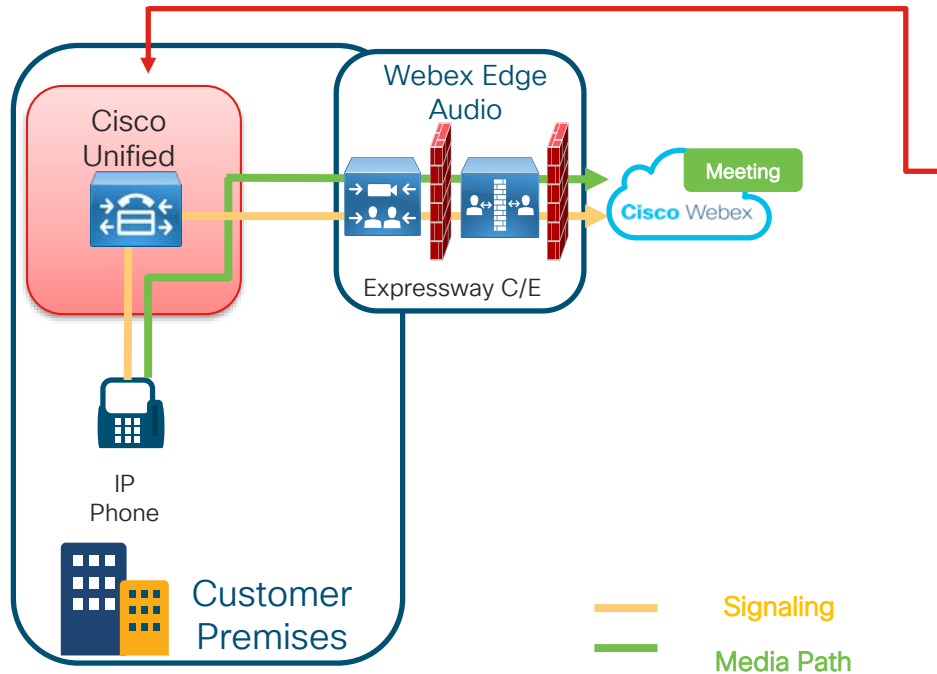
- Webex Edge Audio DNS SRV for a Webex region
- x-cisco-site-uuid parameter

To header will be changed to have

- Webex access number added

Cisco Webex Edge Audio

Architecture configuration – Dial in



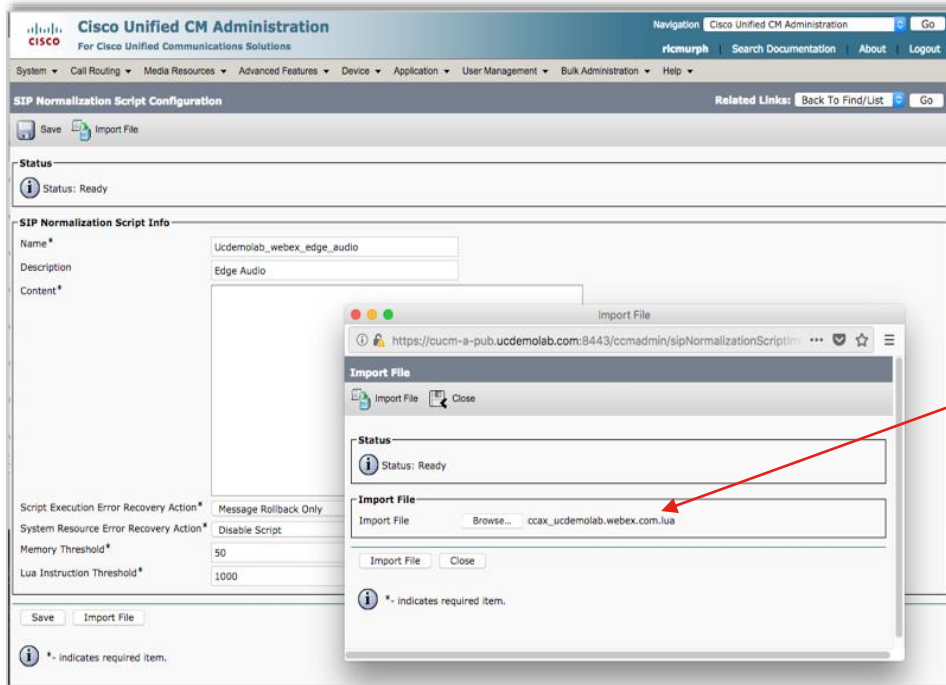
Webex Edge Audio Call-in Set Up Steps:

2. Configure Unified CM

- Create SIP Normalization Script using the Webex LUA Script
- Create or Update Early Offer Profile.
- Create a Sip Trunk Security Profile.
- Create a CSS for class of service for incoming Webex Edge Audio calls
- Create a new Trunk between Cisco UCM and Expressway-C and apply above CSS
- Create Route Patterns for Webex numbers.

Cisco Webex Edge Audio

Architecture configuration



Webex Edge Audio Call-in Set Up Steps:

2. Configure Unified CM

- ✓ Create SIP Normalization Script using the Webex LUA Script
- Device -> Device Settings -> SIP Normalization Script
- Import file or input script details in the Content section.

Cisco Webex Edge Audio

Architecture configuration

SIP Profile Configuration Related Links: [Back To Find/List](#) Go

Save Delete Copy Reset Apply Config Add New

Incoming Requests FROM URI Settings

Caller ID DN

Caller Name

Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on*

Resource Priority Namespace List

SIP Rel1XX Options*

Video Call Traffic Class*

Calling Line Identification Presentation*

Session Refresh Method*

Early Offer support for voice and video calls*

Webex Edge Audio Call-in Set Up Steps:

2. Configure Unified CM

- ✓ Create SIP Normalization Script using the Webex LUA Script
- ✓ Create or Update Early Offer Profile.
 - Device -> Device Settings -> SIP Profile

Cisco Webex Edge Audio

Architecture configuration

SIP Trunk Security Profile Configuration Related Links: Back To Find/List Go

Save Delete Copy Reset Apply Config Add New

SIP Trunk Security Profile Information

Name* Non Secure SIP Trunk Profile WEA 5070

Description webex edge audio TCP 5070

Device Security Mode Non Secure

Incoming Transport Type* TCP+UDP

Outgoing Transport Type TCP

Enable Digest Authentication

Nonce Validity Time (mins)* 600

X.509 Subject Name

Incoming Port* 5070

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Webex Edge Audio Call-in Set Up Steps:

2. Configure Unified CM

- ✓ Create SIP Normalization Script using the Webex LUA Script
- ✓ Create or Update Early Offer Profile.
- ✓ Create a Sip Trunk Security Profile.
 - System -> Security -> SIP Trunk Security Profile
 - Update Security Mode
 - Incoming port to a nonconflicting port. Do not use 5060 or 5061

Cisco Webex Edge Audio

Architecture configuration

Trunk Configuration Related Links: Back To Find/List

Save Delete Reset Add New

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination
1*	exp-c04.ucdemolab.com		5060

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* **Non Secure SIP Trunk Profile WEA 5070**

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* **Standard SIP Profile with EO and SIP OPTIONS Pin** [View Details](#)

DTMF Signaling Method* **RFC 2833**

Normalization Script

Normalization Script **Ucdemolab_webex_edge_audio**

Enable Trace

Webex Edge Audio Call-in Set Up Steps:

2. Configure Unified CM

- ✓ Create SIP Normalization Script using the Webex LUA Script
- ✓ Create or Update Early Offer Profile.
- ✓ Create a Sip Trunk Security Profile.
- Create a CSS for class of service for incoming Webex Edge Audio calls
- Create a new Trunk between Cisco UCM and Expressway-C and apply the above CSS.

Cisco Webex Edge Audio

Architecture configuration

The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', and 'User Management'. The main heading is 'Route Pattern Configuration'. Below this is a toolbar with 'Save', 'Delete', 'Copy', and 'Add New' buttons. The 'Status' section shows 'Status: Ready'. The 'Pattern Definition' section contains the following fields:

Route Pattern*	17206507664
Route Partition	B2B
Description	Webex Edge Audio
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	EXPWY_3_webexEdgeAudio_ucdemolab_site (Edit)
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error
Call Classification*	OffNet

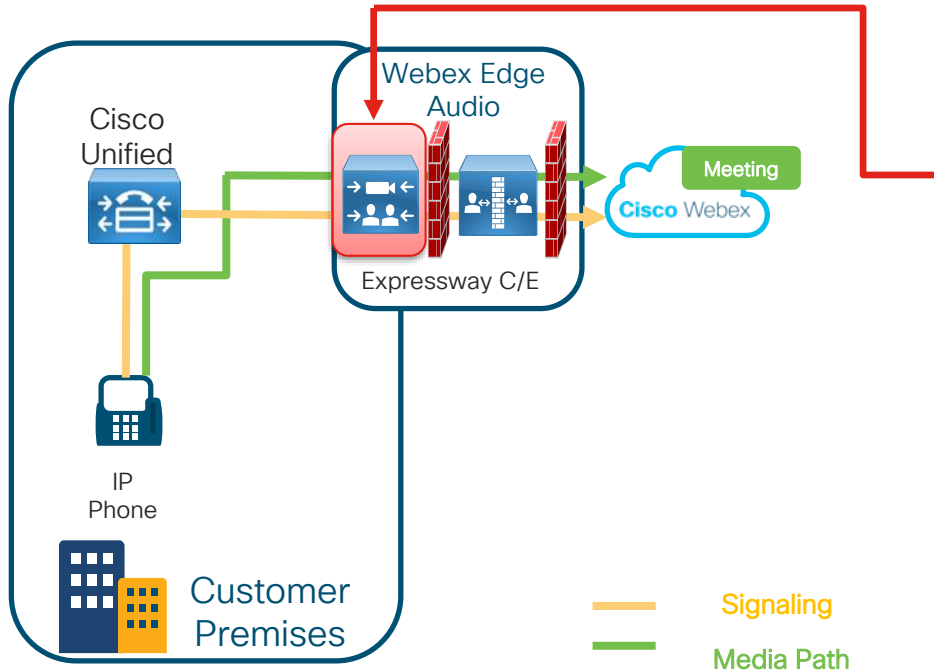
Webex Edge Audio Call-in Set Up Steps:

2. Configure Unified CM

- ✓ Create SIP Normalization Script using the Webex LUA Script
- ✓ Create or Update Early Offer Profile.
- ✓ Create a Sip Trunk Security Profile.
- ✓ Create a CSS for class of service for incoming Webex Edge Audio calls
- ✓ Create a new Trunk between Cisco UCM and Expressway-C and apply above CSS
- Create Route Patterns for the Global Webex access numbers.

Cisco Webex Edge Audio

Architecture configuration



Webex Edge Audio Call-in Set Up Steps:

3. Configure Expressway-C

- Create Neighbor zone
- Define secure traversal client zone
- Define search rules to forward calls between Webex Edge Audio UCM neighbor zone and Webex Edge Audio traversal zone

Cisco Webex Edge Audio

Architecture configuration – Dial in

The screenshot shows the Cisco Expressway-C configuration interface for editing a zone. The 'Configuration' section is highlighted with a red box, showing the following settings:

- Name: * UCUM Core - Edge Audio Only
- Type: Neighbor
- Hop count: * 15

The 'SIP' section is also highlighted with a red box, showing the following settings:

- Mode: On
- Port: * 5070
- Transport: TCP
- Accept proxied registrations: Deny
- Media encryption mode: Auto
- ICE support: Off
- Multistream mode: Off
- Preloaded SIP routes support: Off
- AES GCM support: Off

The 'Authentication' section shows the following settings:

- Authentication policy: Treat as authenticated
- SIP authentication trust mode: Off

Two red arrows point from the 'Edit zone' page to the 'Webex Edge Audio Call-in Set Up Steps' list on the right.

Webex Edge Audio Call-in Set Up Steps:

3. Configure Expressway-C

- Create Neighbor zone
- Define secure traversal client zone

The screenshot shows the 'Location' configuration page. The 'Look up peers by' dropdown is set to 'Address'. The 'Peer 2 address' field is highlighted with a red box, showing the following settings:

- Peer 1 address: 10.99.150.111
- Peer 2 address: 10.99.150.112
- Peer 3 address: [Empty]
- Peer 4 address: [Empty]
- Peer 5 address: [Empty]
- Peer 6 address: [Empty]

The 'Advanced' section shows the following settings:

- Zone profile: Cisco Unified Communications Manager (9.x or later)

Buttons for 'Save', 'Cancel', and 'Delete' are visible at the bottom.

Cisco Webex Edge Audio

Architecture configuration – Dial in

The screenshot shows the Cisco Expressway-C configuration interface for editing a zone. The page is titled 'Edit zone' and has a breadcrumb trail: 'You are here: Configuration > Zones > Zones > Edit zone'. The configuration is organized into several sections:

- Configuration:** This section is highlighted with a red box. It contains:
 - Name: Webex_Edge_Audio_Traversal
 - Type: Traversal client
 - Hop count: 15
- Connection credentials:** This section contains:
 - Username: apptraversal
 - Password: [Redacted]
- H.323:** This section contains:
 - Mode: Off
- SIP:** This section is also highlighted with a red box. It contains:
 - Mode: On
 - Port: 7003
 - Transport: TLS
 - TLS verify mode: On
 - Accept proxied registrations: Deny
 - Media encryption mode: Force encrypted

Two red arrows point from the text on the right to the 'Name' field in the Configuration section and the 'SIP' section.

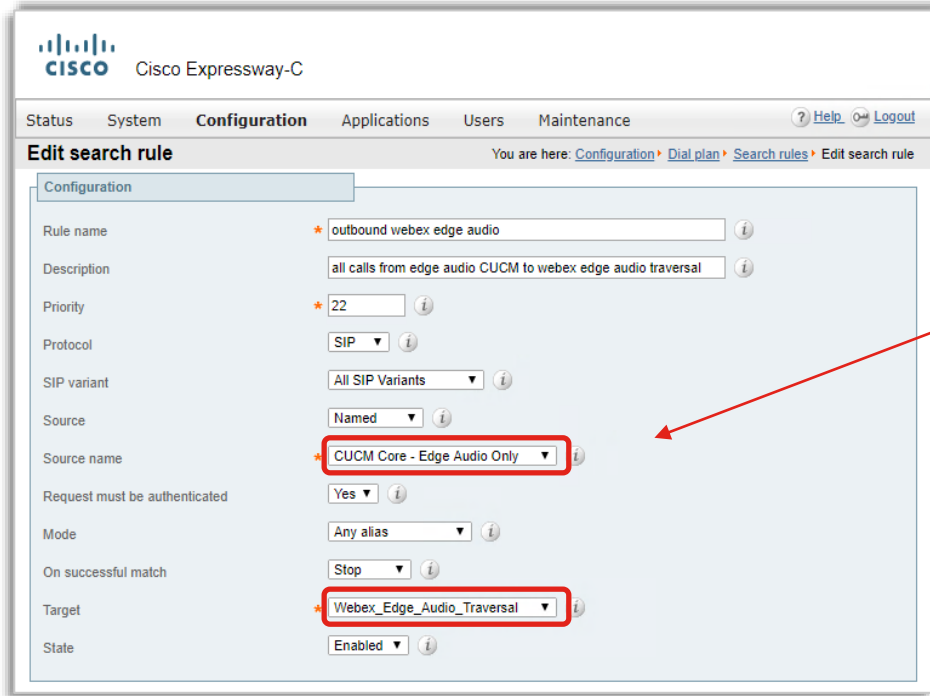
Webex Edge Audio Call-in Set Up Steps:

3. Configure Expressway-C

- ✓ Create Neighbor zone
- Define secure traversal client zone

Cisco Webex Edge Audio

Architecture configuration – Dial in



The screenshot shows the Cisco Expressway-C configuration interface. The page title is 'Cisco Expressway-C'. The navigation menu includes 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The current page is 'Edit search rule', with a breadcrumb trail: 'Configuration > Dial plan > Search rules > Edit search rule'. The configuration form is titled 'Configuration' and contains the following fields:

Rule name	* outbound webex edge audio
Description	all calls from edge audio CUCM to webex edge audio traversal
Priority	* 22
Protocol	SIP
SIP variant	All SIP Variants
Source	Named
Source name	* CUCM Core - Edge Audio Only
Request must be authenticated	Yes
Mode	Any alias
On successful match	Stop
Target	* Webex_Edge_Audio_Traversal
State	Enabled

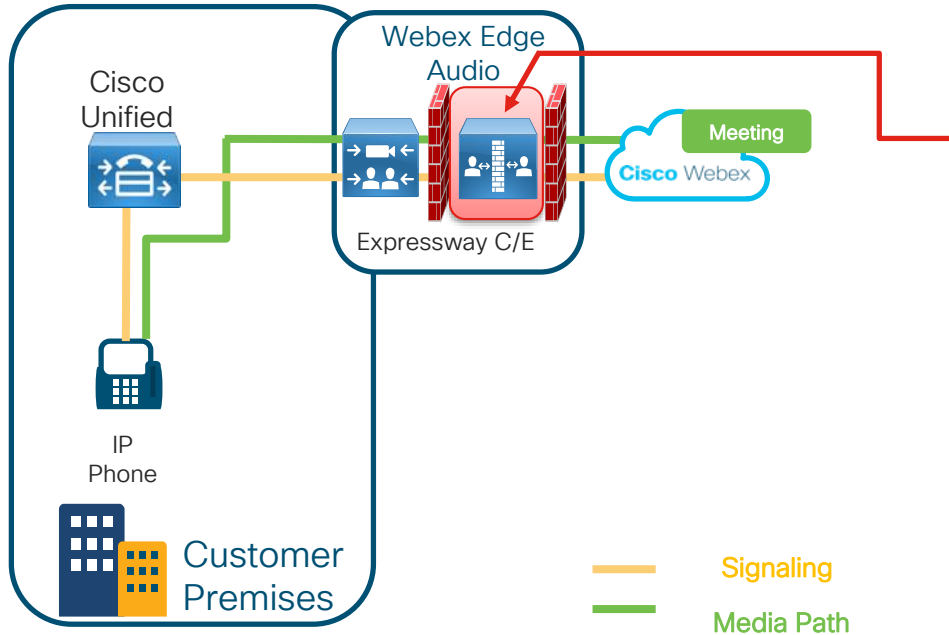
A red arrow points from the 'Webex Edge Audio Call-in Set Up Steps' list to the 'CUCM Core - Edge Audio Only' dropdown menu in the configuration form.

Webex Edge Audio Call-in Set Up Steps:

3. Configure Expressway-C
 - ✓ Create Neighbor zone
 - ✓ Define secure traversal client zone
 - Define search rules to forward calls between Webex Edge Audio UCM neighbor zone and Webex Edge Audio traversal zone

Cisco Webex Edge Audio

Architecture configuration – Dial in



Webex Edge Audio Call-in Set Up Steps:

4. Configure Expressway-E

- Set up Secure Traversal Server Zone.
- Set up mTLS zone to Webex
 - If you're using an Expressway version before X8.11, then the DNS Zone with Mutual TLS (mTLS).
 - If you're using Expressway version x8.11 or later, then the Webex Zone.
- Define search rules to forward calls between between Webex Edge Audio Traversal Zone and Webex Zone
- Configure Mutual TLS (mTLS)

Cisco Webex Edge Audio

Architecture configuration – Dial in

The screenshot shows the 'Edit zone' configuration page in Cisco Expressway-E. The 'Configuration' section is highlighted with a red box. The 'Name' field is set to 'Webex_Edge_Audio_Traversal' and the 'Type' is 'Traversal server'. The 'Connection credentials' section shows the 'Username' as 'apptraversal'.

Field	Value
Name	Webex_Edge_Audio_Traversal
Type	Traversal server
Username	apptraversal

The screenshot shows the 'SIP' configuration page in Cisco Expressway-E. The 'SIP' section is highlighted with a red box. The 'Port' is set to '7003', 'Transport' is 'TLS', and 'TLS verify subject name' is 'exp-c04.ucdemolab.com'.

Field	Value
Mode	On
Port	7003
Transport	TLS
TLS verify subject name	exp-c04.ucdemolab.com

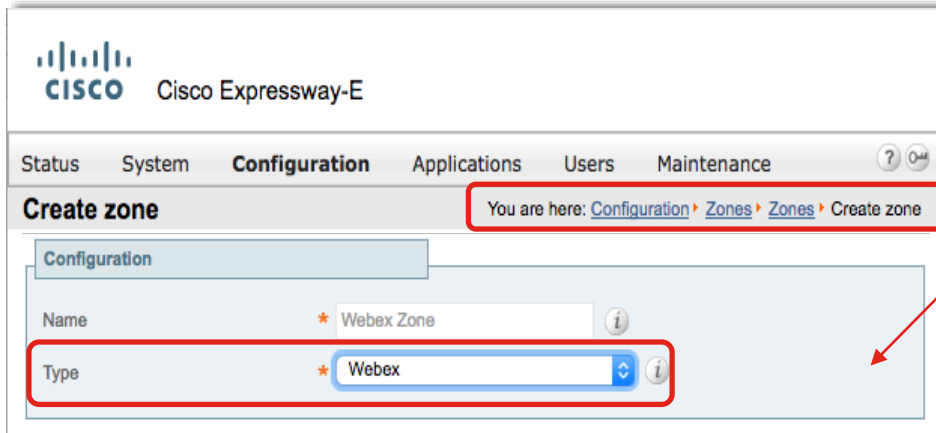
Webex Edge Audio Call-in Set Up Steps:

4. Configure Expressway-E

- Set up Secure Traversal Server Zone.

Cisco Webex Edge Audio

Architecture configuration – Dial in



Webex Edge Audio Call-in Set Up Steps:

4. Configure Expressway-E

- ✓ Set up Secure Traversal Server Zone.
- Set up mTLS zone to Webex
- If you're using an Expressway version before X8.11, then the DNS Zone with Mutual TLS (mTLS).
- If you're using Expressway version x8.11 or later, then the Webex Zone.

Cisco Webex Edge Audio

Architecture configuration – Dial in

The screenshot shows the Cisco Expressway-E configuration interface. The breadcrumb trail is: Configuration > Dial plan > Search rules > Create search rule. The configuration form is titled "Create search rule" and includes the following fields:

- Rule name:
- Description:
- Priority:
- Protocol:
- SIP variant:
- Source:
- Source name:
- Request must be authenticated:
- Mode:
- On successful match:
- Target:
- State:

Red boxes highlight the "Source name" and "Target" fields, with red arrows pointing to them from the right side of the page.

Webex Edge Audio Call-in Set Up Steps:

4. Configure Expressway-E

- ✓ Set up Secure Traversal Server Zone.
- ✓ Set up mTLS zone to Webex
 - ✓ If you're using an Expressway version before X8.11, then the DNS Zone with Mutual TLS (mTLS).
 - ✓ If you're using Expressway version x8.11 or later, then the Webex Zone.
- Define search rules to forward calls between Webex Edge Audio Traversal Zone and Webex Zone

Cisco Webex Edge Audio

Architecture configuration – Dial in

The screenshot shows the Cisco Expressway-E configuration interface. The top navigation bar includes 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The 'Configuration' tab is active. Below the navigation bar, the breadcrumb path 'You are here: Configuration > Protocols > SIP' is highlighted with a red box. The main configuration area is titled 'SIP' and contains a list of settings. The 'Mutual TLS mode' and 'Mutual TLS port' settings are highlighted with a red box, and a red arrow points to the 'Mutual TLS port' input field, which contains the value '5062'. Other settings include SIP mode (On), UDP mode (Off), UDP port (5060), TCP mode (On), TCP port (5060), TLS mode (On), TLS port (5061), TCP outbound port start (25000), TCP outbound port end (29999), Session refresh interval (1800), Minimum session refresh interval (500), and TLS handshake timeout (5).

Setting	Value
SIP mode	On
UDP mode	Off
UDP port	5060
TCP mode	On
TCP port	5060
TLS mode	On
TLS port	5061
Mutual TLS mode	On
Mutual TLS port	5062
TCP outbound port start	25000
TCP outbound port end	29999
Session refresh interval (seconds)	1800
Minimum session refresh interval (seconds)	500
TLS handshake timeout (seconds)	5

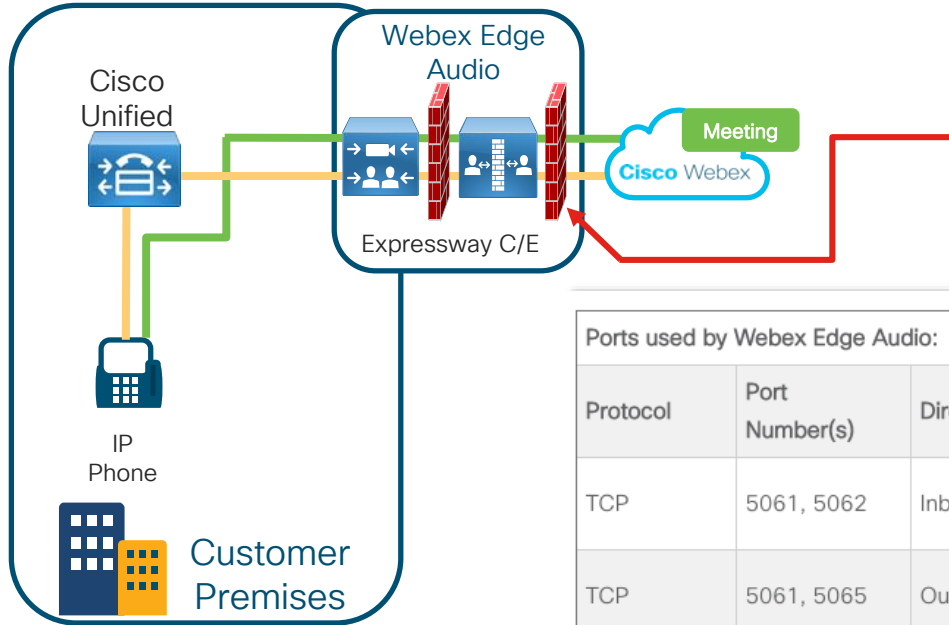
Webex Edge Audio Call-in Set Up Steps:

4. Configure Expressway-E

- ✓ Set up Secure Traversal Server Zone.
- ✓ Set up mTLS zone to Webex
 - ✓ If you're using an Expressway version before X8.11, then the DNS Zone with Mutual TLS (mTLS).
 - ✓ If you're using Expressway version x8.11 or later, then the Webex Zone.
- Define search rules to forward calls between Webex Edge Audio Traversal Zone and Webex Zone
- Configure Mutual TLS (mTLS)

Cisco Webex Edge Audio

Architecture configuration – Dial in



Webex Edge Audio Call-in Set Up Steps:

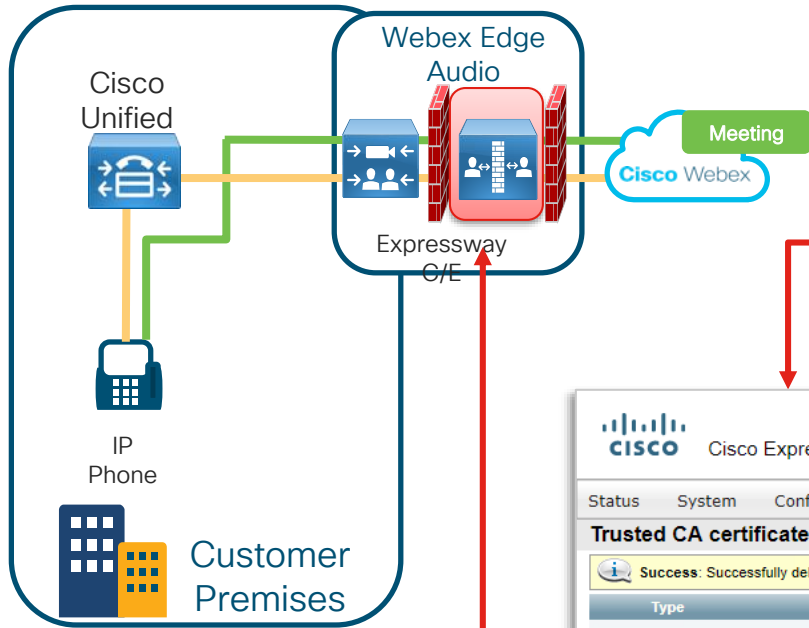
5. **Open Firewall ports**
 - <https://collaborationhelp.cisco.com/article/en-us/WBX264>

Ports used by Webex Edge Audio:

Protocol	Port Number(s)	Direction	Access Type	Comments
TCP	5061, 5062	Inbound	SIP Signaling	Inbound SIP signaling for Webex Edge Audio
TCP	5061, 5065	Outbound	SIP Signaling	Outbound SIP signaling for Webex Edge Audio
UDP	Ephemeral Ports 8000 - 59999	Inbound and Outbound	Media Ports	On Cisco Expressway, the media ranges need to be set to 36000 - 59999

Cisco Webex Edge Audio

Architecture configuration – Dial in



Webex Edge Audio Call-in Set Up Steps:

5. Open Firewall ports

- <https://collaborationhelp.cisco.com/article/en-us/WBX264>

6. Apply Signed Certificate From Trusted Certificate Authority

- <https://collaborationhelp.cisco.com/article/en-us/WBX9000008850>

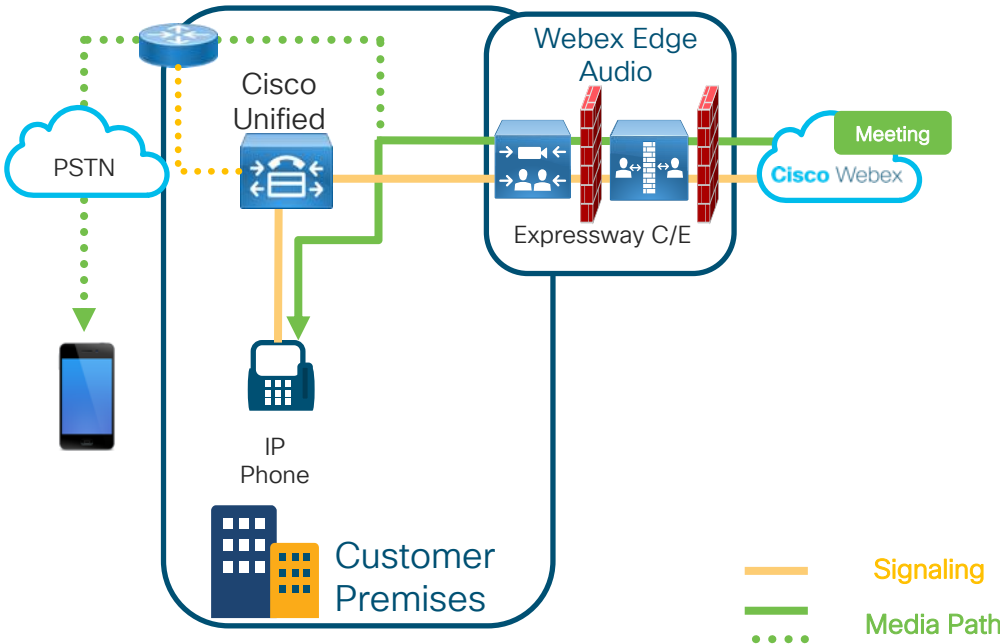
The screenshot shows the Cisco Expressway-E web interface. The page title is 'Cisco Expressway-E'. The navigation tabs are 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The 'Maintenance' tab is selected. The page content is titled 'Trusted CA certificate'. A red box highlights the breadcrumb navigation: 'You are here: Maintenance > Security > Trusted CA certificate'. Below the breadcrumb is a success message: 'Success: Successfully deleted CA certificates'. A table lists the trusted CA certificates. A red box highlights the first certificate entry.

Type	Issuer	Subject	Expiration date	Validity	View
<input type="checkbox"/>	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer	Nov 24 2031	Valid	View (decoded)
<input type="checkbox"/>	O=QuoVadis Limited, CN=QuoVadis Root CA 2	O=HydrantID (Avalanche Cloud Corporation), CN=HydrantID SSL ICA G2	Dec 17 2023	Valid	View (decoded)

Buttons at the bottom: Show all (decoded), Show all (PEM file), Delete, Select all, Unselect all

Cisco Webex Edge Audio

Overview Architecture configuration – Call Back

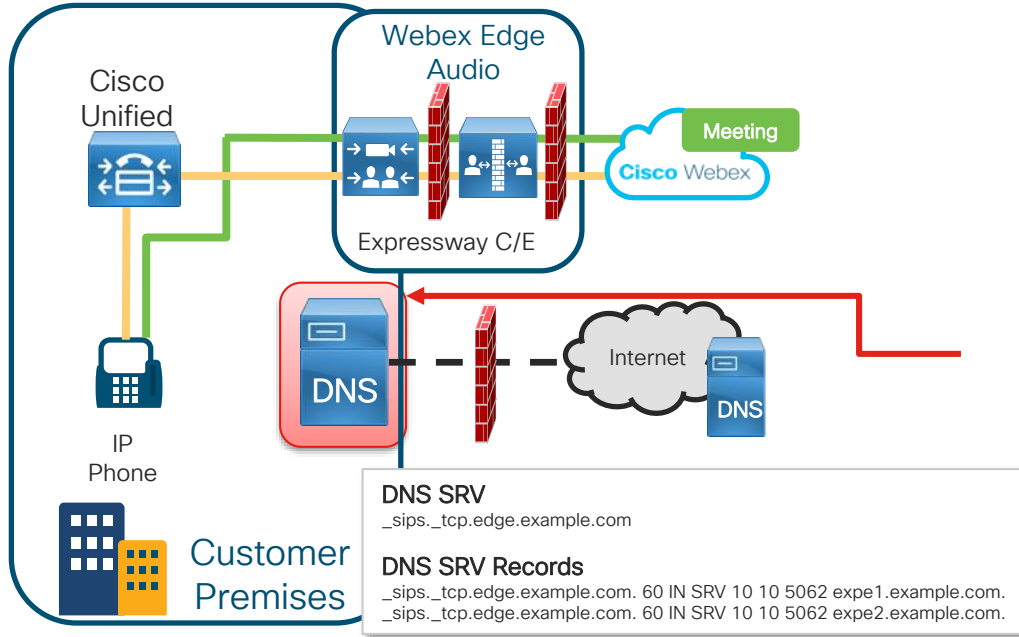


Overview of the Webex Edge Audio Callback Set Up Steps:

1. Apply Webex Edge Audio Callback Settings
 - Define country callback parameters in Control Hub
 - Ensure the proper SRV record configuration for Expressway - E
 - Ensure connectivity checks are successful.
2. Configure Expressway- E to accept calls and route to Expressway - C
3. Configure Expressway - C to accept calls and route them to Cisco UCM
4. Cisco UCM routes the +E.164 audio call to the IP phones or local PSTN

Cisco Webex Edge Audio

Architecture configuration – Call Back



Create DNS SRV Records for Expressway-E with the following parameters:

1. SIPs (_sips._tcp) DNS SRV record for peering domain (for example edge.example.com). It is recommended that Edge Audio Expressways have its own subdomain.
2. The DNS SRV records must refer to the mutual TLS port (the default mutual TLS port is 5062). You cannot 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. Both MRA and B2b cannot use mutual TLS.
3. The hostnames (FQDNs) in the DNS SRV records must resolve to the Expressway-E cluster's IP addresses through DNS A/AAAA record(s).

[DNS-SRV-Records-for-Expressway-E document](https://help.webex.com/preview/en-us/eb6cb7/DNS-SRV-Records-for-Expressway-E)

<https://help.webex.com/preview/en-us/eb6cb7/DNS-SRV-Records-for-Expressway-E>

Cisco Webex Edge Audio

Architecture configuration – Call Back



Cisco Webex Control Hub

Webex Edge Audio

Cisco Webex Meetings Sites > Configure ucdemolab-webex.com > Webex Edge Audio

Dial-in Settings

Click Generate Lua Script to save the Lua Script to your computer. Then apply the Lua script to your CUCM in order to update its configuration to allow for appropriate routing of dial-in calls to the cloud. [Click here](#) to view the list of phone numbers allowed under this setting.

[Generate Lua Script](#)

Callback Settings

Country/Region:

Expressway DNS SRV: [Add](#)

Country/Region	Expressway DNS SRV	Connectivity Check Status	Action
American Samoa (1)	mtls.ucdemolab.com	Successful	
Canada (1)	mtls.ucdemolab.com	Successful	
Northern Mariana Islands (1)	mtls.ucdemolab.com	Successful	
United States of America (1)	mtls.ucdemolab.com	Successful	

Settings last updated on Thursday, September 27, 2018 7:29 am. [Click Apply Settings for updates to take effect. Details](#) [Apply Settings](#)

Overview of the Webex Edge Audio Callback Set Up Steps:

1. Apply Webex Edge Audio Callback Settings
 - Define country callback parameters in Control Hub
 - Default settings: **+E.164 number for callback**
 - Ensure proper SRV record configuration for Expressway
 - Note: do not enter the full SRV record entry
 - Ensure connectivity checks are successful.

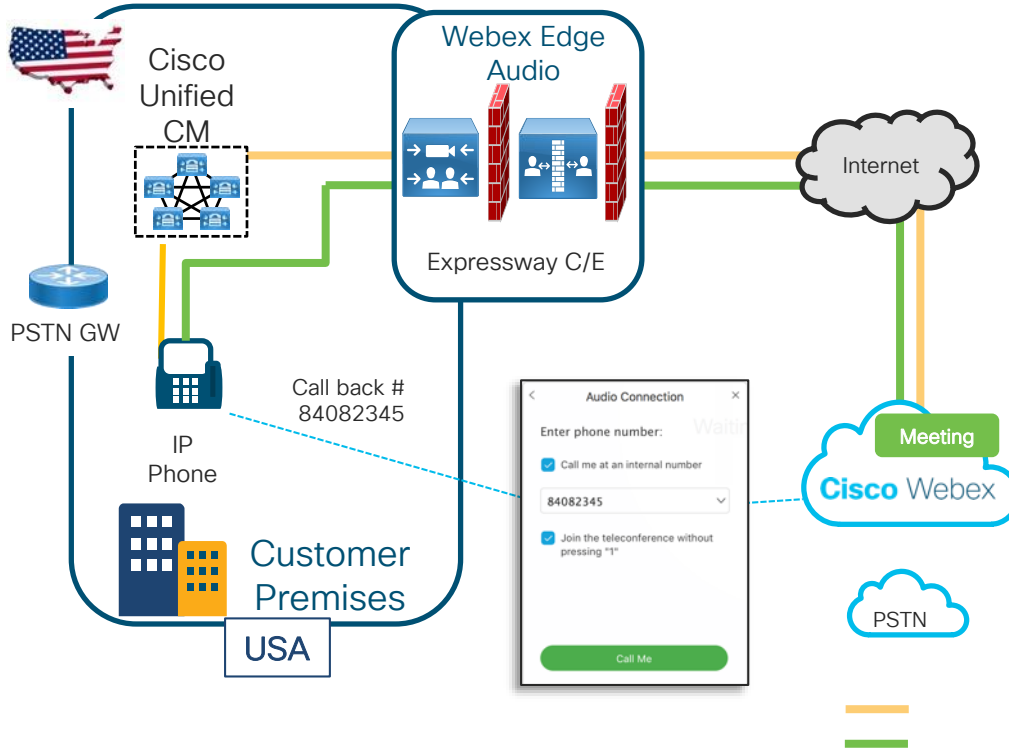
Callback Settings

Country/Region:

Expressway DNS SRV: [Add](#)

Country/Region	Expressway DNS SRV
----------------	--------------------

Extension callback



Edge Audio Extension Callback:

- User defines local extension
- Webex calls back to that extension
- Expressway C/E and CUCM figures out where to send the extension and routes the call to the device

Considerations:

- There will be no PSTN fallback support for extension based call routing.
- It will take a maximum of 30 mins for the extension callback settings to apply

Extension callback configuration



Webex Edge Audio

Cisco Webex Meetings Sites > Configure ucdemolab.webex.com > Webex Edge Audio

solution.

Dial-in Settings

Click Generate Lua Script and save the Lua script to your computer. Then apply the Lua script to [Click here](#) to view the list of phone numbers allowed under this setting.

Callback Settings

Retry call using PSTN Audio Enable

Country/Region: Extension

Expressway DNS SRV:

- Select "Extension" from the drop down list
- Add SRV and click "Apply Settings" button
- A single SRV can be configured for callback

Callback Settings

Retry call using PSTN Audio Enable

Country/Region: Extension

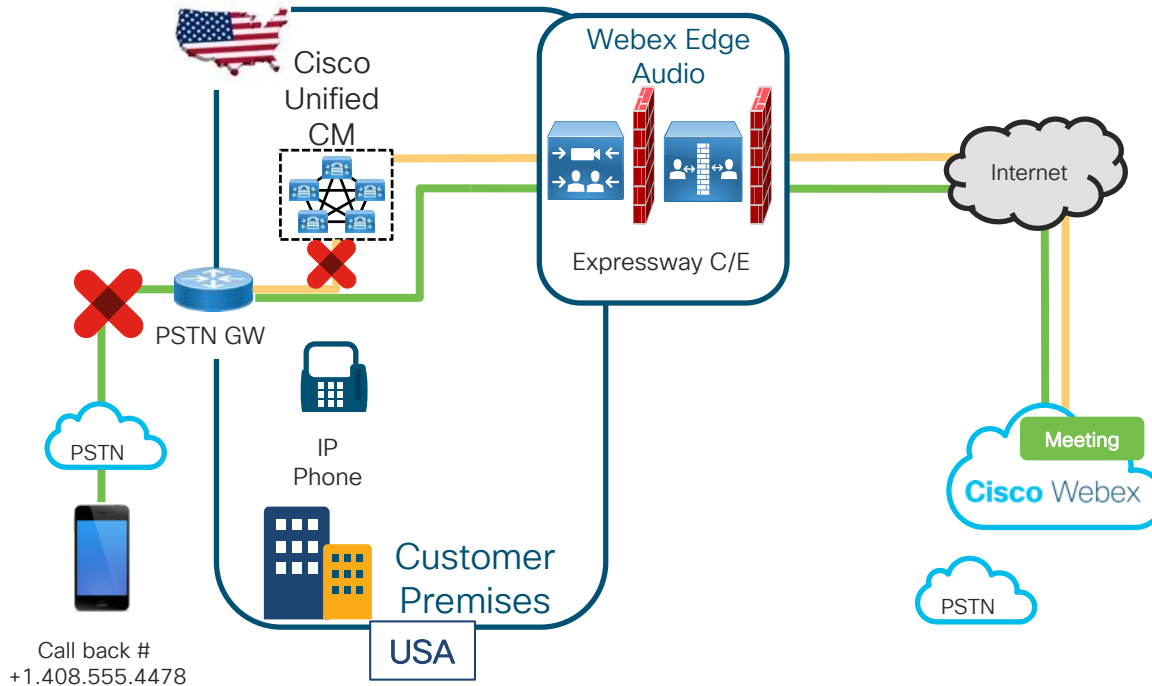
Expressway DNS SRV:

Country/Region	Expressway DNS SRV	Connectivity Check Status
Extension	mtls.ucdemolab.com	● Successful
American Samoa (1)	mtls.ucdemolab.com	● Successful

- Webex 33.x or higher required

Country/Region	Expressway DNS SRV	Connectivity Check Status
Extension	mtls.ucdemolab.com	● Successful
American Samoa (1)	mtls.ucdemolab.com	● Successful

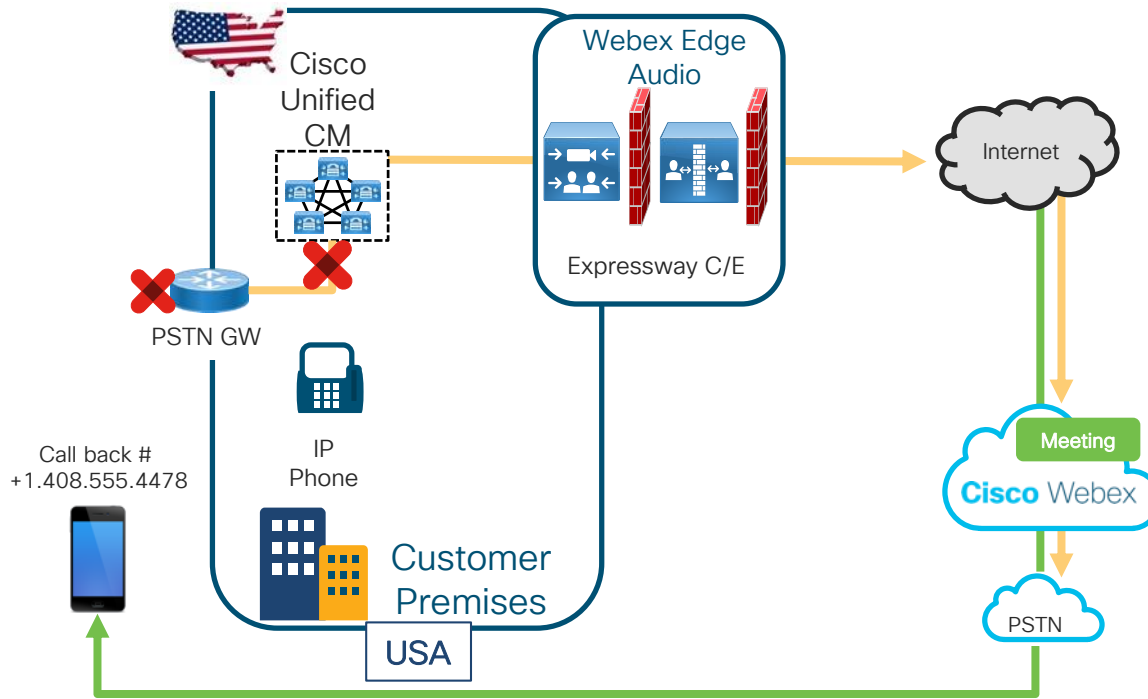
PSTN Fall Back



What if any of these happen?

- No local PSTN capacity
- CUCM blocks callback to PSTN GW
- Customer wants to use Webex PSTN
- Connectivity issue in the path from Webex to the local PSTN GW

PSTN Fall Back



When PSTN fallback will be triggered?

When an Edge Audio call is failed due to

1. DNS issues
 - DNS timeouts / failures
2. TCP issues
 - TCP timeouts / failures
3. TLS issues
 - TLS timeouts / handshake failures
4. SIP error responses
 - 380 / 4xx / 5xx / 6xx

Results:

- A SIP response code is sent to the Webex cloud and the call is rerouted out Webex's PSTN.
- Media is sent from Webex PSTN to the cell phone.

PSTN Fall Back



Cisco Webex Control Hub

- Overview
- Users
- Places
- Services
- Devices
- Analytics
- Troubleshooting
- Settings

Webex Edge Audio

Cisco Webex Meetings Sites > Configure ucdemolab.webex.com > Webex Edge Audio

solution.

Dial-in Settings

Click Generate Lua Script and save the Lua script to your computer. Then apply the Lua script to your Unified CM to update its configurations that allow for the appropriate routing of dial-in calls to the cloud. [Click here](#) to view the list of phone numbers allowed under this setting.

[Generate Lua Script](#)

Callback Settings

When enabled, this option allows calls that fail or are rejected via Edge Audio to redirect using the configured PSTN provider. PSTN charges will apply.

Retry call using PSTN Audio Enable

Country/Region:

Expressway DNS SRV: [Add](#)

Country/Region	Expressway DNS SRV	Connectivity Check Status <input type="checkbox"/>	Action
----------------	--------------------	--	--------

Cisco Webex Edge Audio

Architecture configuration – Call Back



Webex Edge Audio

Cisco Webex Meetings Sites > Configure ucdemolab-webex.com > Webex Edge Audio

Dial-in Settings

Click Generate Lua Script to save the Lua Script to your computer. Then apply the Lua script to your CUCM in order to update its configuration to allow for appropriate routing of dial-in calls to the cloud. [Click here](#) to view the list of phone numbers allowed under this setting.

[Generate Lua Script](#)

Callback Settings

Country/Region:

Expressway DNS SRV: [Add](#)

Country/Region	Expressway DNS SRV	Connectivity Check Status	Action
American Samoa (1)	mtls.ucdemolab.com	Successful	
Canada (1)	mtls.ucdemolab.com	Successful	
Northern Mariana Islands (1)	mtls.ucdemolab.com	Successful	
United States of America (1)	mtls.ucdemolab.com	Successful	

Settings last updated on Thursday, September 27, 2018 7:29 am. [Click Apply Settings](#) for updates to take effect. [Details](#) [Apply Settings](#)

Overview of the Webex Edge Audio Callback Set Up Steps:

1. Apply Webex Edge Audio Callback Settings

- ✓ Define country callback parameters in Control Hub
- Ensure proper SRV record configuration for Expressway
- Ensure connectivity checks are successful.
 - Success – successfully able to connect to Expressway – E.
 - Partial – unable to connect to a node(s)
 - Error – unable to connect to the Expressway – E

Cisco Webex Edge Audio



Callback Settings

Country/Region:

Expressway DNS SRV:

Country/Region	Expressway DNS SRV	Connectivity Check Status
American Samoa (1)	mtls.ucdemolab.com	Partial
Canada (1)	mtls.ucdemolab.com	Partial
Northern Mariana Islands (1)	mtls.ucdemolab.com	Partial
United States of America (1)	mtls.ucdemolab.com	Partial

Settings last updated on Thursday, November 29, 2018 12:30 pm are in effect [View details here](#)

Ensure connectivity checks are successful.

- Success – successfully able to connect to Expressway – E.
- Partial – unable to connect to a node(s)
- Error – unable to connect to the Expressway – E

Mozilla Firefox

https://ucdemolab.webex.com/wbxadmin/ottconnchkresp.do?methodname=connChkResp&dnssrv=mtls.ucdemolab.com

DNS SRV Name	Fully Qualified Domain Name	IP Address
mtls.ucdemolab.com	exp-e03.ucdemolab.com	198.135.2.105
	exp-e04.ucdemolab.com	198.135.2.102

Test for: **exp-e03.ucdemolab.com 198.135.2.105:5062**

Test	Result	Detail	Troubleshooting Detail
TCP Connection	Error	Connect attempt to the host timed out.	Check network connectivity, connection speed, firewall configuration.

Test for: **exp-e04.ucdemolab.com 198.135.2.102:5062**

Test	Result	Detail	Troubleshooting Detail
State Check Complete	Successful	SIP Connectivity check successful.	

[Webex Edge Audio Troubleshooting Guide](#) Close



Cisco Webex Edge Audio

Architecture configuration – Call Back



Webex Edge Audio

Cisco Webex Meetings Sites > Configure ucdemolab.webex.com > Webex Edge Audio

Dial-in Settings

Click Generate Lua Script to save the Lua Script to your computer. Then apply the Lua script to your CUCM in order to update its configuration. After the configuration of dial-in calls to the cloud, click here to view the list of phone numbers allowed under this setting.

The page at <https://ucdemolab.webex.com> says:
Note that applying this setting may take up to 30 minutes to be effective.

Cancel OK

Generate Lua Script

Callback Settings

Country/Region: Afghanistan (93)

Expressway DNS SRV: Add

Country/Region	Expressway DNS SRV	Connectivity Check Status	Action
American Samoa (1)	mtls.ucdemolab.com	Successful	
Canada (1)	mtls.ucdemolab.com	Successful	
Northern Mariana Islands (1)	mtls.ucdemolab.com	Successful	
United States of America (1)	mtls.ucdemolab.com	Successful	

Settings last updated on Thursday, September 27, 2018 7:29 am. Click Apply Settings for updates to take effect. Details

Apply Settings

Overview of the Webex Edge Audio Callback Set Up Steps:

1. Apply Webex Edge Audio Callback Settings
 - ✓ Define country callback parameters in Control Hub
 - ✓ Ensure proper SRV record configuration for Expressway
 - ✓ Ensure connectivity checks are successful.
 - ✓ Success – successfully able to connect to Expressway – E.
 - ✓ Partial – unable to connect to a node(s)
 - ✓ Error – unable to connect to the Expressway – E
 - Click Apply to activate the call back settings

Cisco Webex Edge Audio

Architecture configuration – Call Back



Exp - E

The screenshot shows the Cisco Expressway-E configuration interface. At the top, there is a navigation bar with tabs for Status, System, Configuration, Applications, Users, and Maintenance. Below this is a breadcrumb trail: 'You are here: Configuration > Zones > Zones > Create zone'. The main content area is titled 'Create zone' and contains two input fields: 'Name' with the value 'Webex Zone' and 'Type' with a dropdown menu set to 'Webex'. A red arrow points to the 'Webex' option in the dropdown menu.

Overview of the Webex Edge Audio Callback Set Up Steps:

- ✓ Apply Webex Edge Audio Callback Settings
 - ✓ Define country callback parameters in Control Hub
 - ✓ Ensure proper SRV record configuration for Expressway
 - ✓ Ensure connectivity checks are successful.
- 2. **Configure Expressway-E to accept calls and route to Expressway - C**
 - Create Webex zone (x8.11) or DNS zone (x8.10).
 - Note: this could have already been done if dial in configuration is enabled.
 - Create search rule to route Edge Audio Calls to Expressway - C

Cisco Webex Edge Audio

Architecture configuration – Call Back



Exp - E

Cisco Expressway-E

Status System **Configuration** Applications Users Maintenance

Edit search rule

Configuration

Rule name * Inbound - webex edge audio v2 ⓘ

Description match on mtls subdomain and NEW tags for edge audio calls ⓘ

Priority * 22 ⓘ

Protocol SIP ⓘ

SIP variant All SIP Variants ⓘ

Source Named ⓘ

Source name * Webex Zone ⓘ

Request must be authenticated No ⓘ

Mode Alias pattern match ⓘ

Pattern type Regex ⓘ

Pattern string * ([*]@mtls.ucdemolab.com.*-cisco-webex-service=audio) ⓘ

Replace Replace ⓘ

Replace string l1@ucdemolab.com ⓘ

On successful match Stop ⓘ

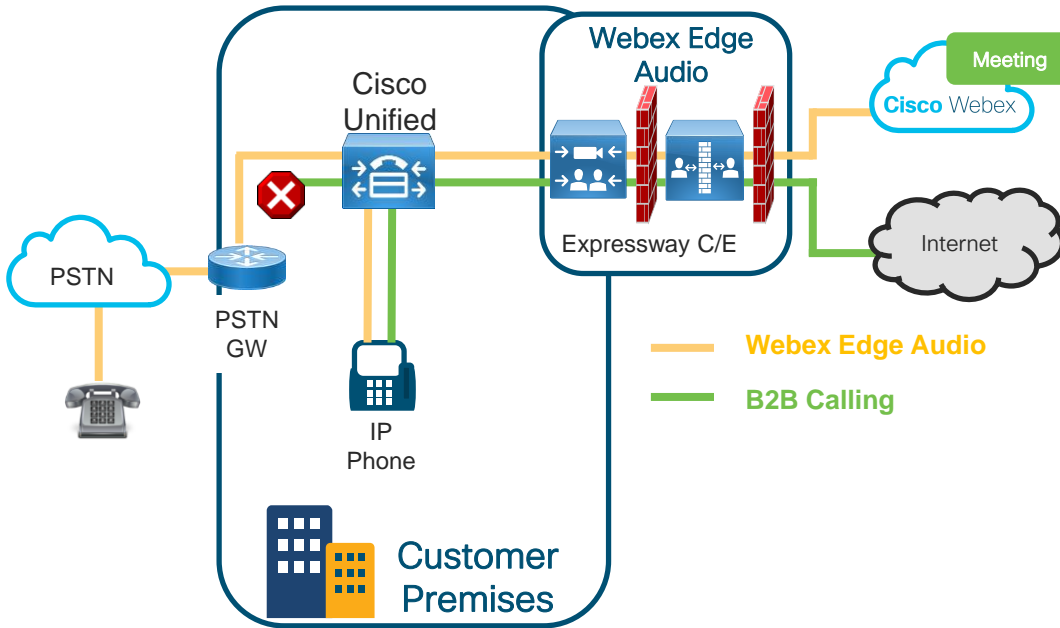
Target * Expy-C_WEA ⓘ

State Enabled ⓘ

Overview of the Webex Edge Audio Callback Set Up Steps:

- ✓ Apply Webex Edge Audio Callback Settings
 - ✓ Define country callback parameters in Control Hub
 - ✓ Ensure proper SRV record configuration for Expressway
 - ✓ Ensure connectivity checks are successful.
- 2. **Configure Expressway-E to accept calls and route to Expressway - C**
 - ✓ Create Webex or DNS zone (depends on version of Expressway software.)
 - Create search rule to route Edge Audio Calls to Expressway - C

Best practices/Toll Fraud



- When sharing Expressway-C/E for Webex Edge Audio and B2B calling differentiated CoS is required
- Make a new SIP trunk from CUCM to Exp-C. Do not use an existing trunk
- B2B calls should not have access to PSTN
- Create dedicated traversal zones, Expressway neighbor zones and UCM SIP trunks for Webex Edge call-back
- Apply tag to search rule “.*x-cisco-webex-service=audio” to only allow Edge Audio calls to traverse the path.
- MRA and Edge Audio can co-reside on the same Expressway C/E pair

Best practices/Toll Fraud



Exp - E

The screenshot shows the Cisco Expressway-E configuration interface. The top section is titled "Edit search rule" and contains the following fields:

- Rule name: `* inbound - webex edge audio v2`
- Description: `match on mtls subdomain and NEW tags for edge audio calls`
- Priority: `22`
- Protocol: `SIP`
- SIP variant: `All SIP Variants`
- Source: `Named`
- Source name: `Webex Zone`
- Request must be authenticated: `No`
- Mode: `Alias pattern match`
- Pattern type: `Regex`
- Pattern string: `(.*)@mtls\ucdemolab\.com;.*x-cisco-webex-service=audio`

The bottom section is titled "Call Policy rules" and contains a table of rules:

Source	Destination	Action	Rearrange	Actions
<input type="checkbox"/> Webex Zone	.*	Allow	↓	View/Edit
<input type="checkbox"/> .*	^[a-z].*@(ce\ space\)\ucdemolab\.com.*	Allow	↑↓	View/Edit
<input type="checkbox"/> .*	^d{4,6}@(\ space\)\ucdemolab\.com.*	Allow	↑↓	View/Edit
<input type="checkbox"/> .*	.*	Reject	↑	View/Edit

- Apply tag to search rule:
`(.*)@mtls.ucdemolab.com;.*x-cisco-webex-service=audio`
- Makes sure only Edge Audio traffic goes across the zone.
- Allows customers to add a new rule to trust Webex Zone in the Call Policy and not change existing rules.
- Place Webex Zone rule first before other rules

Cisco Webex Edge Audio

Architecture configuration – Call Back



Exp - C

Cisco Expressway-C

Status System **Configuration** Applications Users Maintenance

Edit search rule You are here: Configuration > Dial plan > Search rules > Edit search rule

Configuration

Rule name: * inbound from webex edge audio

Description: all webex edge audio traversal route to edge audio CUCM trunk

Priority: * 21

Protocol: SIP

SIP variant: All SIP Variants

Source: Named

Source name: * Webex_Edge_Audio_Traversal

Request must be authenticated: No

Mode: Any alias

On successful match: Stop

Target: * CUCM Core - Edge Audio Only

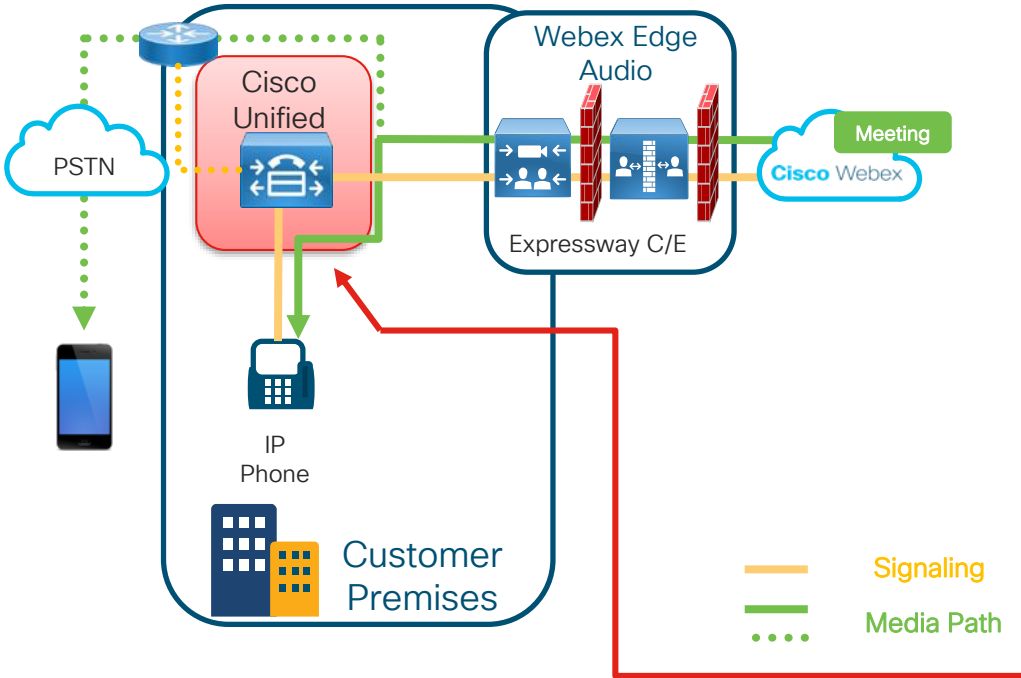
State: Enabled

Overview of the Webex Edge Audio Callback Set Up Steps:

- ✓ Apply Webex Edge Audio Callback Settings
 - ✓ Define country callback parameters in Control Hub
 - ✓ Ensure proper SRV record configuration for Expressway
 - ✓ Ensure connectivity checks are successful.
- ✓ Configure Expressway-E to accept calls and route to Expressway - C
- 3. **Configure Expressway-C to accept calls and route to Cisco UCM**

Cisco Webex Edge Audio

Architecture configuration – Call Back

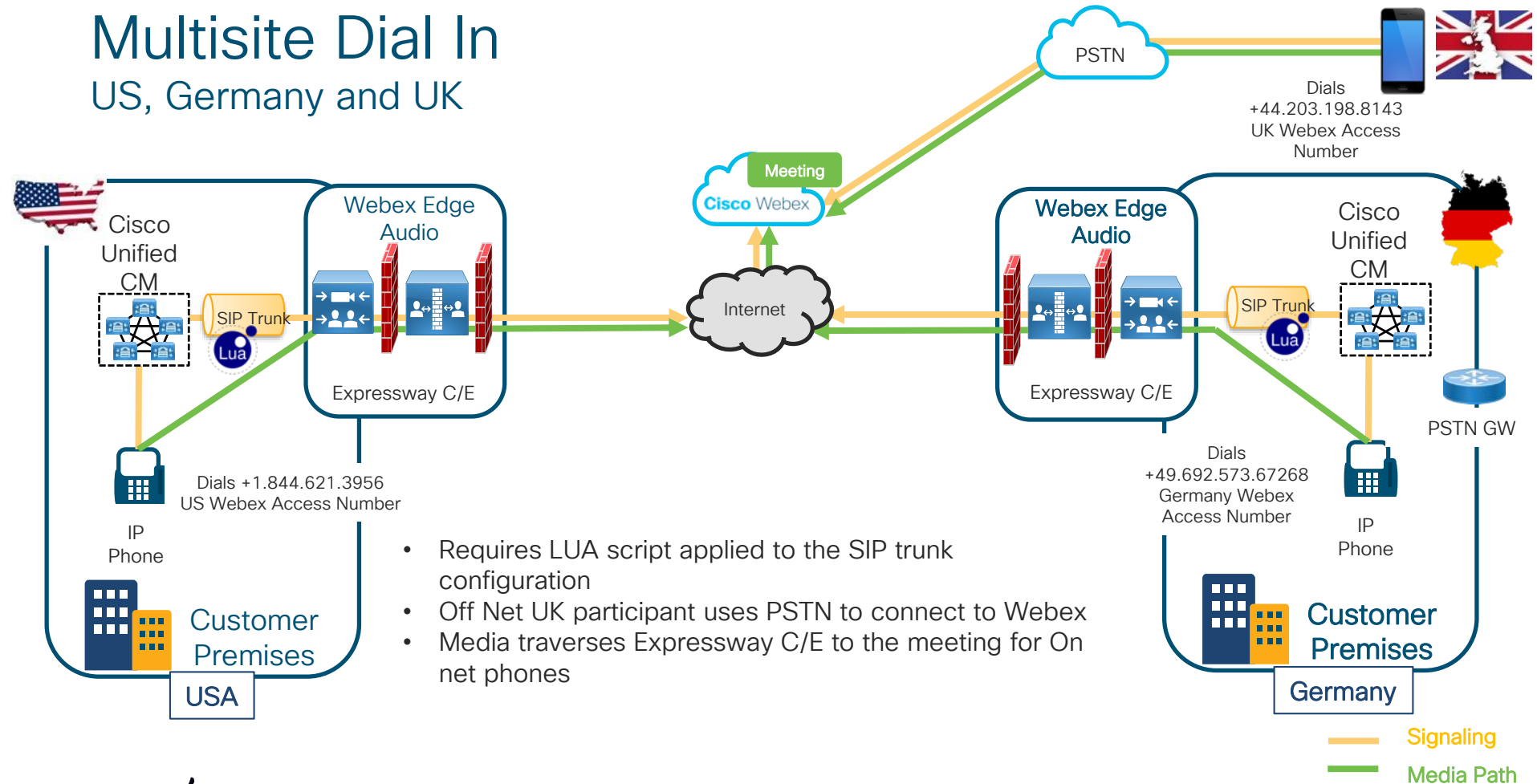


Overview of the Webex Edge Audio Callback Set Up Steps:

- ✓ Apply Webex Edge Audio Callback Settings
 - ✓ Define country callback parameters in Control Hub
 - ✓ Ensure proper SRV record configuration for Expressway
 - ✓ Ensure connectivity checks are successful.
- ✓ Configure Expressway-E to accept calls and route to Expressway – C
- ✓ Configure Expressway-C to accept calls and route to Cisco UCM
- 4. **Cisco UCM routes the +E.164 audio call to the IP phones or local PSTN**

Deployment Scenarios

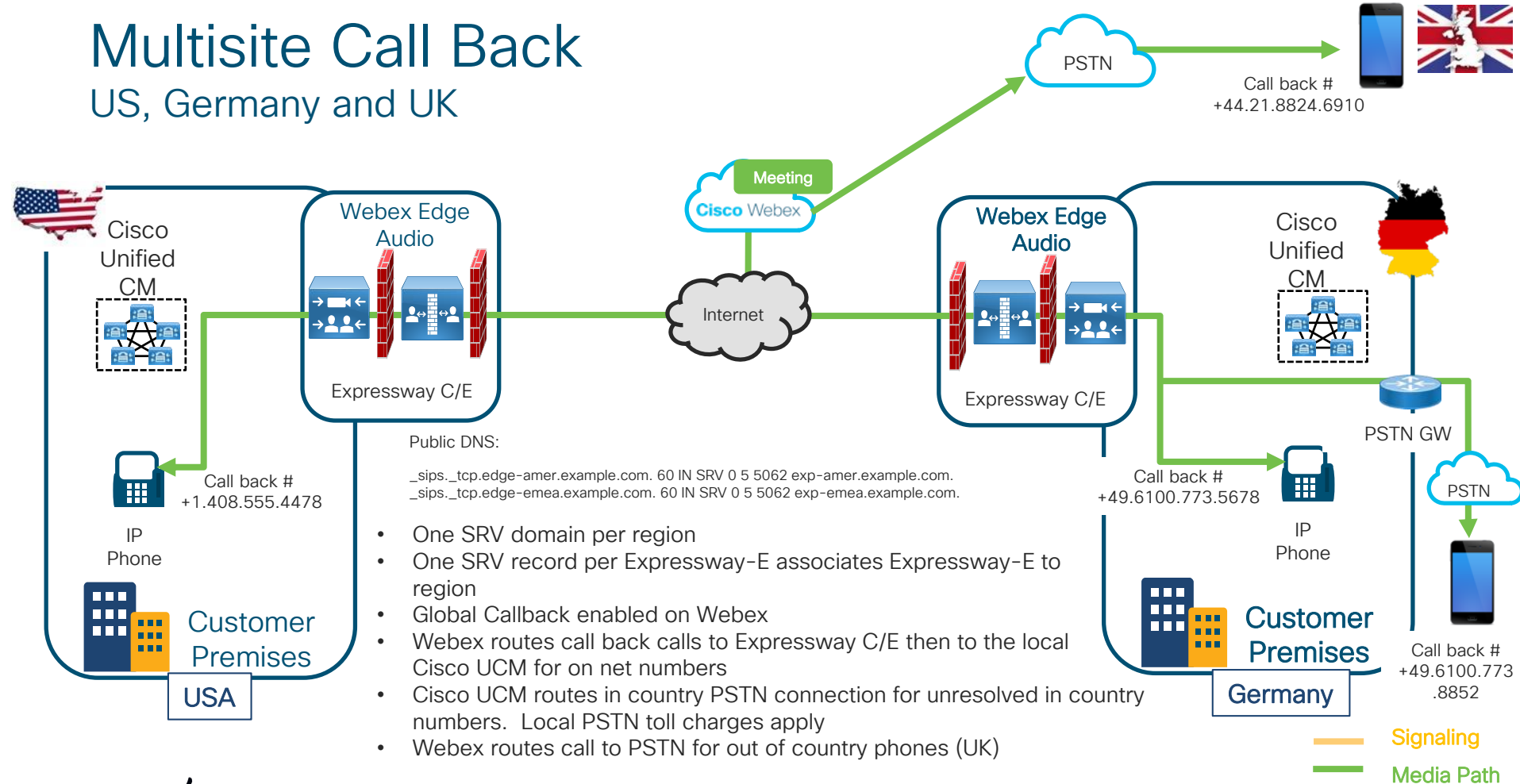
Multisite Dial In US, Germany and UK



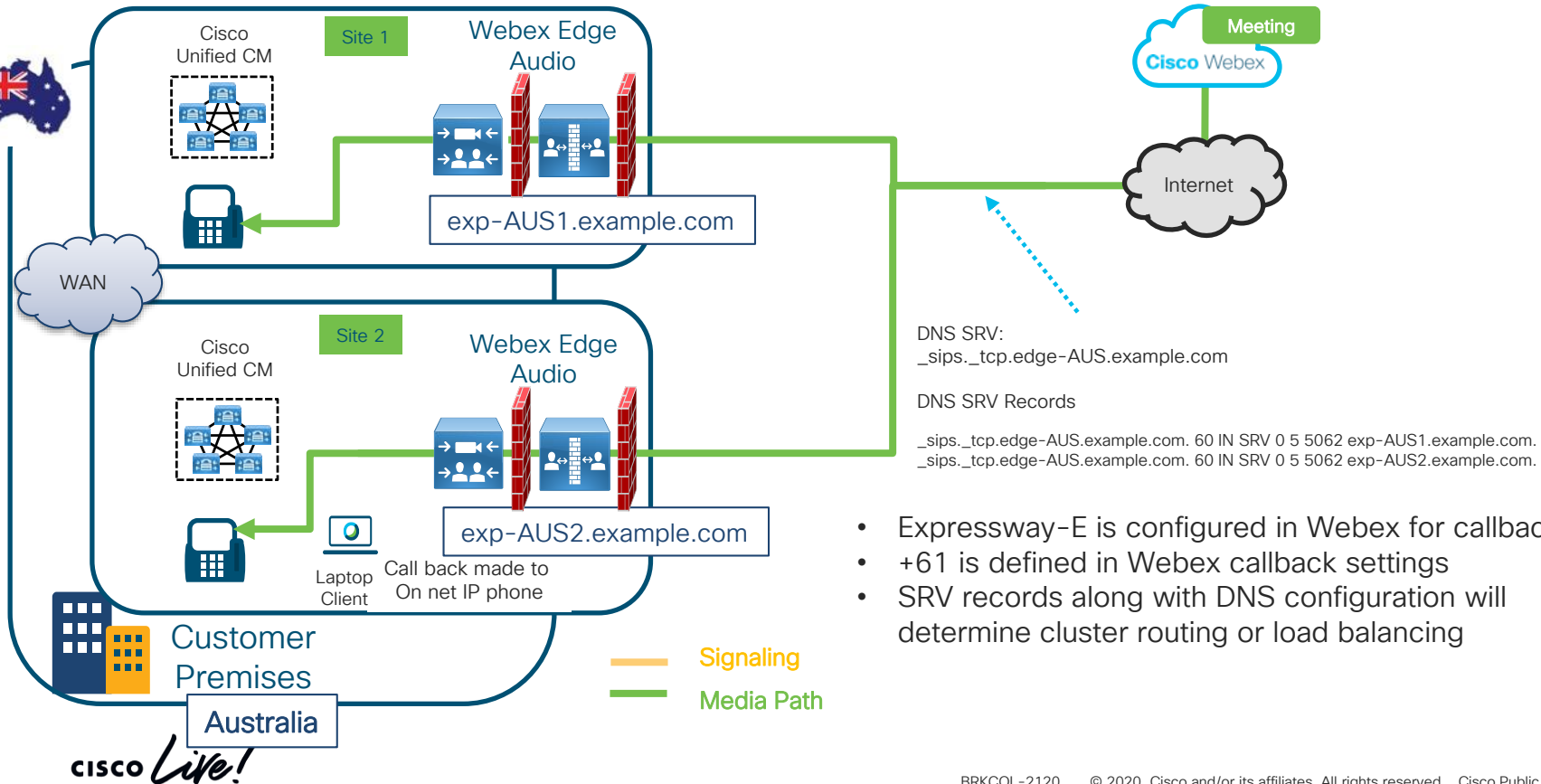
- Requires LUA script applied to the SIP trunk configuration
- Off Net UK participant uses PSTN to connect to Webex
- Media traverses Expressway C/E to the meeting for On net phones

Multisite Call Back

US, Germany and UK

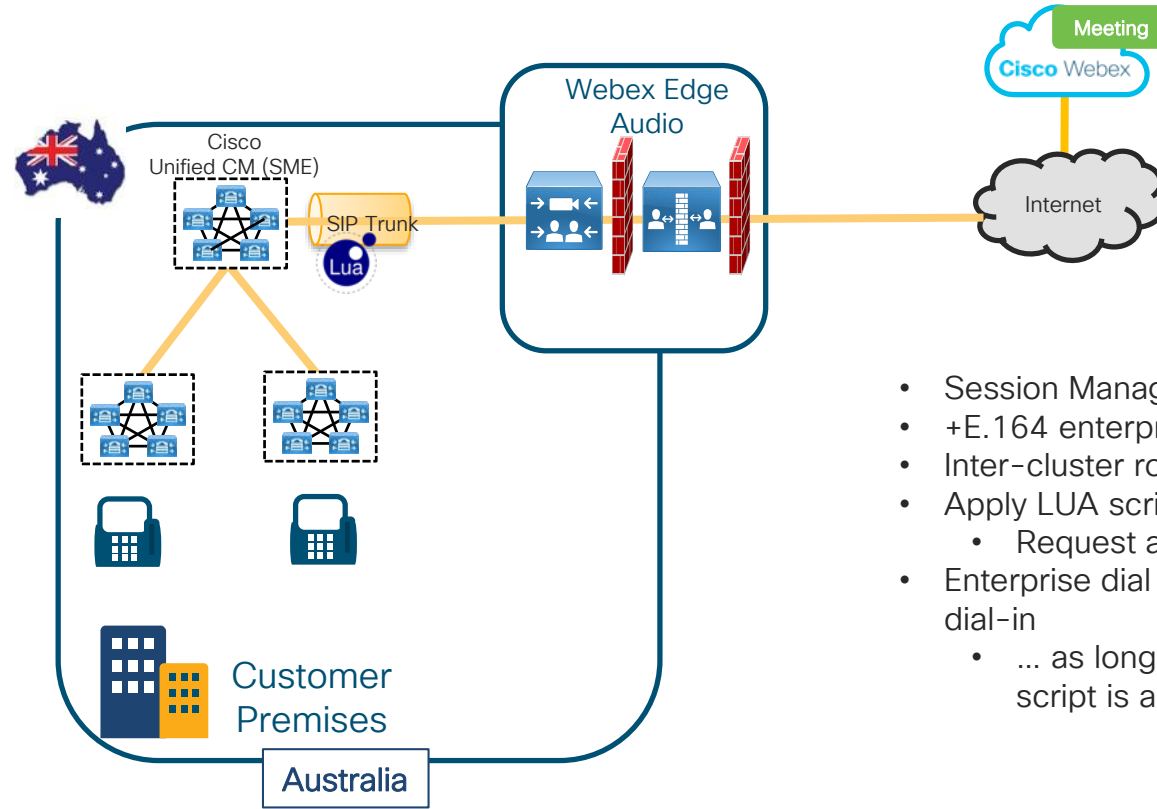


Single Country Call Back – Multiple Expressways clusters



- Expressway-E is configured in Webex for callback
- +61 is defined in Webex callback settings
- SRV records along with DNS configuration will determine cluster routing or load balancing

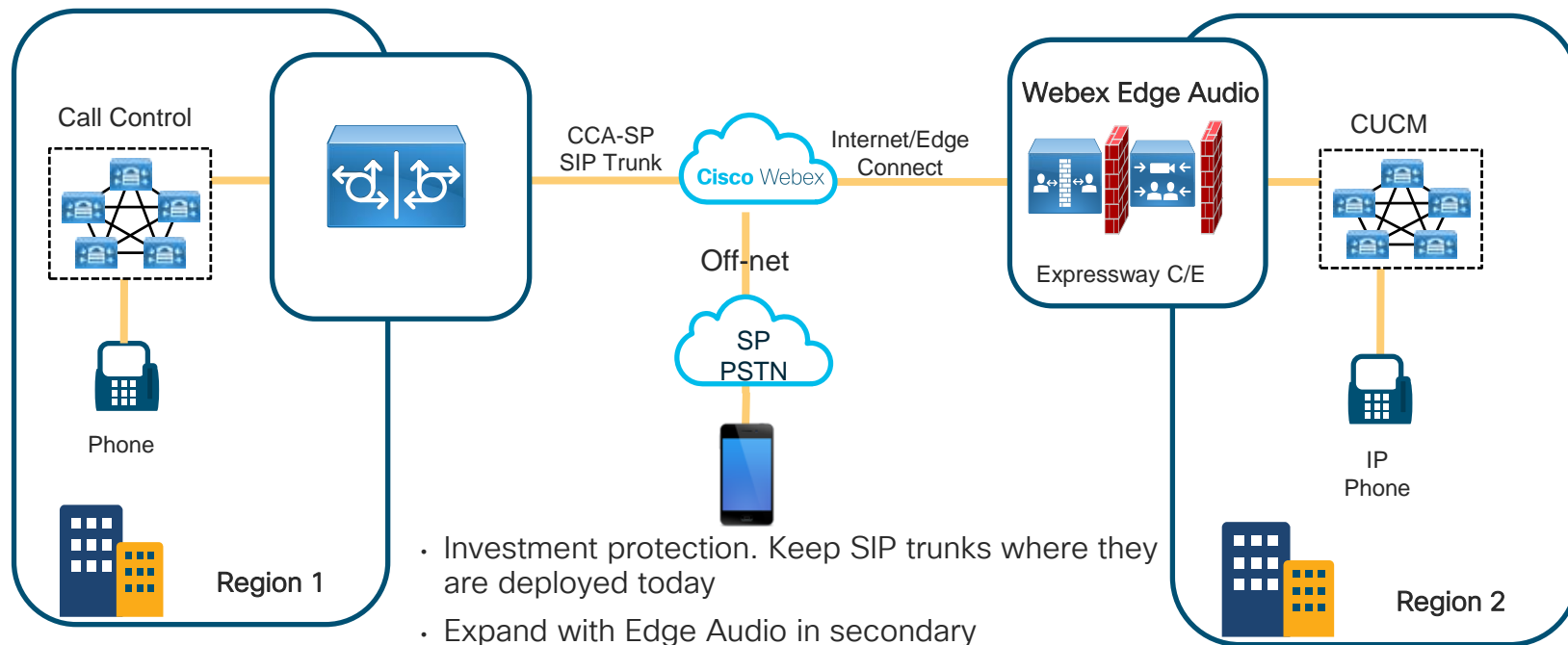
Single site with SME



- Session Manager Edition is supported
- +E.164 enterprise dial plan to route dial-in and call-back
- Inter-cluster routing using ILS/GDPR
- Apply LUA script on SME trunk for dial-in
 - Request and To: URI manipulation
- Enterprise dial plan can support arbitrary dialing habits for dial-in
 - ... as long as the number ultimately exposed to LUA script is a valid +E.164 Webex dial-in number

Cisco Webex Edge Audio w/ CCA-SP

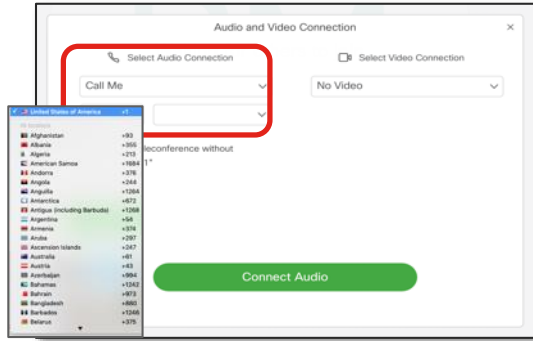
Mixed SIP Trunk & Expressway as Edge in Region 1 and Region 2



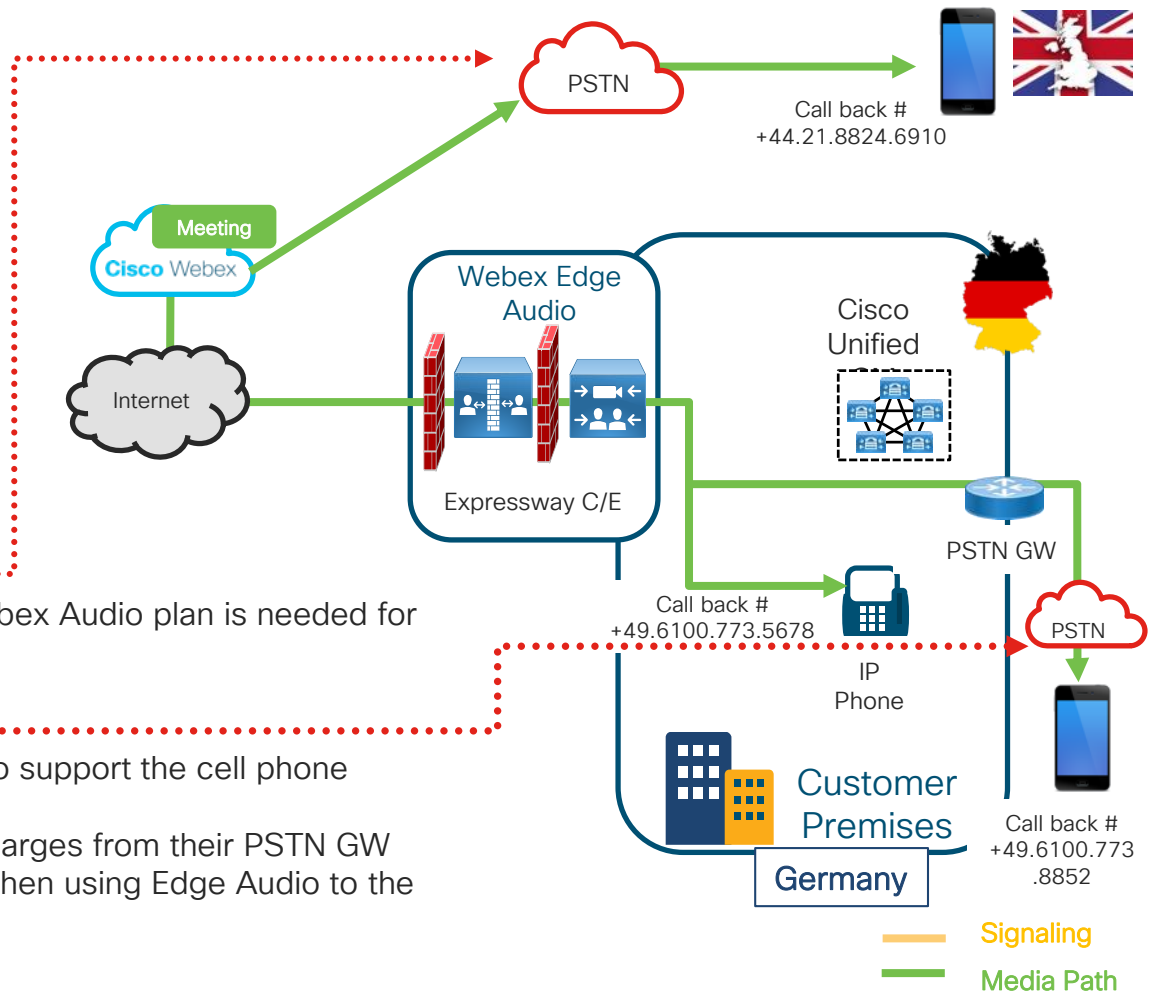
- Investment protection. Keep SIP trunks where they are deployed today
- Expand with Edge Audio in secondary locations/regions
- Both architectures work to support the audio calls

Audio Costs

Where can it occur?



- Webex
 - A committed or uncommitted Webex Audio plan is needed for Webex PSTN
- Customer premises
 - Customer needs audio capacity to support the cell phone users
 - Customer will have local PSTN charges from their PSTN GW
 - Webex PSTN minutes not used when using Edge Audio to the customer premises



Edge Audio Reporting

- Number of Edge Audio calls
- Dial in and callback numbers are combined.

Audio Sources

Audio usage minutes breakdown in various sources.

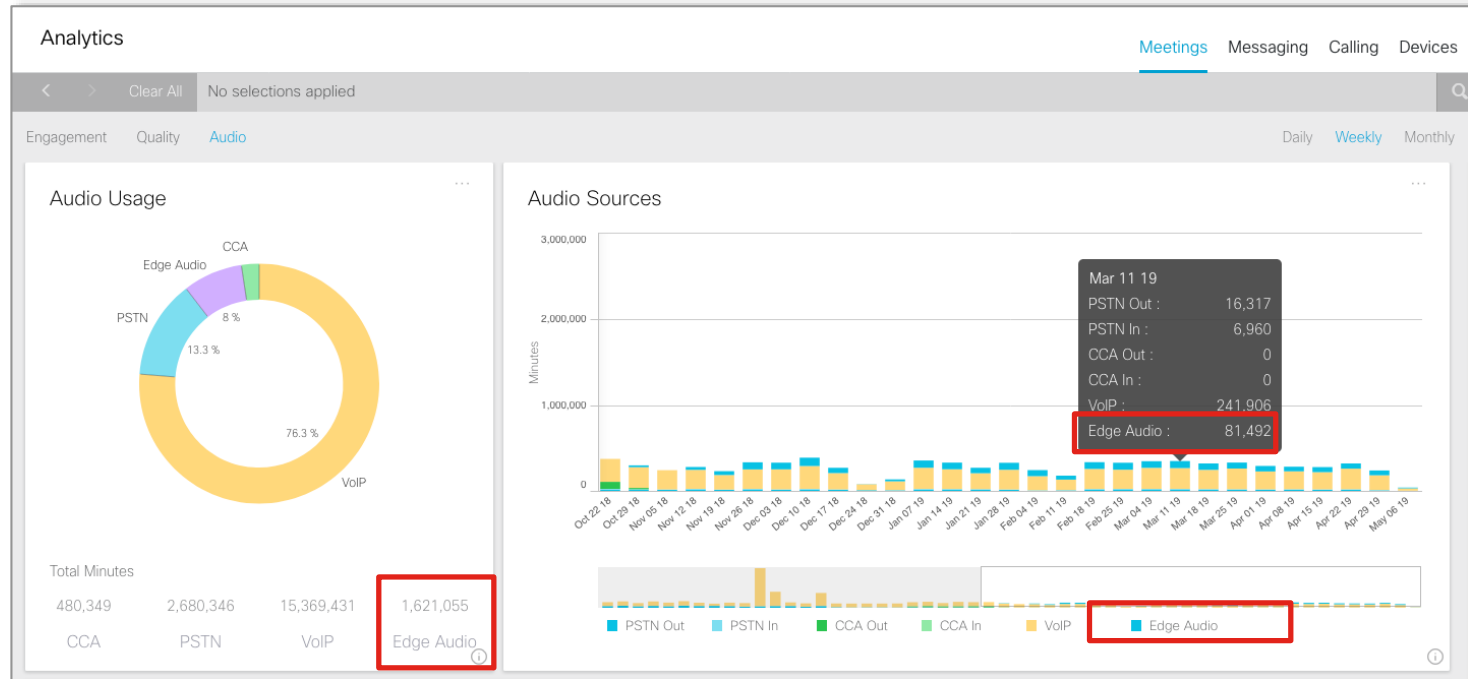
PSTN In/Out - users dialed In/Out through WebEx audio providers' PSTN network.

CCA In/Out IP - users dialed In/Out through CCA partners' PSTN network.

VoIP - users selected the "Call Using Computer" audio and video option from the Webex client.

Edge Audio - calls via IP Phone through Webex Edge Audio VoIP.

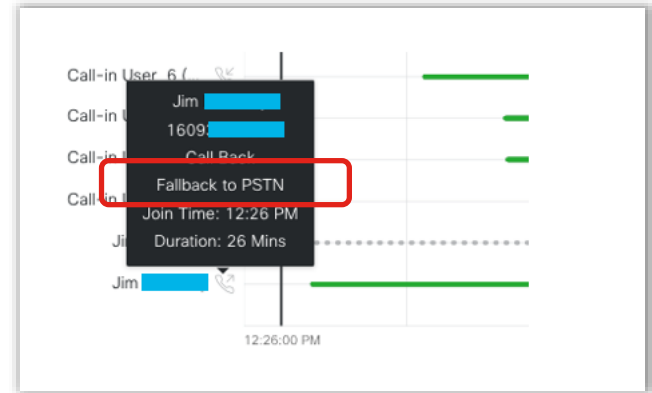
Fallback - calls routed over PSTN/CCA when Webex meeting callback over Edge Audio failed.



Edge Audio Reporting

PSTN Fallback indicators

- Possible Fallback Reasons:
 - DNS TimeOut
 - DNS Error
 - TCP Timeout
 - TLS Timeout
 - TLS Failure
 - SIP error



- If PSTN/CCA fallback occurred in a call back situation, it is indicated in the client details popup.

Participants								
User Name	Activity	Start Date	Duration	Endpoint	Client IP	Gateway IP	End Reason	Location
Jim [REDACTED]		2019-06-29 12:26:57	25:28	Call Back 1609-[REDACTED]			Fallback to PSTN SIP Error(404)	N/A

Webex Edge Video Mesh

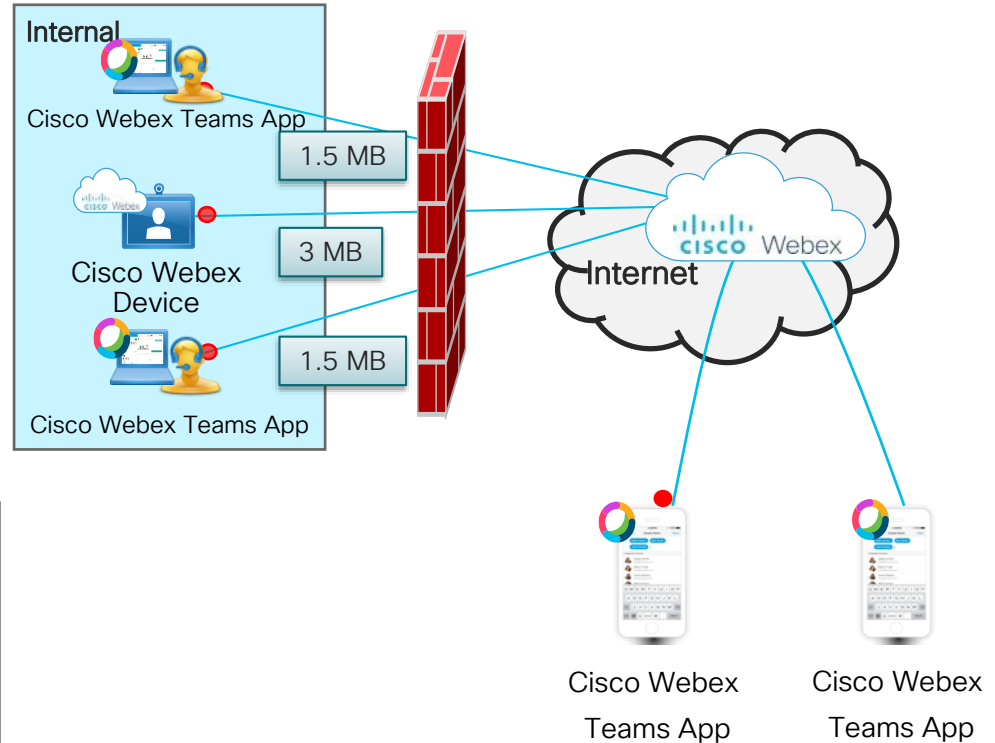
Webex Video Mesh

Problem

- 1:1 meetings use a cloud resource to meet
- Multiparty meetings use a cloud resource to meet
- Signaling and media go to and from the cloud
- Increased bandwidth requirement for the Internet with adoption of Cisco Webex Meetings

Solution

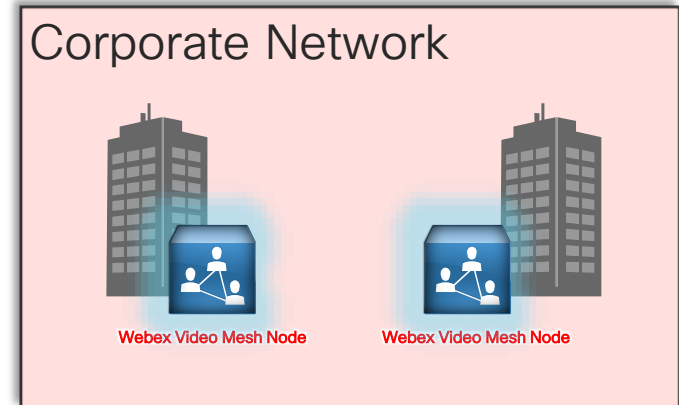
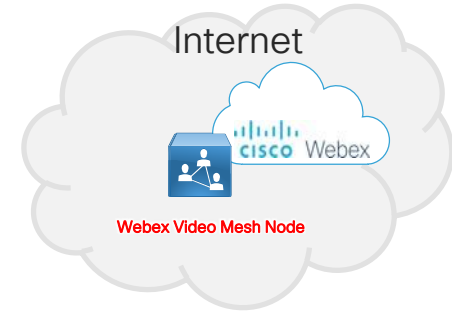
Cisco Webex Video Mesh



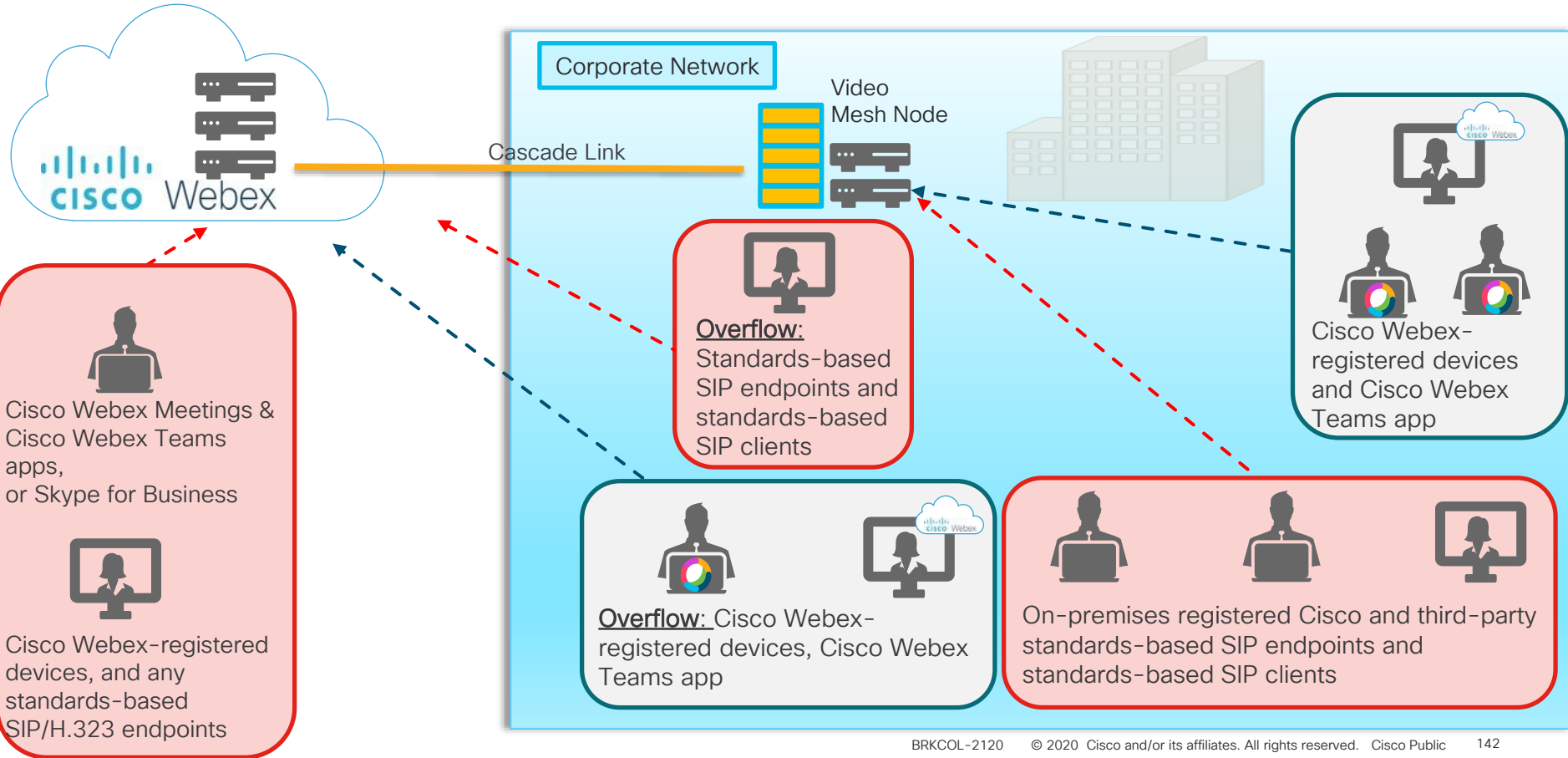
Webex Video Mesh

What is it?

- A little piece of our cloud on your premises
- Cisco cloud meeting capabilities packaged in a software image for on-premises deployment
- Ability to provide local media processing on the corporate network.
- Customers can deploy Video Mesh Nodes across multiple locations, optimizing media quality within a location and bandwidth across locations
- Automatic overflow from on-premises Video Mesh Node to cloud nodes
- Automatic upgrades of Video Mesh Nodes
- Single pane of glass for management, resource monitoring and usage metrics

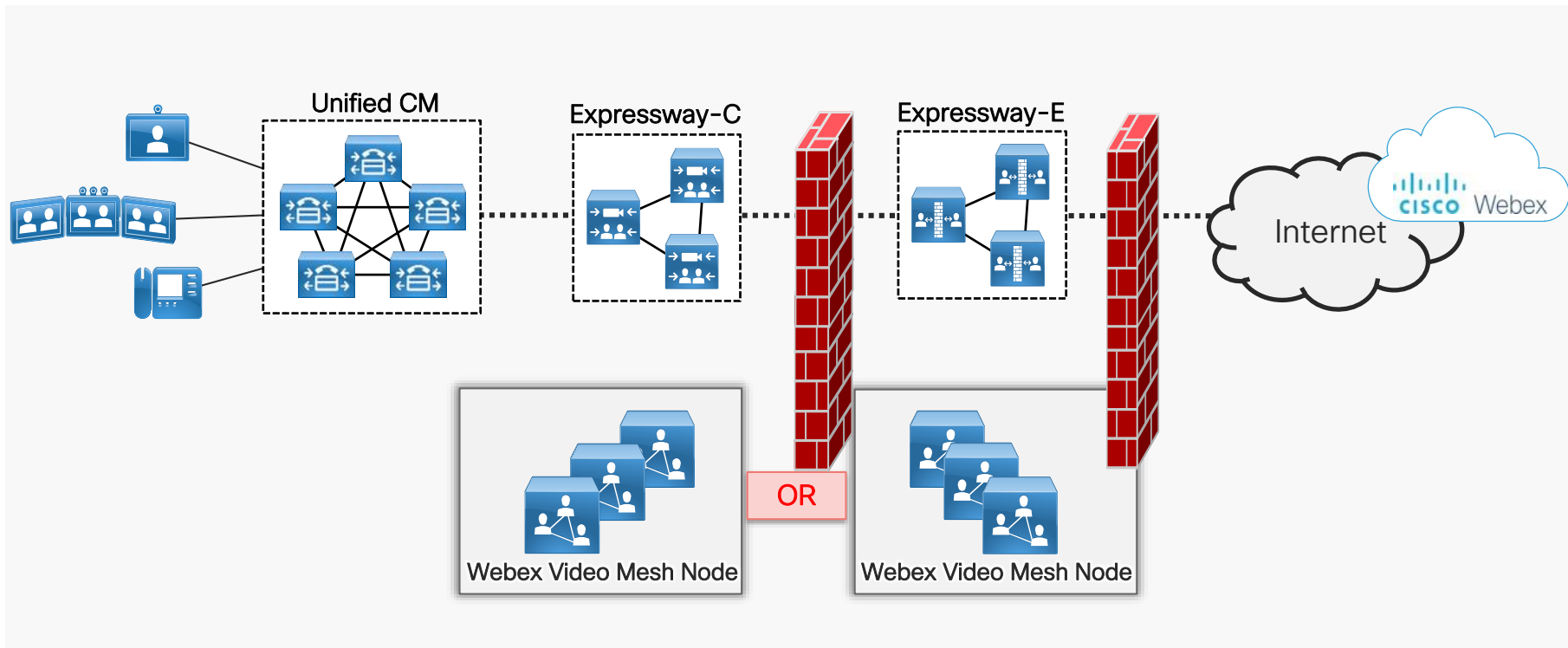


Cisco Webex Video Mesh



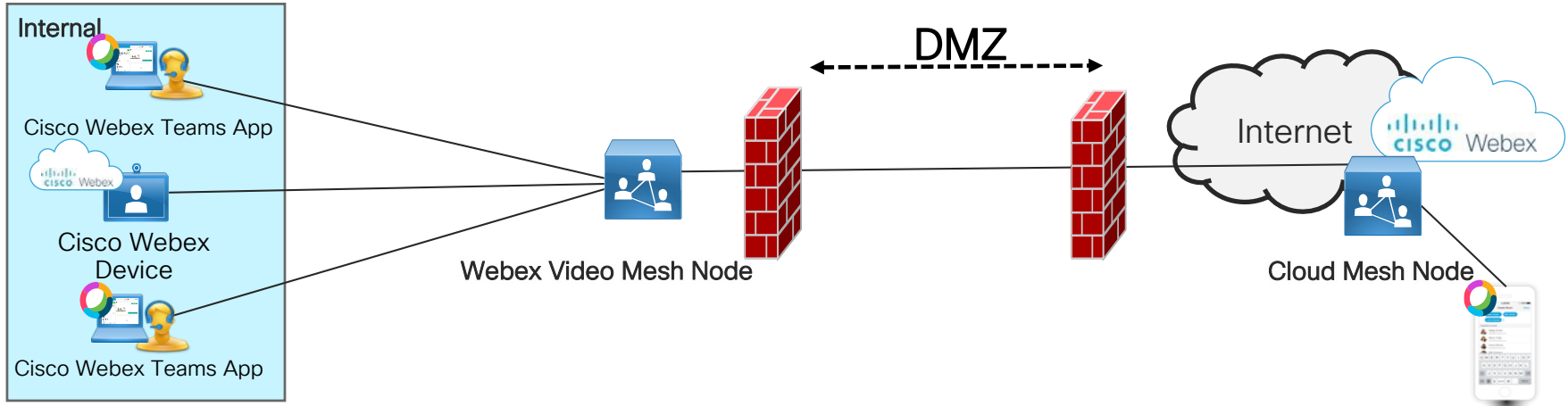
Architecture

Webex Video Mesh



Architecture

Webex Video Mesh – Option 1

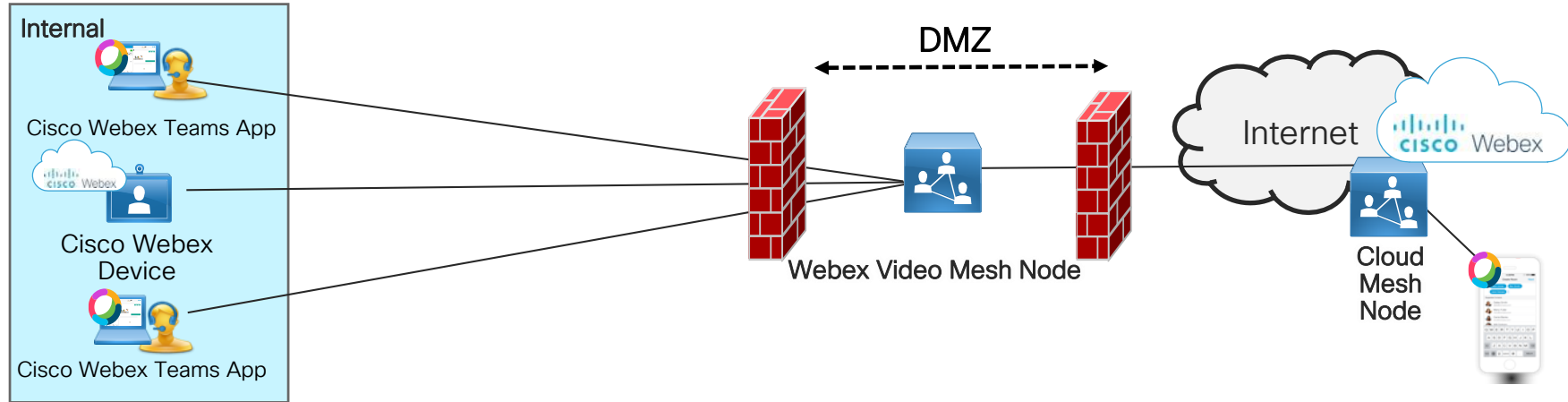


Internal installation considerations:

- All media for internal participants stay internal
- Placed with other collaboration infrastructure devices
- Single connection per conference to Cloud Mesh Nodes

Architecture

Webex Video Mesh – Option 2

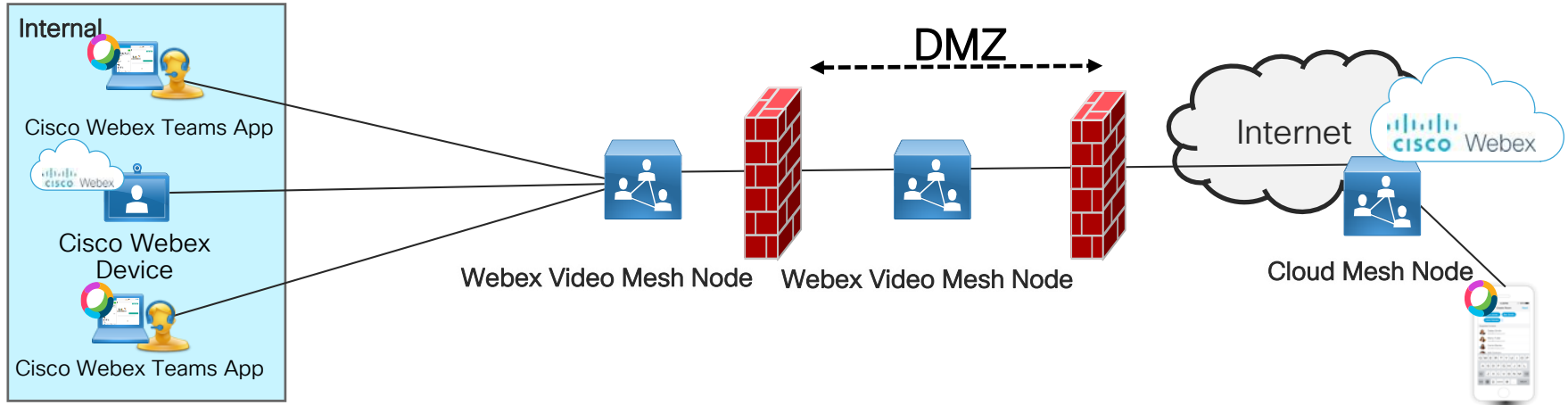


DMZ installation considerations:

- External media does not traverse the internal network.
- All media for internal participants goes to the DMZ.
- Security policy does not allow Cisco Webex network ports to be opened outbound for media directly to the Internet from the internal network.

Architecture

Webex Video Mesh – Not an Option



- Not a firewall-traversal solution
- Different architecture than Expressway C/E pair
- Each Video Mesh Node communicates directly to the cloud
- Can not use Expressway C/E pair for firewall traversal

What devices and scenario can the Video Mesh node be used?

Uses the Node



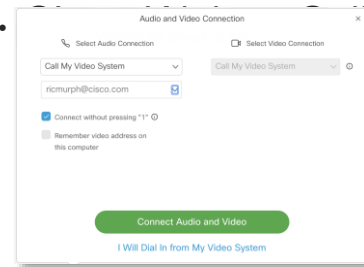
- Any Cisco Webex-registered device
 - SX, MX, DX, Room-series, Webex Board
- Cisco Webex Teams app
 - Desktop and Mobile
- CUCM-registered devices
 - Calling a Cisco Webex scheduled meeting or personal room.
 - SX, MX, DX, Room-series, Jabber, Jabber VDI (12.6 or higher)



Uses the Node



- Cisco VCS/Exp.-registered devices
 - Calling a Cisco Webex scheduled meeting or personal room.
 - SIP or H.323 (requires Interworking)
- Cisco Webex VDI client (39.3 or higher)



My Video System endpoints

What devices and scenario can the video mesh node be used?

✘ Can NOT use the Node

- Webex Teams browser client
 - teams.webex.com



- Webex Calling-registered phones



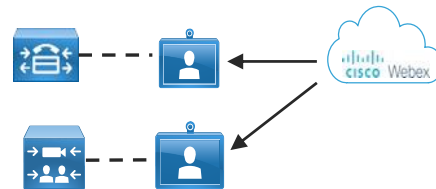
CISCO *Live!*

✘ Can NOT use the Node

- Webex Meetings app

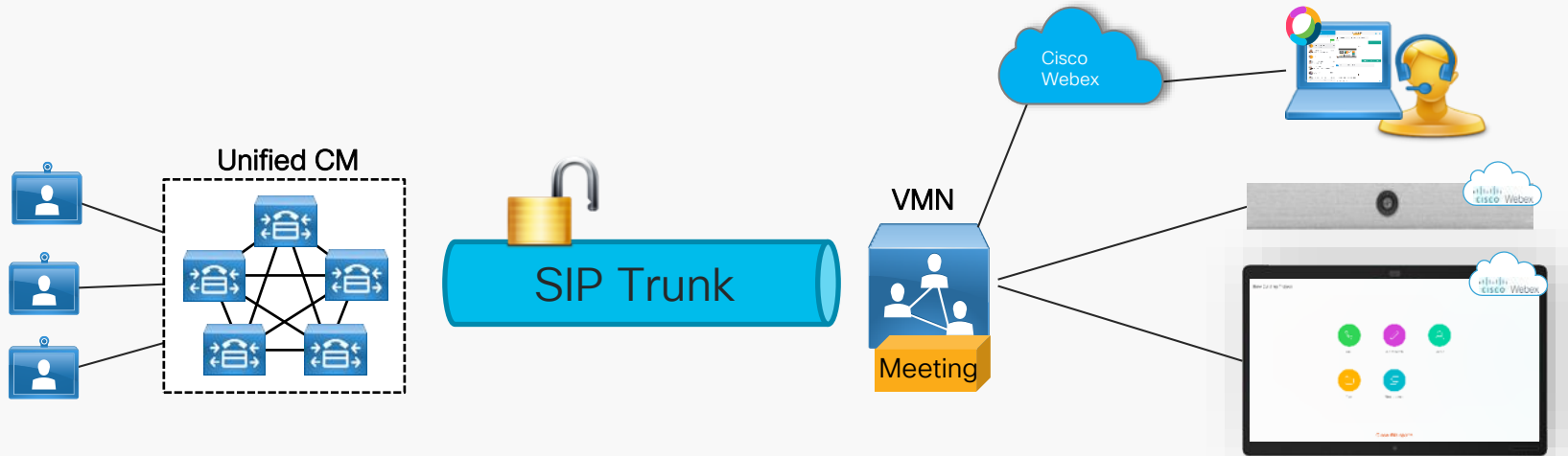


- Cisco Webex Call My Video System to premises-registered endpoints



Call Control Connectivity

Cisco Unified Communications Manager



- Supported with Unified CM version 11.5(1) and higher. Recommended versions 12.5(1) and higher.

Unified CM Configuration

SIP Profile

- Create a SIP Profile for VMN
 - Modify Early Offer Support to
 - “Best Effort (no MTP inserted)”
- Make sure SIP Options Ping is Enabled (default setting)

SIP Profile Information

Name*	Video Mesh SIP Profile
Description	SIP Profile For Video Mesh Node
Default MTP Telephony Event Payload Type*	101
Early Offer for G.Clear Calls*	Disabled
User-Agent and Server header information*	Send Unified CM Version Information as User-Agent
Version in User Agent and Server Header*	Major And Minor
Dial String Interpretation*	Phone number consists of characters 0-9, *, #, and
Confidential Access Level Headers*	Disabled

Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on*	Never
Resource Priority Namespace List	< None >
SIP Rel1XX Options*	Disabled
Video Call Traffic Class*	Immersive
Calling Line Identification Presentation*	Default
Session Refresh Method*	Invite
Early Offer support for voice and video calls*	Best Effort (no MTP inserted)
<input type="checkbox"/> Enable ANAT	

SIP OPTIONS Ping

Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds)* 60

Unified CM Configuration

SIP Trunk Security Profile

- Create a new SIP Trunk Security Profile
- Add appropriate name and description
- Use default settings

SIP Trunk Security Profile Information

Name*	Video Mesh Trunk Security Profile
Description	Video Mesh Trunk Security Profile
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	
Incoming Port*	5060
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

Unified CM Configuration

SIP Trunk

- Create a new SIP Trunk
 - Name the trunk
 - IPv4 or FQDN of VMN
 - Port 5060
 - Add VMN SIP Trunk Security Profile
 - Add VMN SIP Profile
 - Run On All Active Unified CM Nodes
 - Calling and Connecting Party Info Format
 - Deliver URI and DN in connected party, if available.

Next

Status

Status: Ready

Trunk Information

Trunk Type* SIP Trunk

Device Protocol* SIP

Trunk Service Type* None(Default)

Next

Device Information

Product: SIP Trunk

Device Protocol: SIP

Trunk Service Type: None(Default)

Device Name*: Video_Mesh_SIP_Trunk

Description: VMN SIP Trunk

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* videomesh2.ucdemolab.com		5060

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Video Mesh Trunk Security Profile

Rerouting Calling Search Space noExternal

Out-Of-Dialog Refer Calling Search Space noExternal

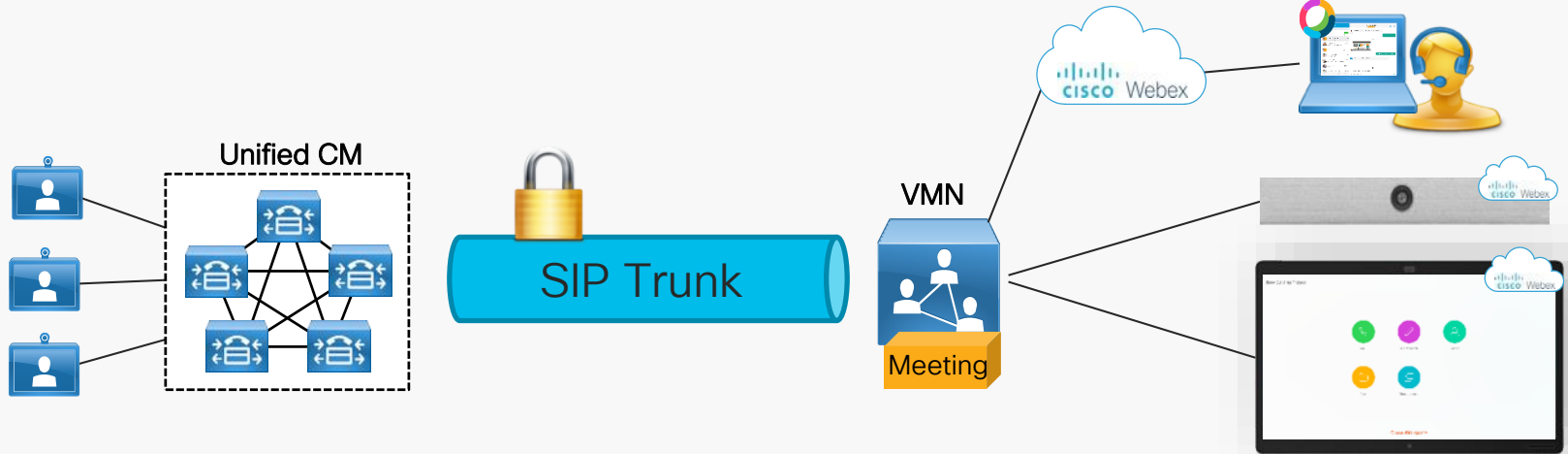
SUBSCRIBE Calling Search Space < None >

SIP Profile* Video Mesh SIP Profile [View Details](#)

DTMF Signaling Method* No Preference

Call Control Connectivity

Unified Communications Manager

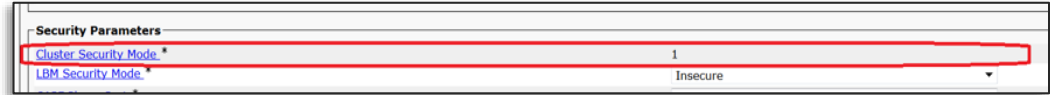


- Previously only supported unencrypted SIP over 5060
- Added support for SIP over TLS using port 5061 on the trunk

Secured Media & Signaling to CUCM

- Secured trunk between CUCM & VMN

- CUCM in Mixed Mode.



- Certificate Management

- CUCM

VMN



- Enabled on the Control Hub at the organization Level

- All VM Nodes must be enabled with secured trunks within organization

- Endpoints must use encrypted connections to the VMN. Endpoints running without encrypted connections to the VMN will overflow to cloud, assuming the environment has a Expressway C/E for Internet connectivity and CUCM has a trunk setup to the Expressway C/E.

SIP over TLS Trunk

Video Mesh -> Settings

Video Quality

Video Quality

Enable 1080P HD video for all participants hosted on on-premises Video Mesh nodes.



Media Encryption

Enable this setting to make encryption mandatory on all media channels that pass through Video Mesh nodes in your organization. Be aware that calls may fail if on-premises devices do not support TLS and SRTP encryption. Once this organization-wide setting is enabled, you must complete the SIP TLS configuration in the Video Mesh cluster settings in Control Hub.



SIP over TLS Trunk

Video Mesh -> Cluster Settings

SIP TLS Configuration

SIP TLS Configuration

⚠ This setting is done at the cluster level and is not available until you enable media encryption for your entire organization under the Video Mesh settings.

Trusted SIP sources

Enter a comma-separated list of Unified CM IP addresses or FQDNs. These entries are identified as trusted SIP sources and are allowed to send secure SIP calls to Webex Video Mesh.

cucm-k9-pub.ucdemolab.com x cucm-k9-sub1.ucdemolab.com x

Enter the trusted SIP sources...

CUCM pub and subs

SIP over TLS – SIP Profile

- Set “Early Offer support for voice and video calls” to Best Effort (no MTP inserted)
- “Enable OPTIONS Ping to monitor destination status for Trunks with Service Type” is checked.

The screenshot displays the configuration interface for a SIP Profile, divided into three main sections:

- Trunk Specific Configuration:** This section contains several dropdown menus and checkboxes. The 'Early Offer support for voice and video calls*' dropdown is highlighted with a red box and set to 'Best Effort (no MTP inserted)'. Other dropdowns include 'Reroute Incoming Request to new Trunk based on *' (Never), 'Resource Priority Namespace List' (< None >), 'SIP Rel1XX Options*' (Disabled), 'Video Call Traffic Class*' (Immersive), and 'Calling Line Identification Presentation*' (Default). The 'Session Refresh Method*' dropdown is also highlighted with a red box and set to 'Invite'. Checkboxes for 'Enable ANAT', 'Deliver Conference Bridge Identifier', 'Allow Passthrough of Configured Line Device Caller Information', 'Reject Anonymous Incoming Calls', 'Reject Anonymous Outgoing Calls', 'Send ILS Learned Destination Route String', and 'Connect Inbound Call before Playing Queuing Announcement' are all unchecked.
- SIP OPTIONS Ping:** This section is highlighted with a red box. The checkbox 'Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"' is checked. Below this are four input fields: 'Ping Interval for In-service and Partially In-service Trunks (seconds)*' (60), 'Ping Interval for Out-of-service Trunks (seconds)*' (120), 'Ping Retry Timer (milliseconds)*' (500), and 'Ping Retry Count*' (6).
- SDP Information:** This section contains four checkboxes: 'Send send-receive SDP in mid-call INVITE' (unchecked), 'Allow Presentation Sharing using BFCP' (checked), 'Allow iX Application Media' (checked), and 'Allow multiple codecs in answer SDP' (checked).

A 'Save' button is located at the bottom left of the configuration area.

SIP over TLS – Trunk Security Profile

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

SIP Trunk Security Profile Configuration

Save

Status
Status: Ready

SIP Trunk Security Profile Information

Name*	VideoMesh_Encrypted
Description	secure trunk to VMN
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	videomesh2.ucdemolab.com
Incoming Port*	5061

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

SIP V.150 Outbound SDP Offer Filtering* Use Default Filter

Save

- Device Security mode: Encrypted
- Incoming and outgoing: TLS
- X.509 Subject Name
- SIP V.150 Outbound SDP Offer Filtering: Use Default Filter

SIP over TLS – Trunk Config

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Trunk Configuration

Save

Status
Status: Ready

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	sipT_VideoMeshNode
Description	encrypted trunk to VideoMeshNode
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	None
Packet Capture Duration	0

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 SRTP Allowed – When this flag is checked, Encrypted TLS needs to be configured in the network to provide end-to-end security. Failure to do so will expose keys and other information.

Consider Traffic on This Trunk Secure* When using both sRTP and TLS

Route Class Signaling Enabled Default

Use Trusted Relay Point* Default

PSTN Access

Run On All Active Unified CM Nodes

- Enable sRTP Allowed
- Run On All Active Unified CM Nodes

SIP TLS – Trunk Config

- Calling and Connecting Party Info Format
 - Deliver URI and DN in connected party, if available.
- Destination Address
- Destination Port – 5061
- Video Mesh Trunk Security Profile
- Video Mesh SIP Profile

Trunk Configuration

Save

Outbound Calls

Called Party Transformation CSS: < None >

Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS: < None >

Use Device Pool Calling Party Transformation CSS

Calling Party Selection*: Originator

Calling Line ID Presentation*: Default

Calling Name Presentation*: Default

Calling and Connected Party Info Format*: Deliver URI and DN in connected party, if available

Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS: < None >

Use Device Pool Redirecting Party Transformation CSS

Caller Information

Caller ID DN: []

Caller Name: []

Maintain Original Caller ID DN and Caller Name in Identity Headers

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1 * videomesh2.ucdemolab.com		5061

MTP Preferred Originating Codec*: 711ulaw

BLF Presence Group*: Standard Presence group

SIP Trunk Security Profile*: VideoMesh_Encrypted

Rerouting Calling Search Space: < None >

Out-Of-Dialog Refer Calling Search Space: < None >

SUBSCRIBE Calling Search Space: < None >

SIP Profile*: Video Mesh SIP Profile [View Details](#)

DTMF Signaling Method*: No Preference

Normalization Script

Normalization Script: < None >

Enable Trace

Parameter Name	Parameter Value
1	[]

Recording Information

None

This trunk connects to a recording-enabled gateway

This trunk connects to other clusters with recording-enabled gateways

Unified CM Configuration

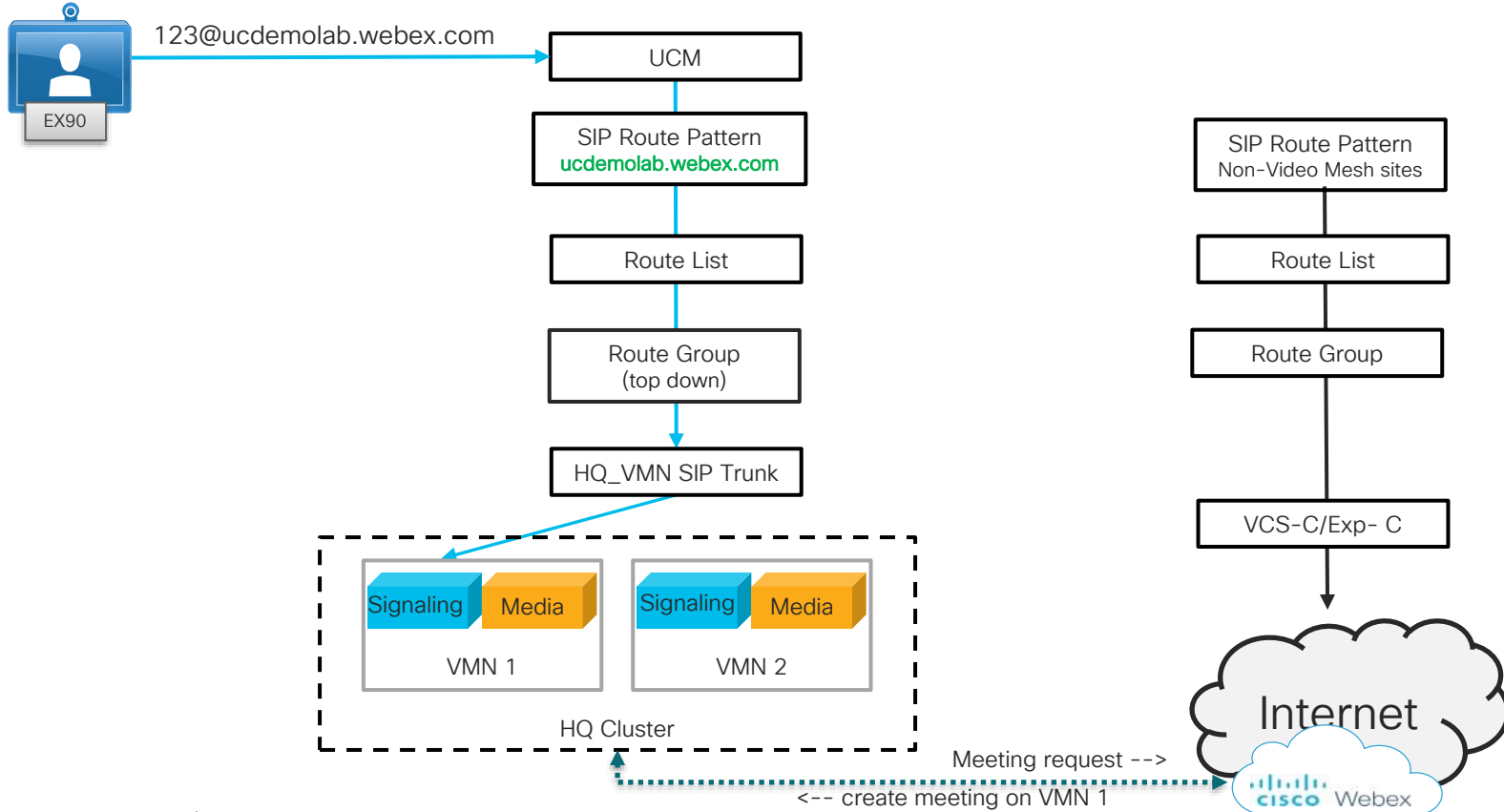
SIP Route Pattern

- SIP route pattern for customer Webex domain
 - sitename.webex.com

The screenshot shows the 'SIP Route Pattern Configuration' page. At the top, there are action buttons: 'Save', 'Delete', 'Copy', and 'Add New'. Below this is the 'Status' section, which shows an information icon and the text 'Status: Ready'. The 'Pattern Definition' section contains several fields: 'Pattern Usage' is set to 'Domain Routing'; 'IPv4 Pattern*' is 'ucdemolab.webex.com' (highlighted with a red box); 'IPv6 Pattern' is empty; 'Description' is 'TME webex site'; 'Route Partition' is 'B2B'; and 'SIP Trunk/Route List*' is 'Hybrid_Media_Nodes_Plus_VCS'. There is also an unchecked checkbox for 'Block Pattern'.

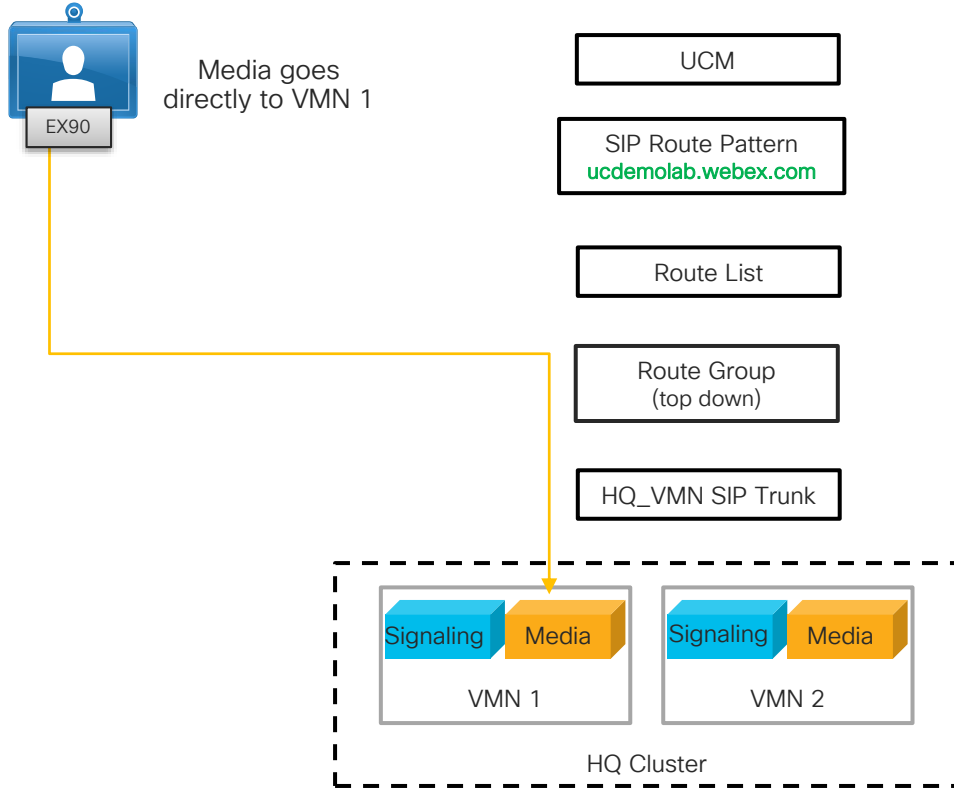
SIP Dial-in Flow to VMN

Ucdemolab = Webex sitename



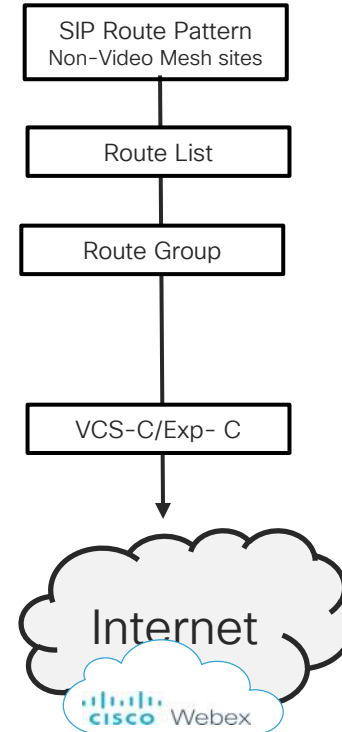
SIP Dial-in Flow to VMN

Ucdemolab = Webex sitename



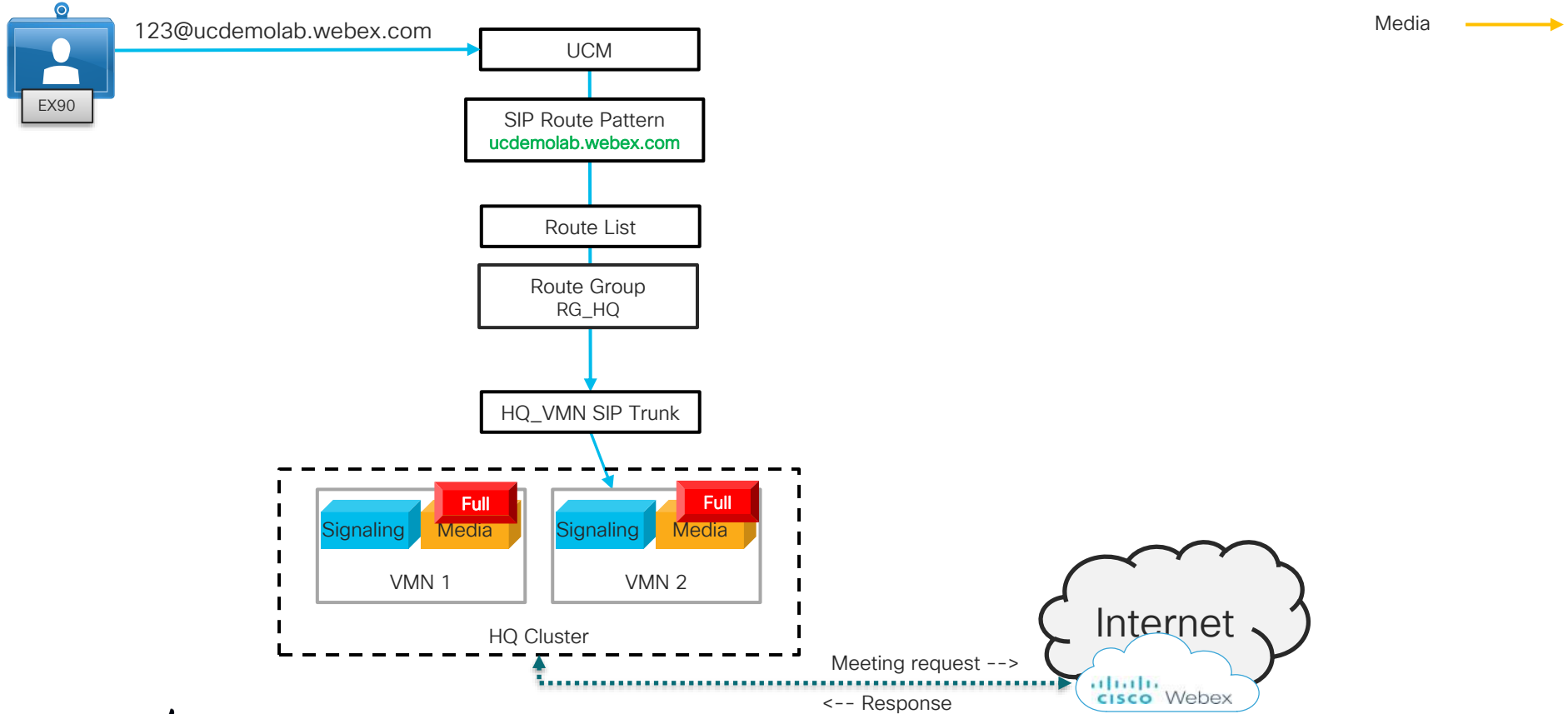
Signaling →

Media →



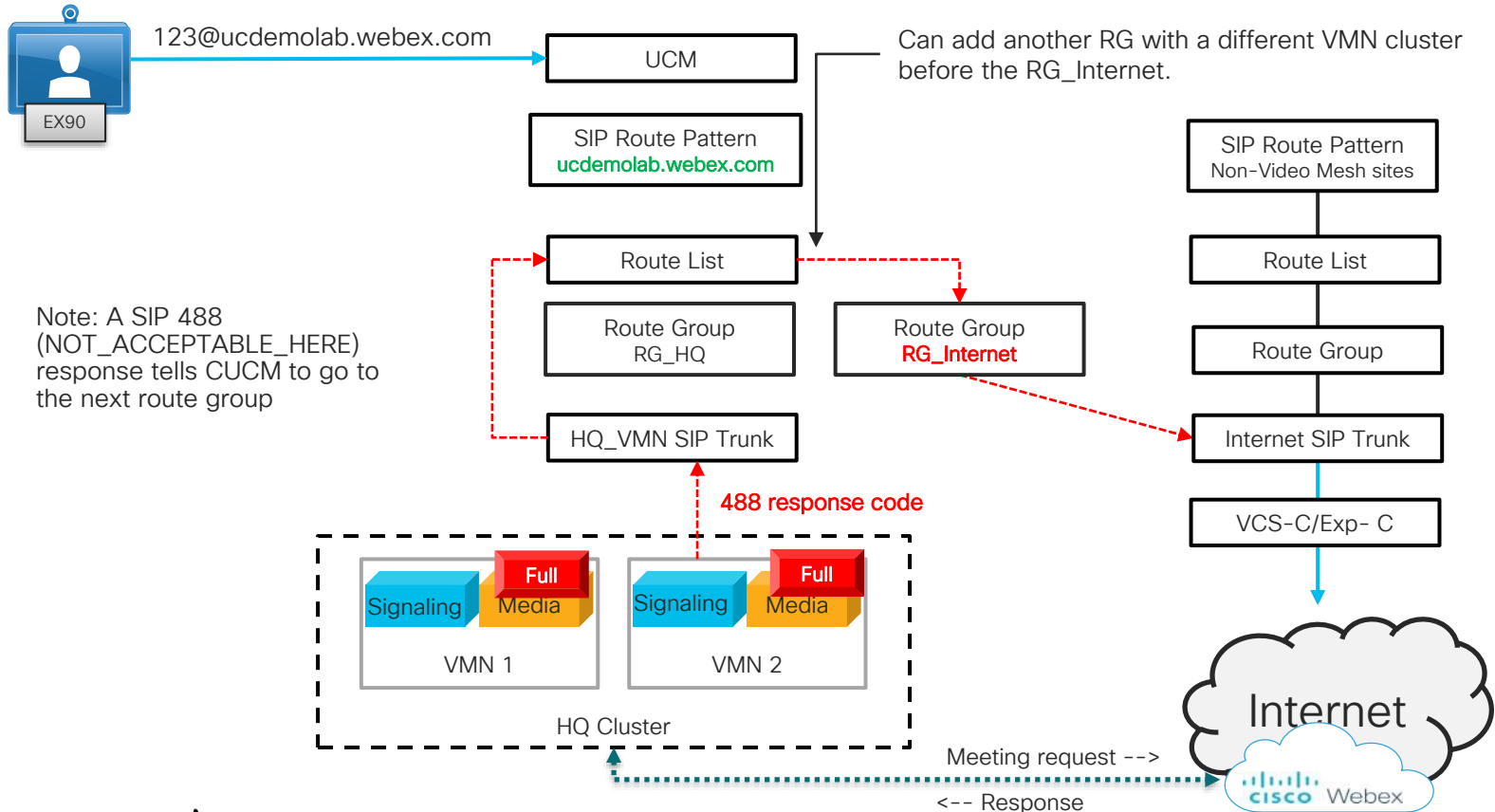
SIP Dial-in Flow to VMN

Ucdemolab = Webex sitename



SIP Dial-in Flow to VMN

ucdemolab = Webex sitename

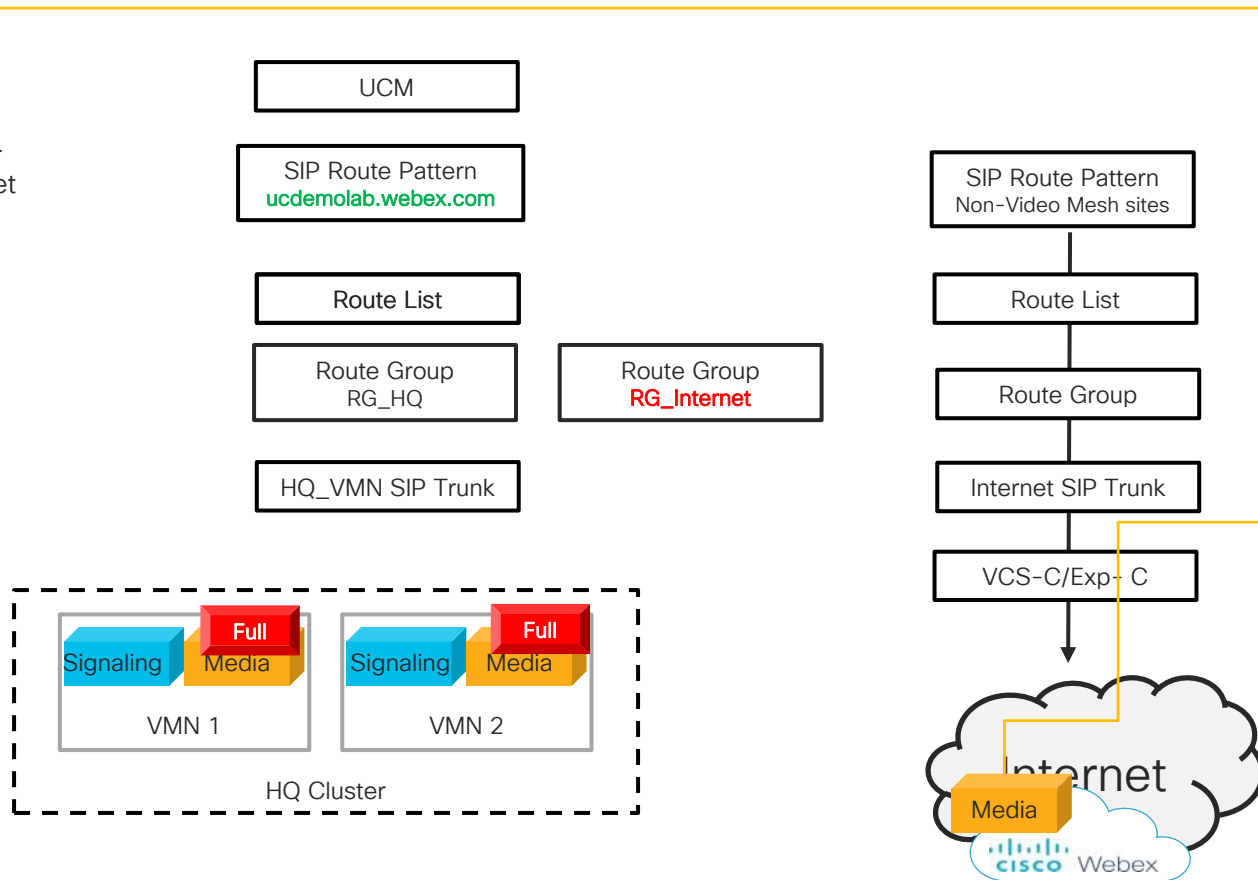


SIP Dial-in Flow to VMN

Ucdemolab = Webex sitename



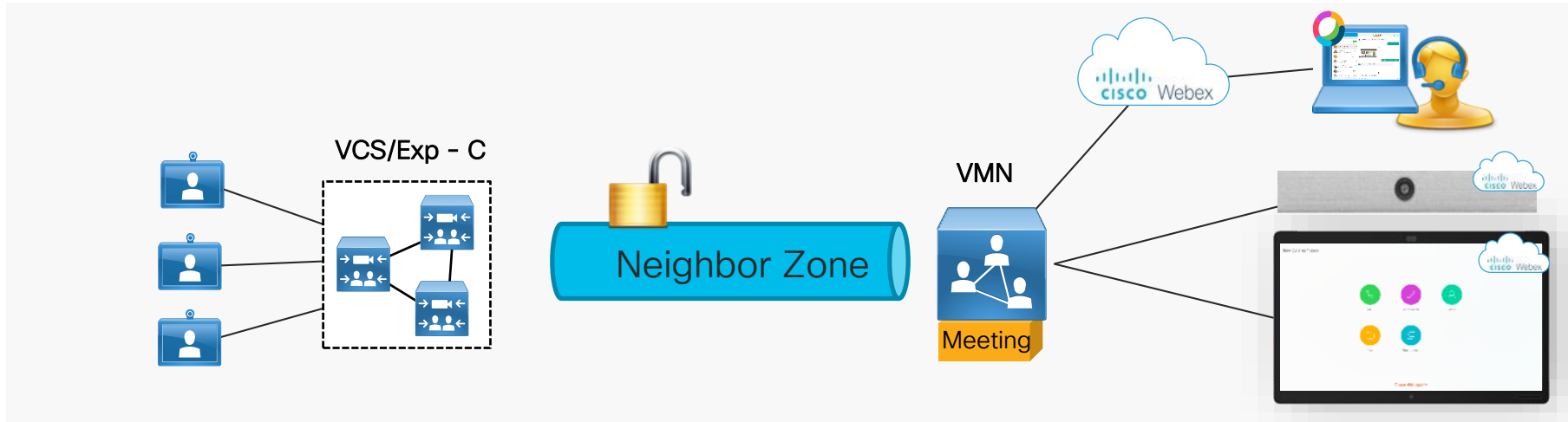
Media goes out VCS or Exp C/E pair to the Internet Mesh nodes



Call Control Connectivity

VCS/EXP - C

VMN = Webex Video Mesh Node



- Supported with VCS or Expressway X8.11.4 or higher

Expressway - C

Neighbor Zone Creation

- Create a neighbor zone for Webex Video Mesh Node
- Configuration > Zones > Zones, and then click New
- 5060 support only

The screenshot displays the Cisco Expressway-C configuration interface. The top navigation bar includes 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The main content area is titled 'Edit zone' and is divided into three sections: 'Configuration', 'H.323', and 'SIP'. In the 'Configuration' section, the 'Name' field is set to 'VideoMeshZone' and is highlighted with a red box. The 'Hop count' is set to '15'. In the 'SIP' section, the 'Port' field is set to '5060' and is also highlighted with a red box. Other SIP settings include 'Mode' (On), 'Transport' (TCP), 'Accept proxied registrations' (Deny), 'Media encryption mode' (Auto), 'ICE support' (On), 'Multistream mode' (On), 'Preloaded SIP routes support' (Off), and 'AES GCM support' (Off). A link for 'Configure TURN servers' is visible next to the ICE support setting.

Expressway - C

Neighbor Zone Creation

- Create a neighbor zone for Webex Video Mesh Node
 - Configuration > Zones > Zones, and then click New
- Add Webex Video Mesh Nodes

CISCO Cisco Expressway-C

Status System **Configuration** Applications Users Maintenance

Edit zone

Configuration

Name * VideoMeshZone ⓘ

Type Neighbor

Hop count * 15 ⓘ

Location

Look up peers by Address ⓘ

Peer 1 address 10.99.255.21 ⓘ SIP Reachable: 10.99.255.21:5060

Peer 2 address 10.99.255.22 ⓘ SIP Reachable: 10.99.255.22:5060

Peer 3 address ⓘ ⓘ

Peer 4 address ⓘ ⓘ

Peer 5 address ⓘ ⓘ

Peer 6 address ⓘ ⓘ

Advanced

Zone profile Default ⓘ

Expressway - C

Search Rule

- Create a search rule for Webex Video Mesh Node calls
 - Configuration > Dial Plan > Search Rules, and then click New
 - SIP only
 - Alias Pattern Match
 - your Webex site
 - Sitename is “ucdemolab”
 - ex: .*@ucdemolab.webex.com.*

The screenshot shows the Cisco Expressway-C configuration interface for editing a search rule. The interface is titled "Cisco Expressway-C" and has a navigation bar with tabs for Status, System, Configuration, Applications, Users, and Maintenance. The "Configuration" tab is selected, and the "Edit search rule" page is displayed. The rule name is "Outbound To VMN for Webex Meetings" and the description is "allows locally registered Expressway endpoints to reach HMN". The rule is configured with a priority of 31, protocol of SIP, and SIP variant of All SIP Variants. The source is set to "Named" and the source name is "Default Subzone". The request must be authenticated, and the mode is "Alias pattern match". The pattern type is "Regex" and the pattern string is ".*@ucdemolab.webex.com.*". The pattern behavior is "Leave" and the action on successful match is "Continue". The target is "VideoMeshZone" and the state is "Enabled". Red arrows point to the "Source name", "Mode", "Pattern string", and "Target" fields. Red boxes highlight the rule name, description, and pattern string.

Expressway - C

Zones

Name	Type	Calls	Bandwidth used	H323 status	SIP status	Search rule status
DefaultZone	Default zone	0	0 kbps	On	On	
<input type="checkbox"/> BasicSipTraversal	Traversal client	0	0 kbps	Off	Active	Enabled search rules: 3
<input type="checkbox"/> CUCM_Core	Neighbor	0	0 kbps	Off	Active	Enabled search rules: 2
<input type="checkbox"/> VideoMeshZone	Neighbor	0	0 kbps	Off	Active	Enabled search rules: 1

New Neighbor Zone created with search rule

Default Traversal Zone between Exp - C and Exp - E

- Used for failover when Webex Video Mesh Nodes are full
- Normally already setup in existing deployments

Enable Video Mesh support on Cisco Webex site

To cascade media to and from the VMN for Webex meetings, a configuration item needs to be modified from the default setting.

This configuration is available when the Webex site is on the new platform running WBS 33 and higher.

Media Resource Type

- Cloud (default)
- Video Mesh



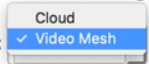
Common Settings

Cisco Webex Meetings Sites > Configure ucdemolab.webex.com > Common Settings

Cloud Collaboration Meeting Room Options

Interactive Voice Response URI: meet@ucdemolab.webex.com

Media Resource Type:

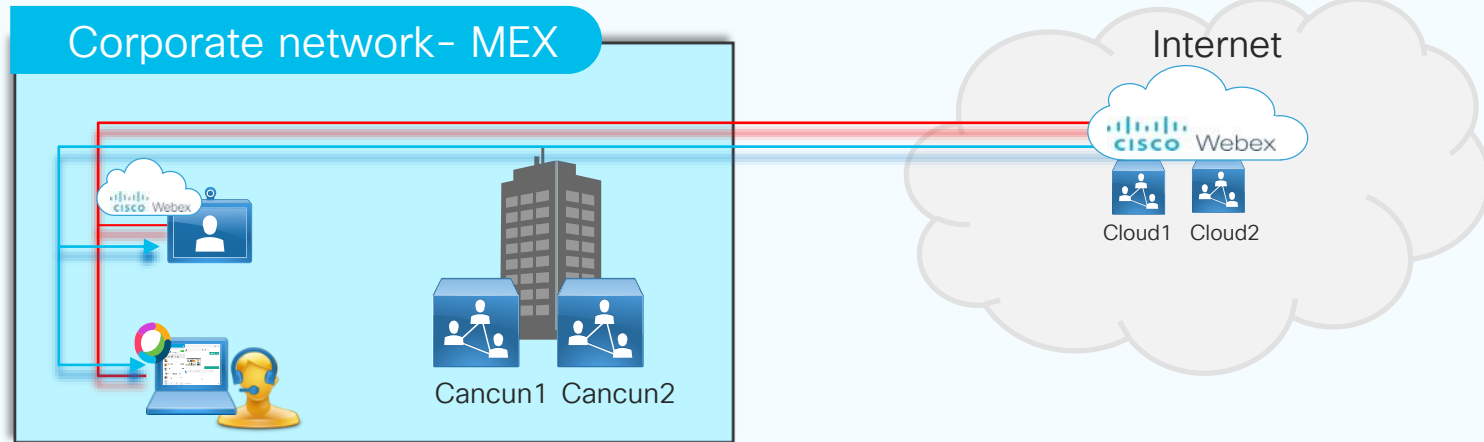


Before you choose Cisco Webex Video Mesh, you must also install on-premises media nodes from <https://admin.webex.com> and complete the related configuration. See the [documentation](#) for details.

Webex Video Mesh Node Discovery - Scenario 1

Scenario 1

Registration



Cisco Webex Teams app and Webex device register to their organization

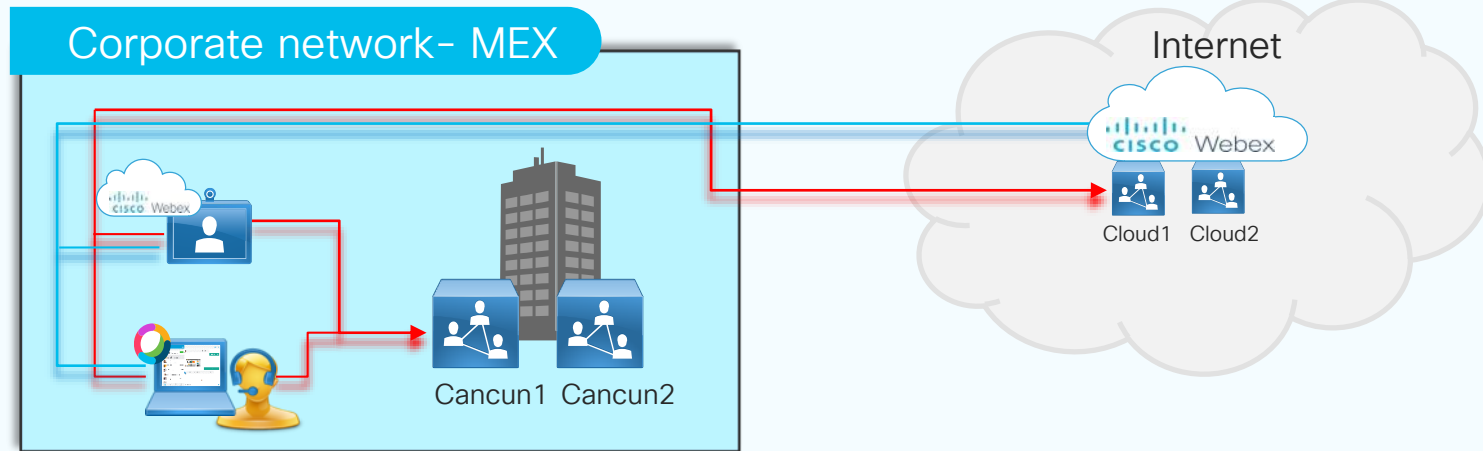
Cisco Webex responds with the clusters available for the users

Cluster - Cancun	Cluster - Cloud
1. Node - Cancun1	1. Node - Cloud1
2. Node - Cancun2	2. Node - Cloud2

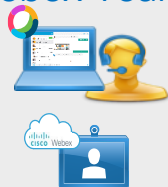
Scenario 1

Reachability Test

- Note:** Checks are performed:
- At launch of Cisco Webex Teams app
 - Network change event
 - Cache expiration (2 hours)



Cisco Webex Teams app and Webex devices do reachability tests to the mesh nodes.
Cisco Webex Teams app and Webex devices sends results to the cloud at call start.



Cluster - Cancun

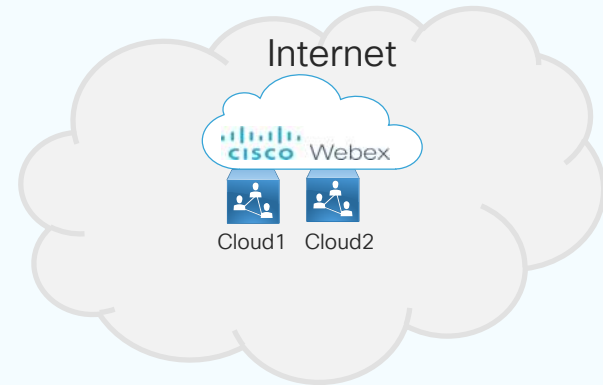
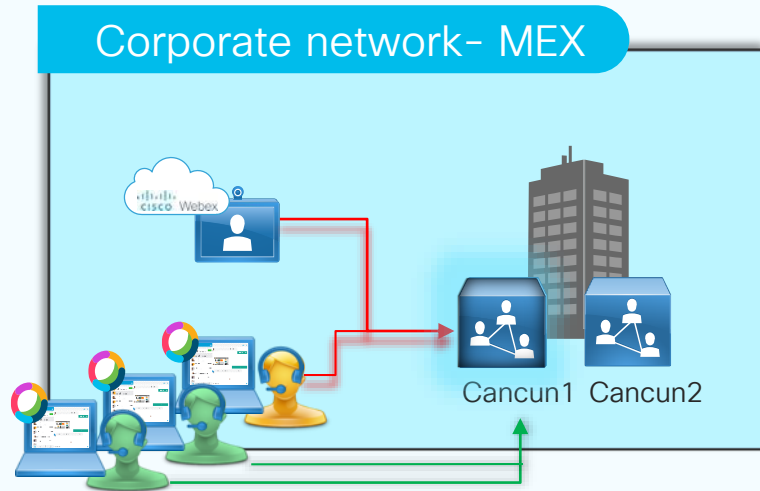
1. Node - Cancun1 (RTD = 10)
2. Node - Cancun2 (RTD = 11)

Cluster - Cloud

1. Node - Cloud1 (RTD = 220)
2. Node - Cloud2 (RTD = 200)

Scenario 1

Registration



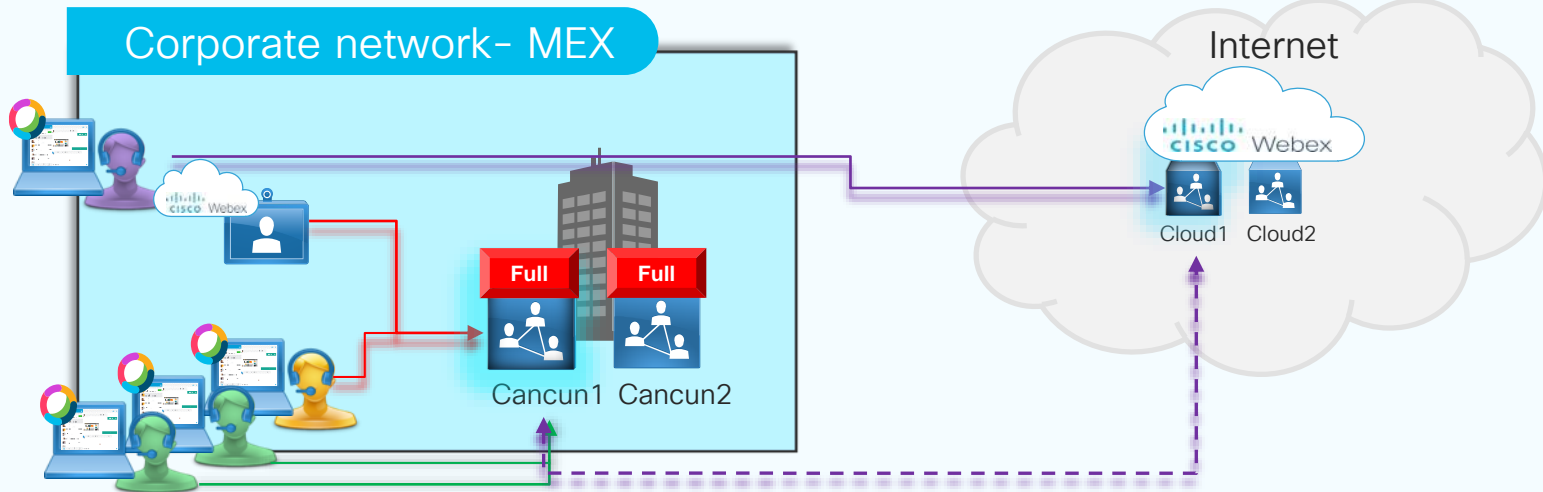
Cisco Webex Teams app and Webex devices connect to a mesh node

Mesh node Cancun1 hosts the meeting

If additional participants join later, they follow the same process

Scenario 1

Meeting with Overflow



Cisco Webex Teams app and Webex devices connect to a mesh node

Mesh node Cancun1 hosts the meeting

If additional participants join later, they follow the same process

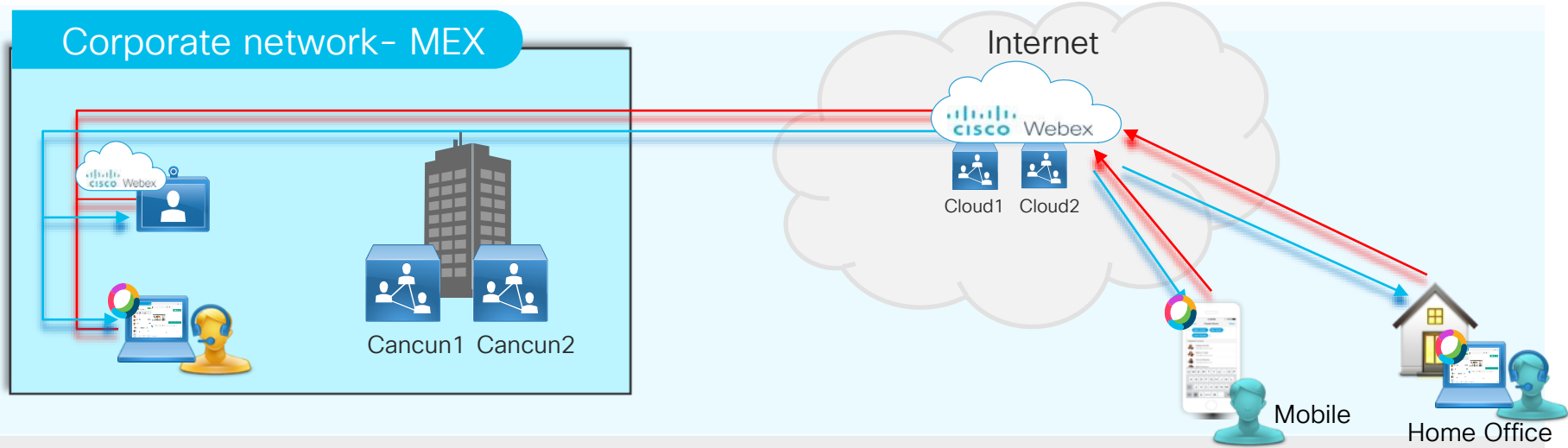
Cancun 1 and Cancun 2 are full

Overflow to the cloud and automatic cascade is created

Webex Video Mesh Node Discovery - Scenario 2

Scenario 2

Registration



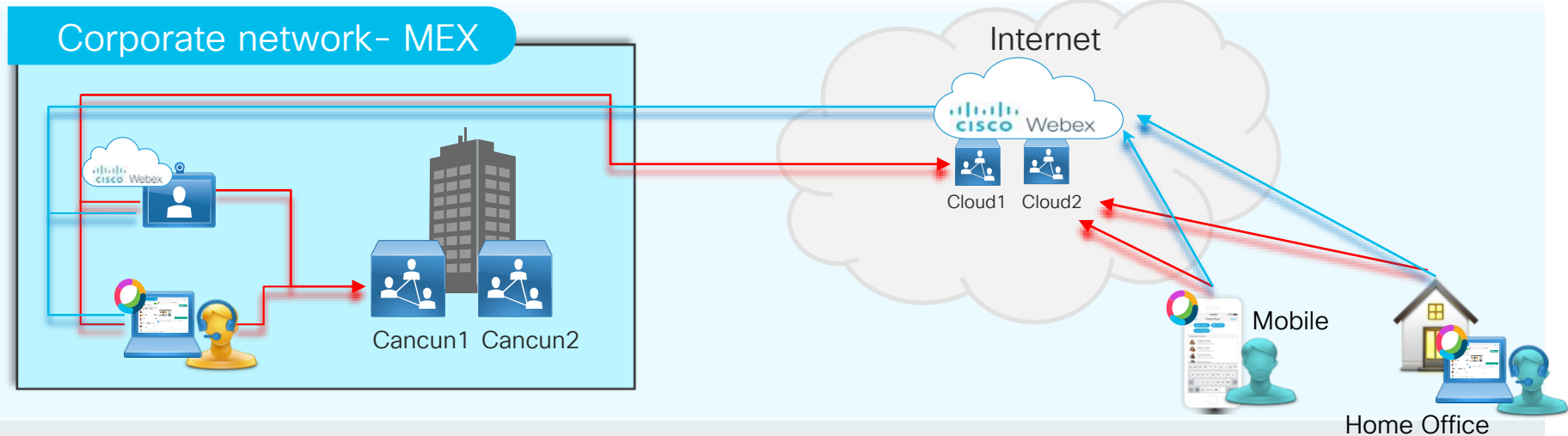
Cisco Webex Teams app and Webex device register to their organization

Cisco Webex responds with the clusters available for the users

Cluster - Cancun	Cluster - Cloud
1. Node - Cancun1	1. Node - Cloud1
2. Node - Cancun2	2. Node - Cloud2

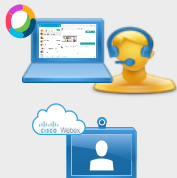
Scenario 2

Reachability Test



Cisco Webex Teams app and Webex devices do reachability tests to the mesh nodes.

Cisco Webex Teams app and Webex devices sends results to the cloud at call start.



Cluster - Cancun

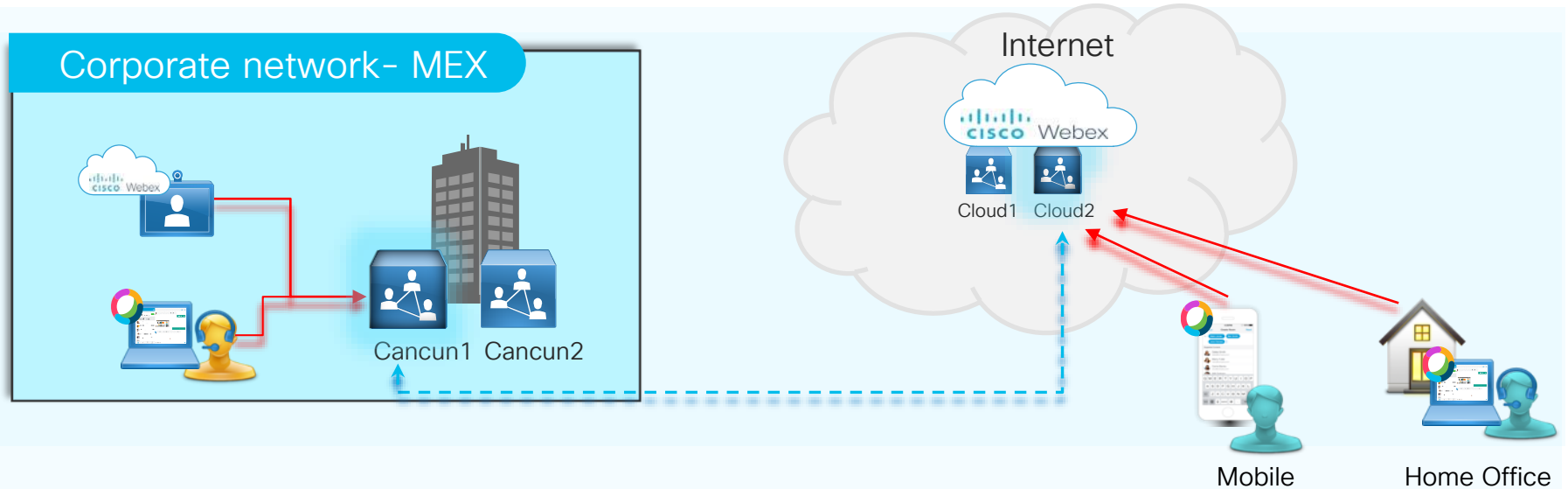
1. Node - Cancun1 (RTD = 10)
2. Node - Cancun2 (RTD = 11)

Cluster - Cloud

1. Node - Cloud1 (RTD = 220)
2. Node - Cloud2 (RTD = 200)

Scenario 2

Meeting



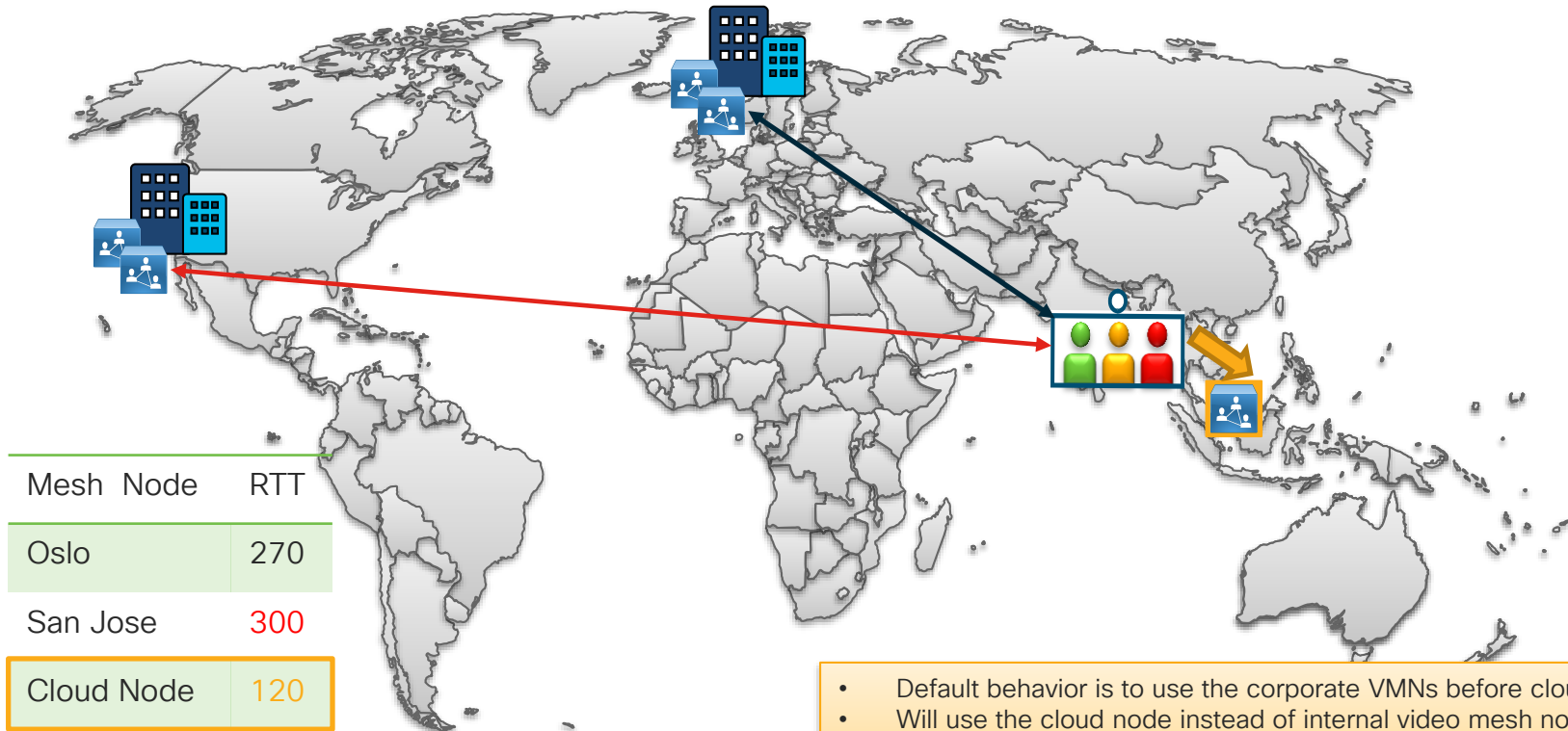
Cisco Webex Teams app and Webex devices connect to a mesh node

Mesh node Cancun1 hosts a meeting for the corporate users

Mesh node Cloud 2 hosts a meeting for remote users

Mesh node Cancun1 cascades automatically to Mesh node Cloud2 to create the meeting for all participants

Reachability to the cloud

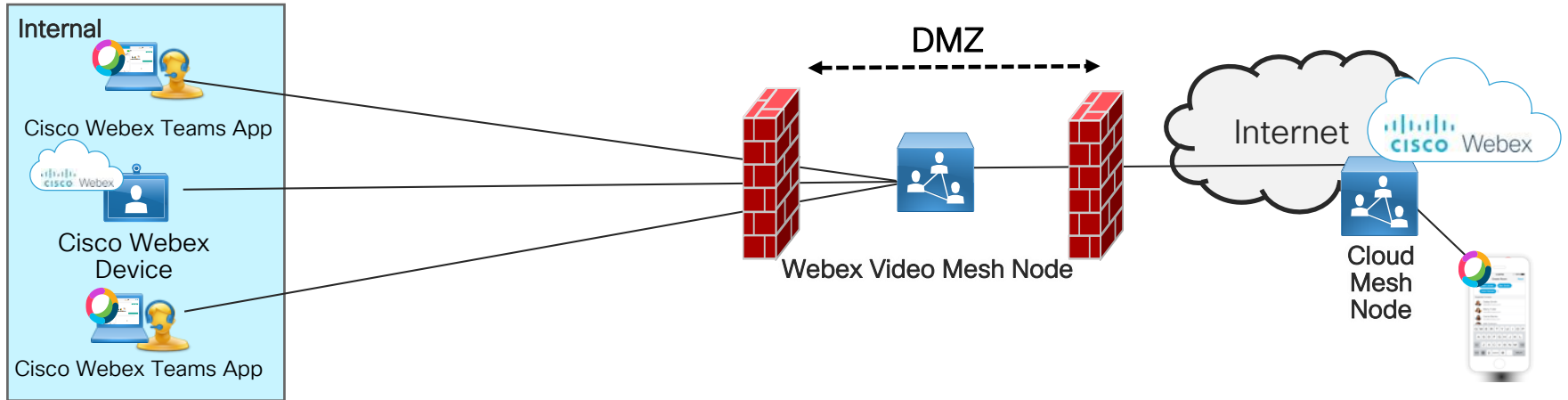


- Default behavior is to use the corporate VMNs before cloud nodes.
- Will use the cloud node instead of internal video mesh nodes if the RTT ≥ 250 ms to the video mesh node and cloud node's RTT is 20% less (200ms or less) than the internal VMN clusters.

DMZ Deployment

Architecture

Webex Video Mesh – Option 2



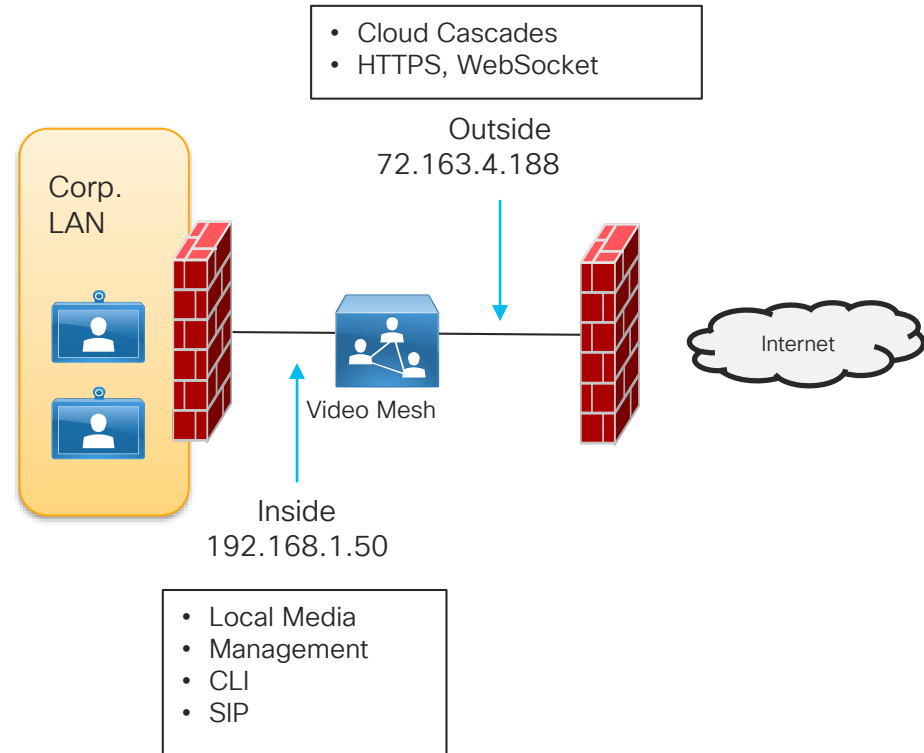
DMZ installation considerations:

- External media does not traverse the internal network
- All media for internal participants goes to the DMZ.
- Security policy does not allow all Cisco Webex ports to be opened outbound for media directly to the Internet from the internal network

Dual Nic

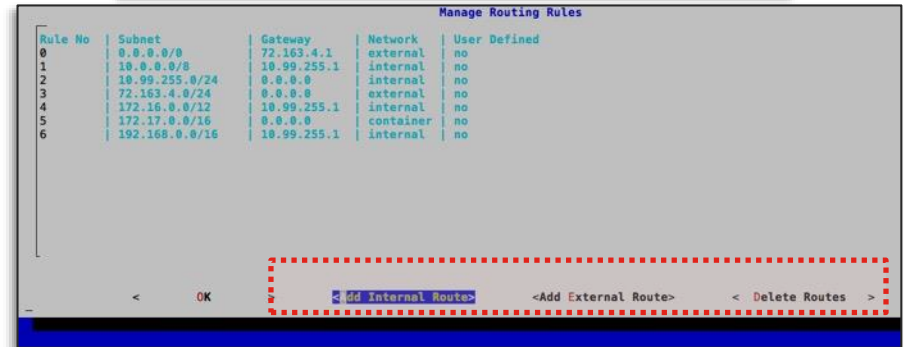
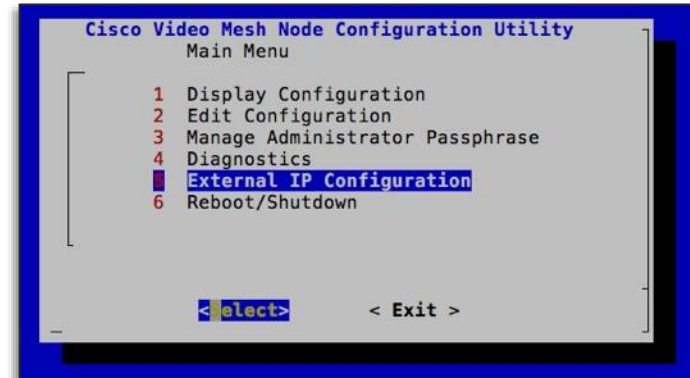
Deployment:

- Require all nodes be the same configuration in the cluster
- For example dual-NIC only
- Recommend changes be done in maintenance mode
- RFC 1918 address is acceptable on the internal interface. The external interface needs to be a publicly routable address.
- Use internal IP address for node registration in Control Hub.
- The browser used for registration of VMN must have connectivity to Cisco Webex cloud as well as the internal IP address of the node.

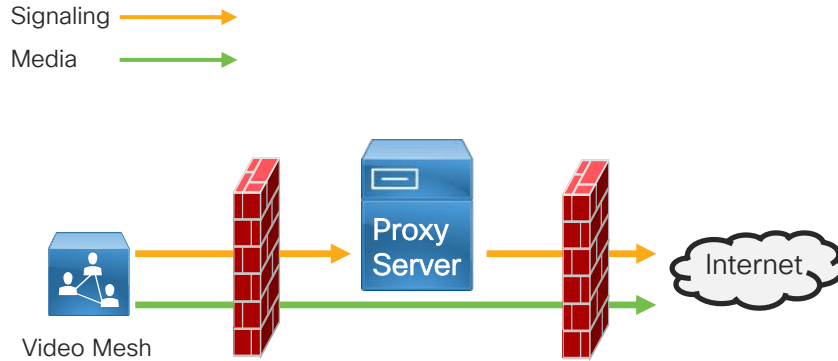


Dual NIC – External IP Configuration

- External IP configuration needs to be explicitly enabled when required.
- External IP can be enabled before or after registration.
- Maintenance Mode is required if registered to production environment.
- All nodes in the cluster need to have the same configuration, either single or dual NIC.
- Menu Options
 - **Enable/Disable** – Configure external IP or switch back to Single interface mode
 - **Display Configuration** – Display the external IP configuration
 - **Manage Routing Rules** – View, Add and Delete the routing rules.



Proxy Support



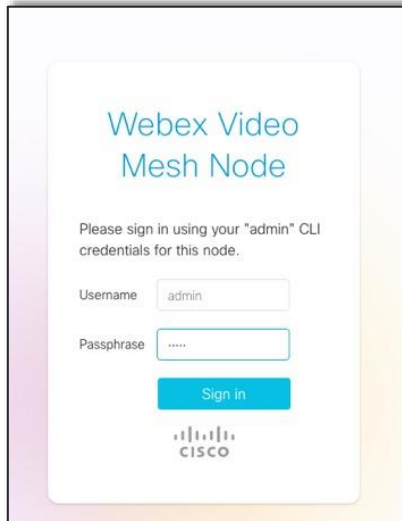
- HTTP(s) signaling support only
 - Ports 443 and 444
- Media goes direct to the cloud
 - UDP port 5004

- Transparent Proxy
 - Inspecting and non inspecting
- Explicit Proxy
 - Inspecting and non inspecting
 - No auth, Basic, Digest and NTLM

Video Mesh Webpage

This webpage is available per node

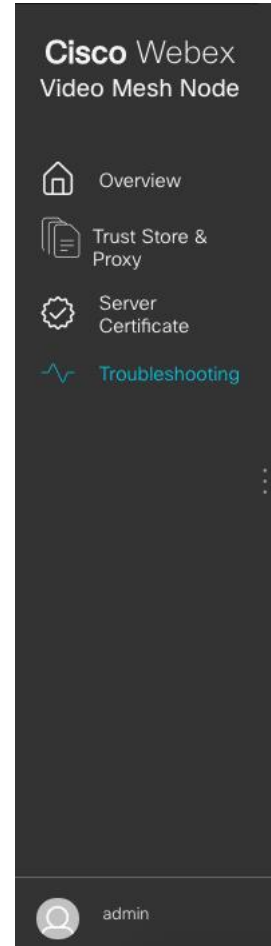
- https://ip_address_of_the_vmn/setup
 - User: admin
 - Password: Use the one that was created when the node was setup via the CLI.



CISCO *Live!*

What can you view?

1. Video Mesh Overview
2. Trust Store
3. Certificate management
4. Troubleshooting



Overview

Number of ongoing calls

Node Type, SW Image

Usage and Service Status

Node specific Alarm Notification

Cisco Webex
Video Mesh Node

Overview

Trust Store & Proxy

Server Certificate

Troubleshooting

Overview

Call Status

0

calls

Node Details

Type	Video Mesh Node
Image	Production
Deployment Type	Cms1000
Release Channel	Beta
Provisioning	Cloud
Version	2019.07.12.1917m.1
OS Version	2135.5.0
QoS	On
Maintenance Mode	Off

Node Health

CPU	70 cores, 0.33% used
Memory	3.66GB of 58.96GB used (6.2%)
Disk Space	13.43GB of 251.56GB used (6%)
Management Service	Active
Messaging Service	Active
NTP Sync	Active

Notifications

Hostname configuration of the Video Mesh Node is invalid.

The Video Mesh node's hostname settings are invalid and these alerts were generated on the node: Unable to resolve FQDN videomesh1.ucdemolab.com's IP address against the current DNS settings. These issues may cause sharing problems for users in Webex meetings. Please check the hostname and domain settings.

Last Reported: Wed Jul 24 2019 13:08:33 GMT-0400 (Eastern Daylight Time)

Experienced problem connecting to Cisco Webex Cloud services

Experienced problem connecting to Cisco Webex Cloud services.

Last Reported: Tue Jul 16 2019 00:44:22 GMT-0400 (Eastern Daylight Time)

Network Settings

Hostname	videomesh1.ucdemolab.com
Interface	00:50:56:88:bb:73
IP	10.99.255.21/24
Gateway	10.99.255.1
DNS	10.99.101.12, 10.99.102.11
NTP	ntp.ucdemolab.com, 10.99.101.12, 10.99.102.11
Dual IP	Disabled

Registration Details

Registered	Yes
Organization	UC Demo Lab
Org ID	35a15b0a-0ef1-4029-9f63-a7c54df5df59
Cluster	Boxborough - Full
Cluster ID	b7c30185-99cc-4ba7-b5b5-77adb1871dd8

Cloud Connectivity

Webex Cloud Resolution Test	Pass
3rd Party Resolution Test	Pass
Webex Cloud Connectivity Test	Pass
3rd Party Connectivity Test	Pass
Webex Cloud Bandwidth Test	Testing
3rd Party Bandwidth Test	Pass

Network Information

Node Registration Status

DNS Test, Server Response time, BW test

Hover to reveal when the test was run and what was checked

cisco *Live!*

Transparent Proxy

Supported Types of Proxies

1. No Proxy
2. Non-Inspecting
 - Video Mesh nodes are not configured to use a specific proxy server address and should not require any changes to work with a non-inspecting proxy.
3. Inspecting
 - Requires certificate upload to VMN
 - 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 types of content that are not permitted. This type of proxy decrypts all your traffic, even https.
 - Reboot is required after the certificate is install.
 - Proxy connectivity check

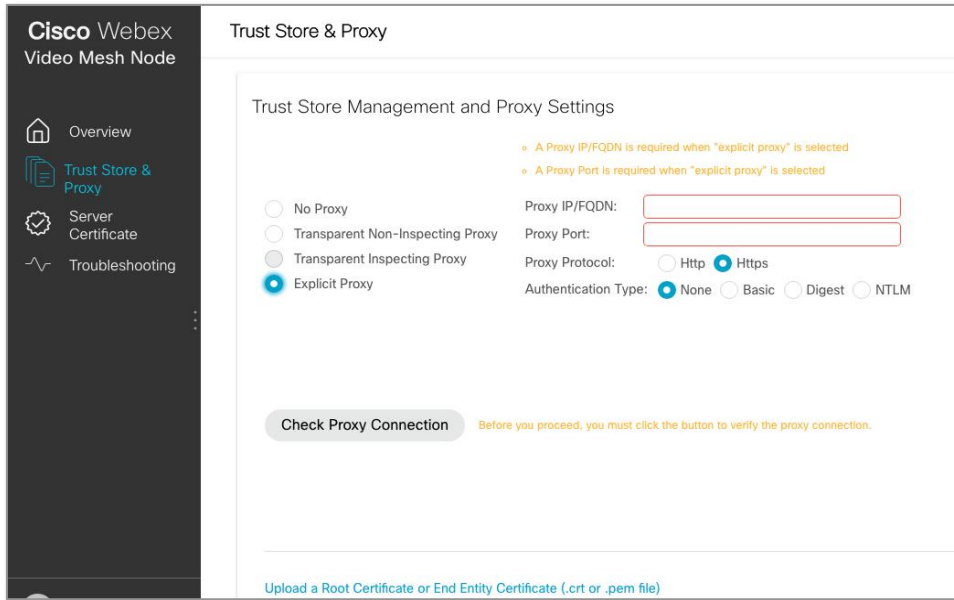
The image displays three screenshots of the Cisco Webex Video Mesh Node configuration interface, specifically the 'Trust Store & Proxy' section. Each screenshot shows a sidebar with navigation options: Overview, Trust Store & Proxy (highlighted), Server Certificate, and Troubleshooting. The main content area is titled 'Trust Store Management and Proxy Settings'.

Top Screenshot: Shows 'No Proxy' selected. A message states: 'You don't need to update the trust store if no proxy is present.'

Middle Screenshot: Shows 'Transparent Non-Inspecting Proxy' selected. A message states: 'You don't need to update the trust store to support a non-inspecting transparent proxy.'

Bottom Screenshot: Shows 'Transparent Inspecting Proxy' selected. A message states: 'Uploading a root certificate or end entity certificate is likely required to support an inspecting transparent proxy.' Below the message is a 'Check Proxy Connection' button with a note: 'Before you proceed, you must click the button to verify the proxy connection.'

Explicit Proxy



- Admin tells the VMN which proxy to use and authentication mechanism.
- Admin needs to know the proxy IP address and proxy listening port

Authentication Type:

- **None:** for HTTP or HTTPS explicit proxies, no further authentication is required.
- **Basic:** for HTTP or HTTPS explicit proxies and used for an HTTP user agent to provide a username and password when making a request, and uses Base64 encoding
- **Digest:** for HTTPS explicit proxies only and used to confirm the identity of a user before sending sensitive information, and applies a hash function on the username and password before sending over the network.
- **NTLM:** for HTTP only. Like Digest, NTLM is used to confirm the identity of a user before sending sensitive information. Uses Windows credentials instead of the username and password.

Troubleshooting

- Logs

- Send logs to Cisco
 - Log package contains media, system, and container logs
- Download logs locally to attach to a TAC case manually

- Packet Capture

- Captures packets from all interfaces
- 2 GB limit for the packet capture file
- Include upload identifier to a TAC case for the support engineer to look at the file

- Ping

Troubleshooting the Cisco Webex Video Mesh Solution - BRKCOL-3002

Event: 2019 San Diego

Speaker: Paul Stojanovski

<https://www.ciscolive.com/global/on-demand-library.html?#/>

The screenshot shows the 'Troubleshooting' page for a Cisco Webex Video Mesh Node. The left sidebar contains navigation options: Overview, Trust Store & Proxy, Server Certificate, and Troubleshooting (highlighted). The main content area is divided into three sections: Send Logs, Packet Capture, and Ping. Each section provides instructions and buttons for sending data to Cisco or downloading it locally. The Send Logs section shows an upload identifier and a download link for logs from May 29, 2019. The Packet Capture section shows a toggle for 'Start Packet Capture' and a download link for a 391.55 MB PCAP file from May 13, 2019. The Ping section has a text input for 'FQDN or IP Address' with '127.0.0.1' entered and a 'Ping' button.

Troubleshooting

- Trace Route
- Check NTP Server
- Reflector Tool
 - Used to identify blocked TCP or UDP ports on the node.
 - Requires client reflector script.
 - Must put the node in maintenance mode before you start the reflector server.
- Debug User
 - Only used when working with support

The screenshot shows the Cisco Webex Video Mesh Node Troubleshooting interface. The left sidebar contains navigation options: Overview, Trust Store & Proxy, Server Certificate, and Troubleshooting (highlighted). The main content area is divided into four sections:

- Trace Route:** Includes a "Trace Route To Host" section with a text input field containing "127.0.0.1" and a "Trace Route" button.
- Check NTP Server:** Includes a "View SNTP Query Response" section with a text input field containing "127.0.0.1" and a "Query NTP Server" button.
- Reflector Tool:** Includes a "Reflector Server Type" section with radio buttons for "TCP Reflector Server" (selected) and "UDP Reflector Server". Below it is a "Start Reflector Server" section with a toggle switch for "Start Reflector Server" (disabled) and a note: "Reflector server startup can take upto a minute. Please wait for a confirmation message after starting the reflector server."
- Debug User:** Includes a "Debug User" section with a toggle switch for "Enable Debug User" (enabled) and a note: "Debug user expires: Never".

The bottom left corner of the interface shows a user profile icon and the name "admin".

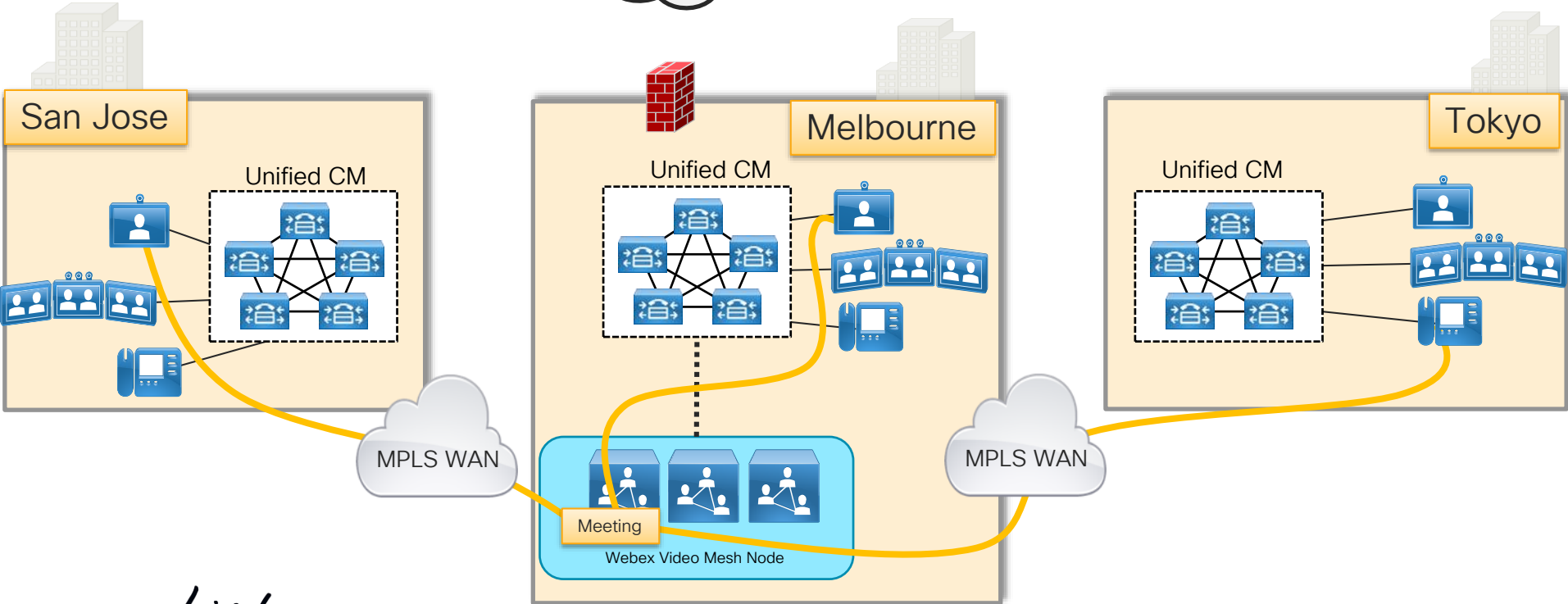
VMN Architecture Deployments

Regional Design

Centralized VMN

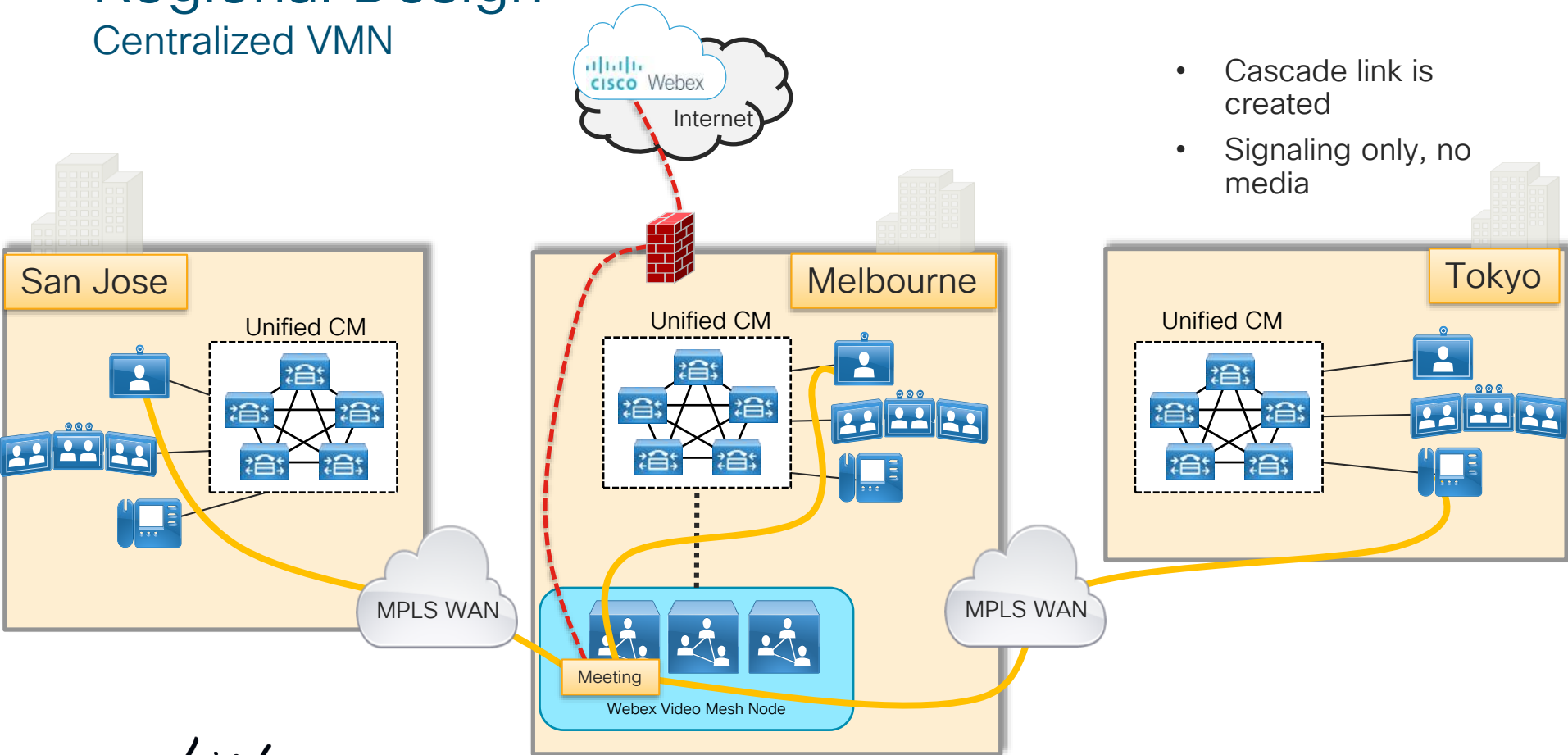


- Internal SIP endpoints have joined



Regional Design

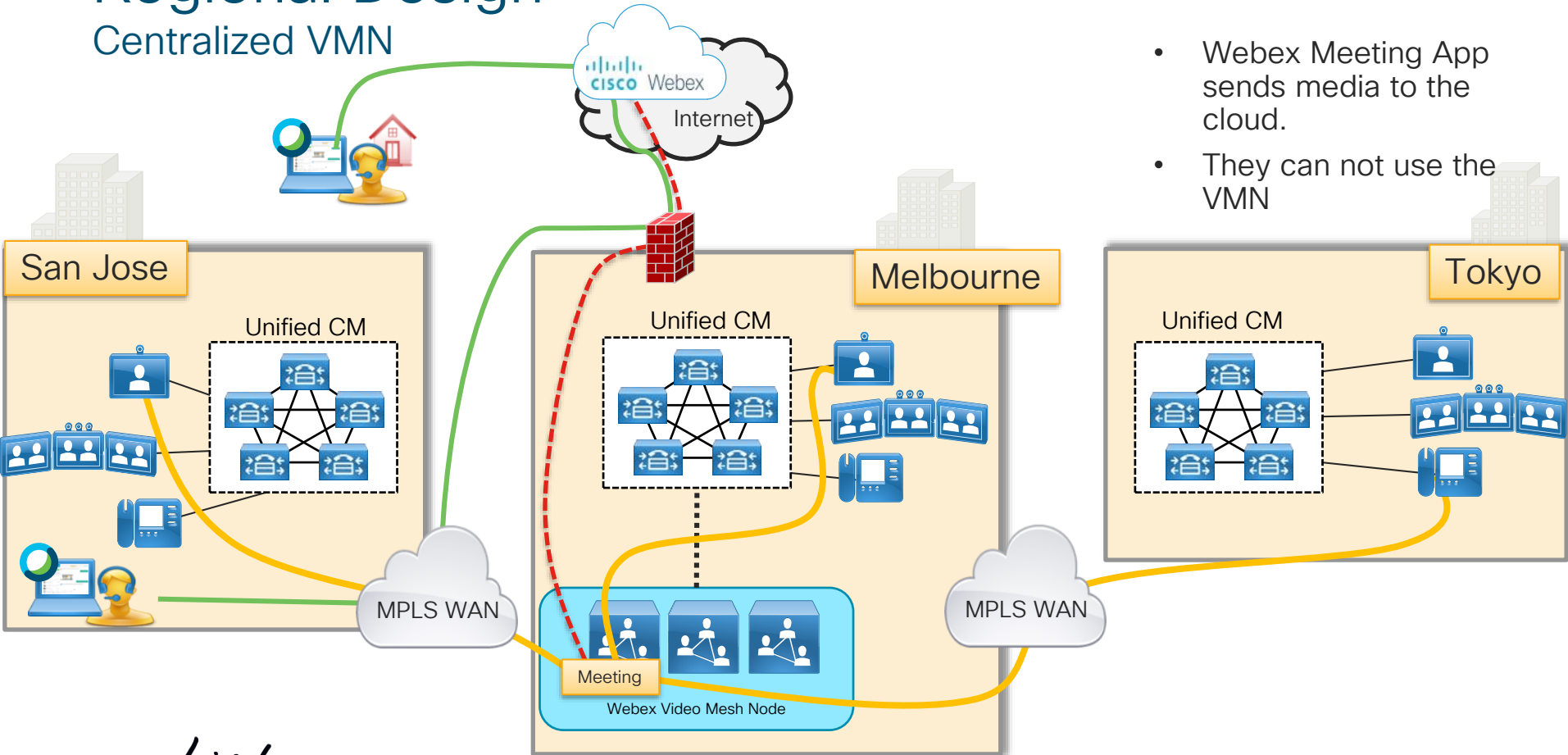
Centralized VMN



- Cascade link is created
- Signaling only, no media

Regional Design

Centralized VMN

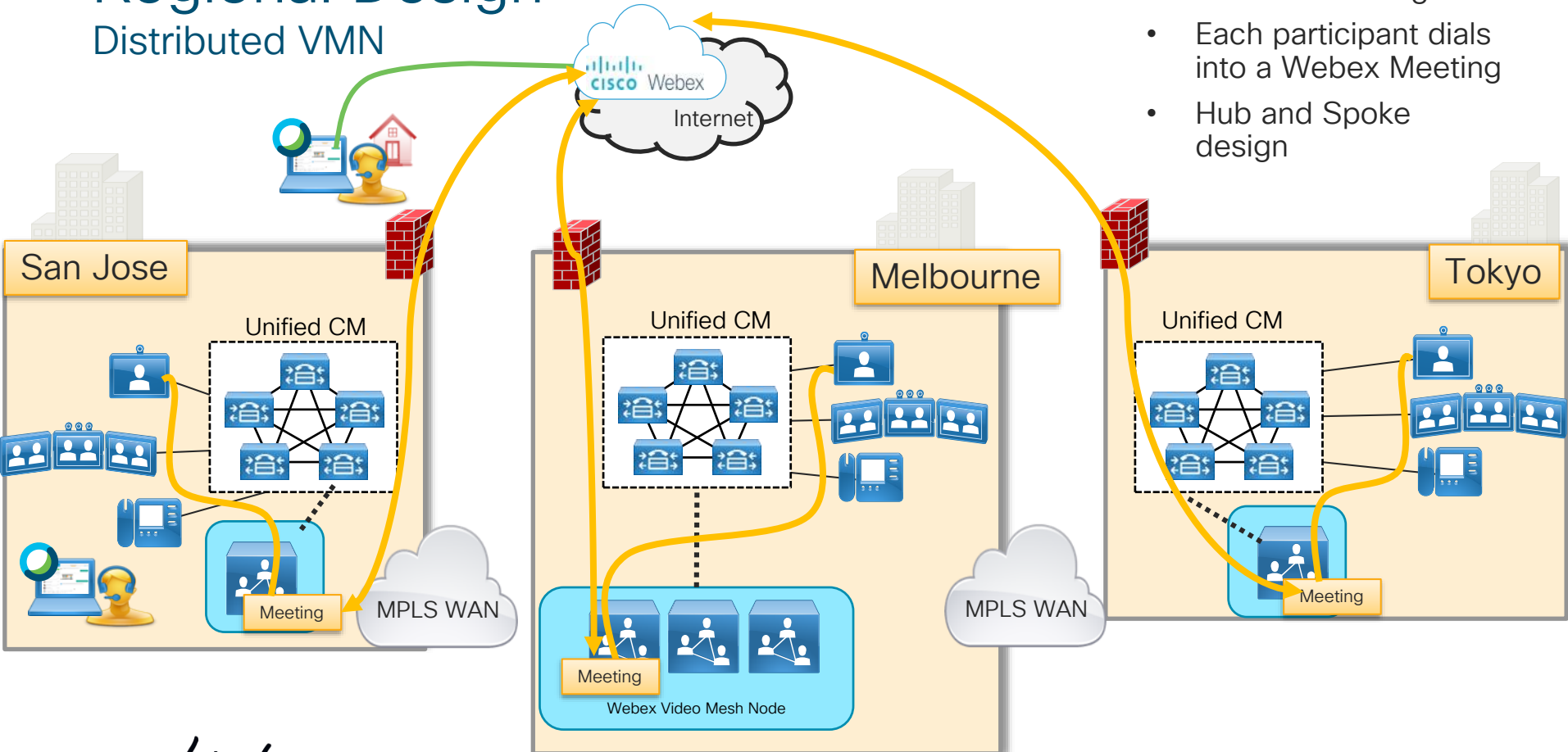


- Webex Meeting App sends media to the cloud.
- They can not use the VMN

Regional Design

Distributed VMN

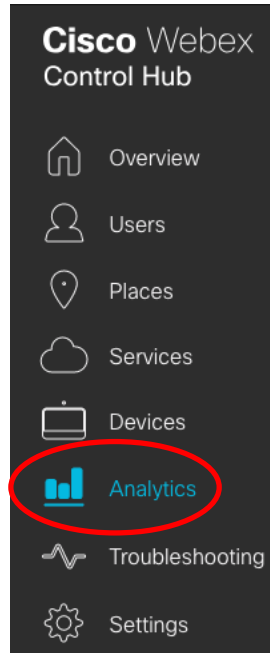
- Local VMs in region
- Each participant dials into a Webex Meeting
- Hub and Spoke design



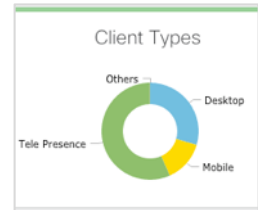
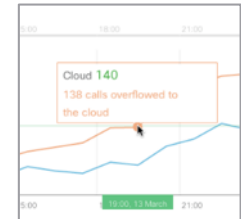
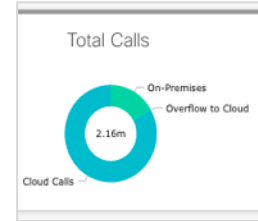
Control Hub Reporting

Cisco Webex Control Hub

<https://admin.webex.com>

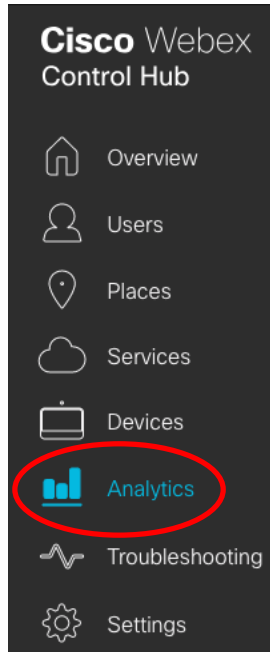


- Webex Video Mesh Reports enables administrator to understand the trend of their on premises resource capacity and utilization, as well as availability that impacts capacity.
- Webex Video Mesh Activity graph gives an overall perspective of the number of calls hosted on the cloud vs the number of calls that were hosted on on-premises clusters in an organization.
- Webex Video Mesh Activity Adoption tab added to the reports to help administrators find the most popular categories of client types and utilization in the organization.



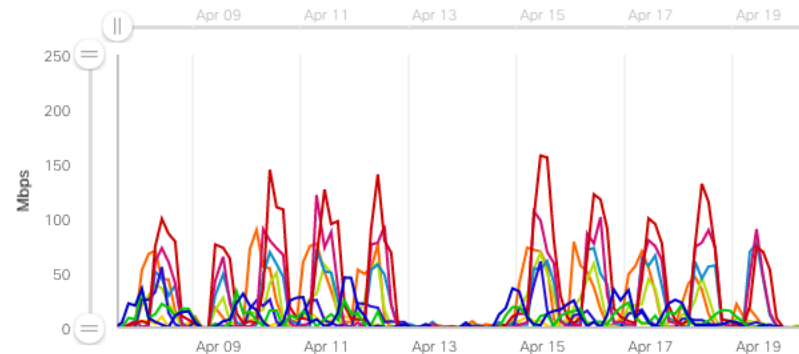
Cisco Webex Control Hub

<https://admin.webex.com>



- Webex Video Mesh Cascade Bandwidth reports enables administrator to understand the amount of bandwidth used with a Video Mesh cluster cascades to the Webex cloud for the meetings

Cluster Cascade Bandwidth Usage ⓘ



Key points to remember in architecting a Video Mesh solution

One recommendation does not fit all deployments

- Video Mesh is a cloud service on the customer premises. It is not the same as an MCU.
- Deploy Video Mesh cluster(s) in a large campus site or Datacenter close to the Internet connection
- Start small and grow
- Continuously monitor the reports in Webex Control Hub.
 - Add more Video Mesh Nodes as the number of overflows to the cloud trend upwards

Documentation

Reference Links

- Deployment Guides
 - Webex Edge Connect: <https://collaborationhelp.cisco.com/article/en-us/n68tcpb>
 - Webex Edge Audio: <https://collaborationhelp.cisco.com/article/en-us/xmsy7d>
 - Video Mesh: <https://collaborationhelp.cisco.com/article/en-us/jgobq2>
- Datasheets
 - Webex Edge: <https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-edge/data-sheet-c78-741264.pdf>
 - Video Mesh: <https://www.cisco.com/c/en/us/solutions/collaboration/webex-hybrid-services/webex-hybrid-media-service.html>
- Webex Audio Coverage: 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>

Components of Webex Edge for Meetings



Webex Edge for Meetings

1 Connect

Direct Connection to the
Webex Datacenter

2 Audio

Webex Meeting Audio via the
Internet or Edge Connect

3 Video Mesh

Meeting Resources on
premises

Complete your online session survey



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education



Demos in the
Cisco Showcase



Walk-In Labs



Meet the Engineer
1:1 meetings



Related sessions



Thank you





You make **possible**