
cisco
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

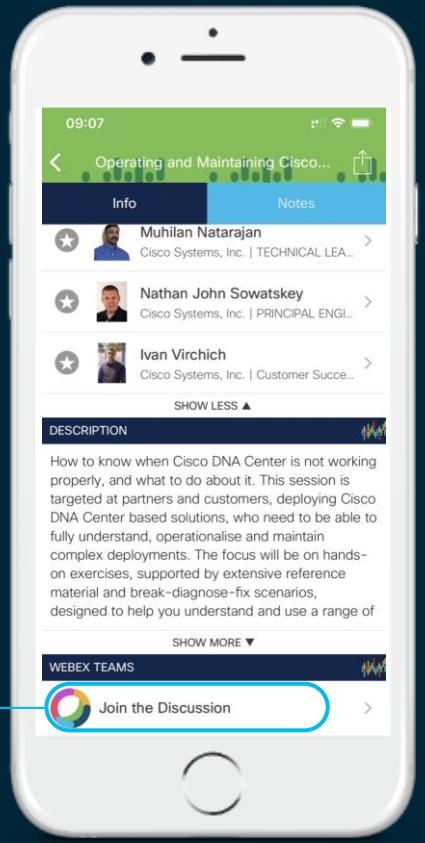
Cisco Webex Teams

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

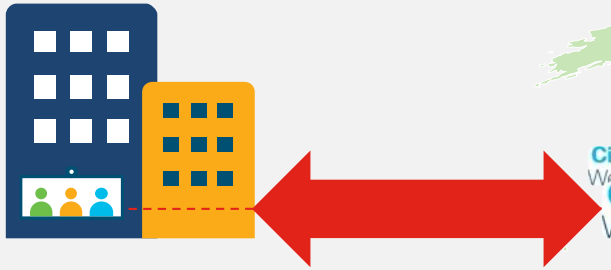
- Webex Edge Connect
  - Overview
- Webex Edge Audio
  - Design and Implementation
- Webex Edge Video Mesh
  - Design and Implementation
- Conclusion

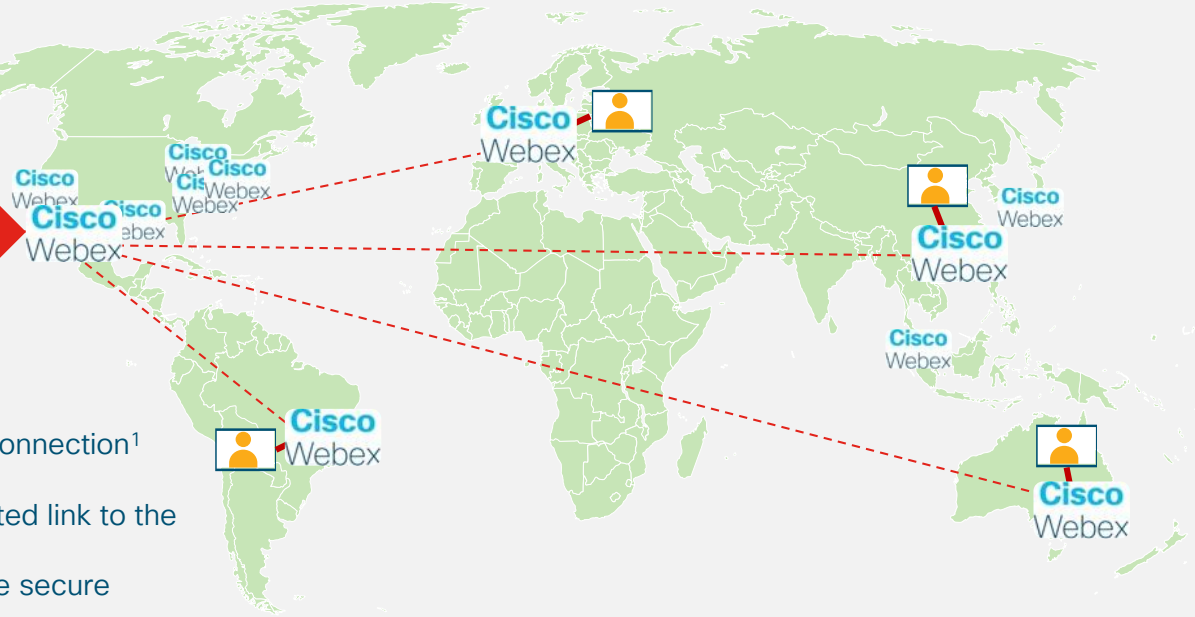
Components of Webex Edge for Meetings

Webex Edge 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 connection[1] 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

[1] *via a peering agreement with Equinix*

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

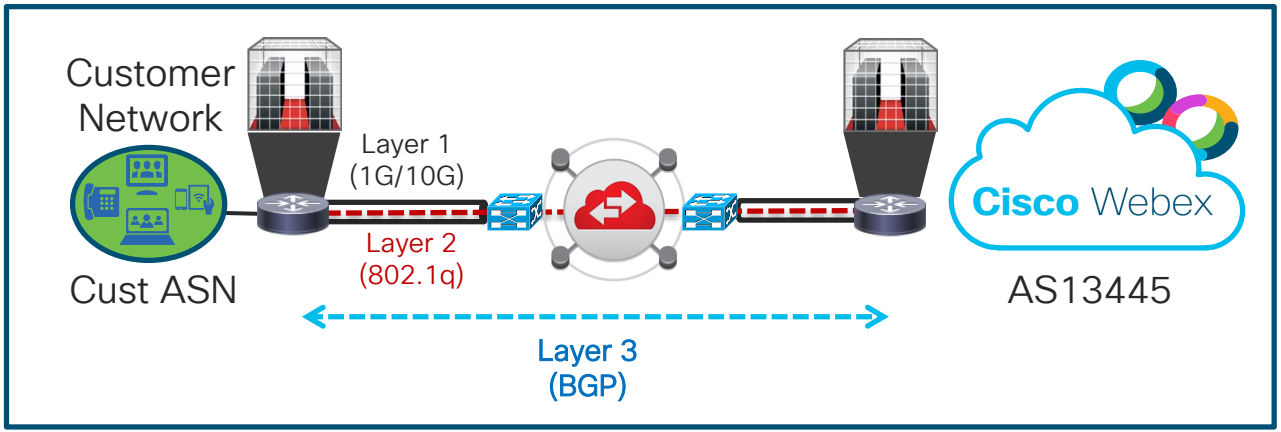
- Webex Meetings
- Webex Teams Media *
- Video Device-Enabled Webex Meetings (CMR)
- Webex Edge Audio

* 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



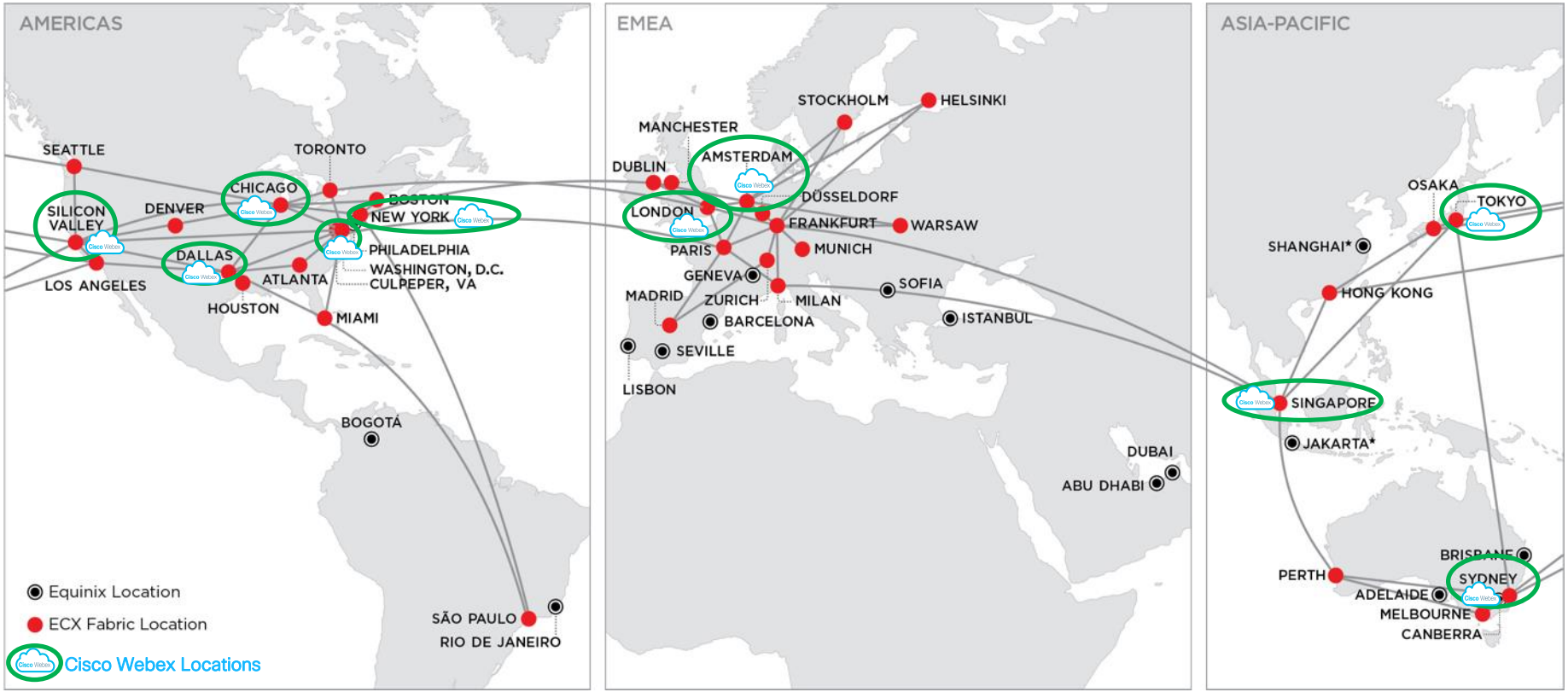
IMPORTANT ROLES AND RESPONSIBILITIES

1. Layer 1 – Physical Connectivity
2. Layer 2 – Ethernet Connectivity

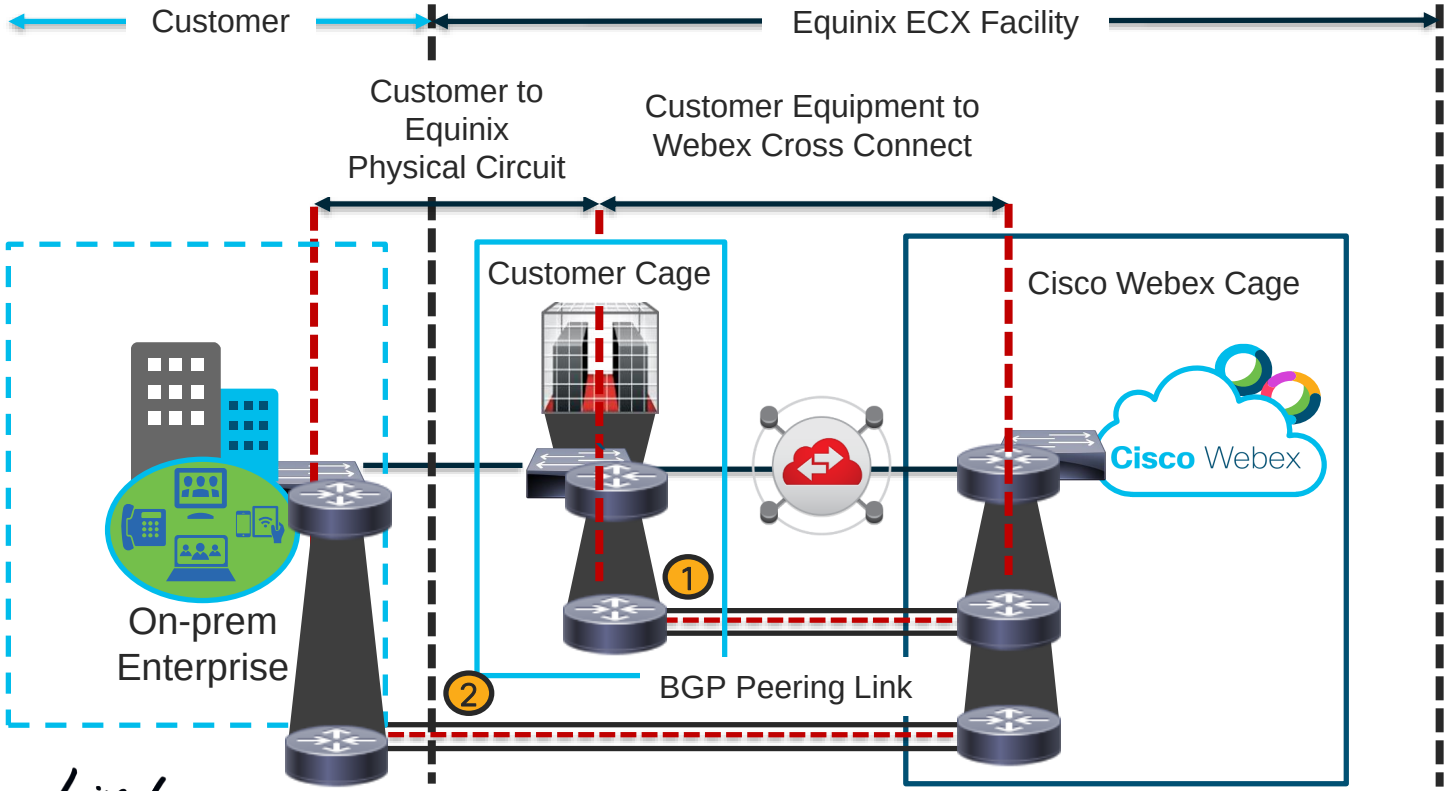
Equinix responsibility:
- ✓ Physical link provisioning (cross connects)
- ✓ Virtual circuit monitoring reports & support

3. Layer 3 – IP connectivity

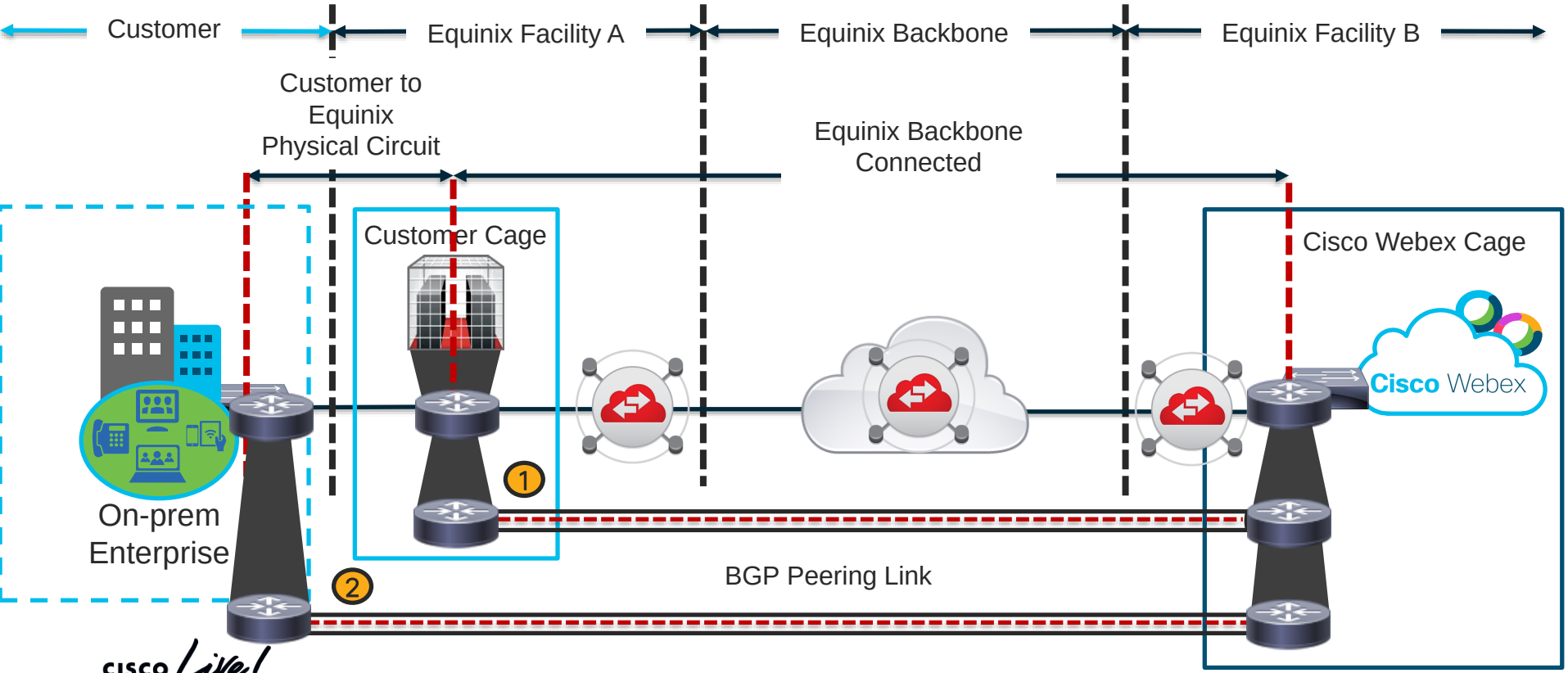
Cisco responsibility
- ✓ peering provisioning and support



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

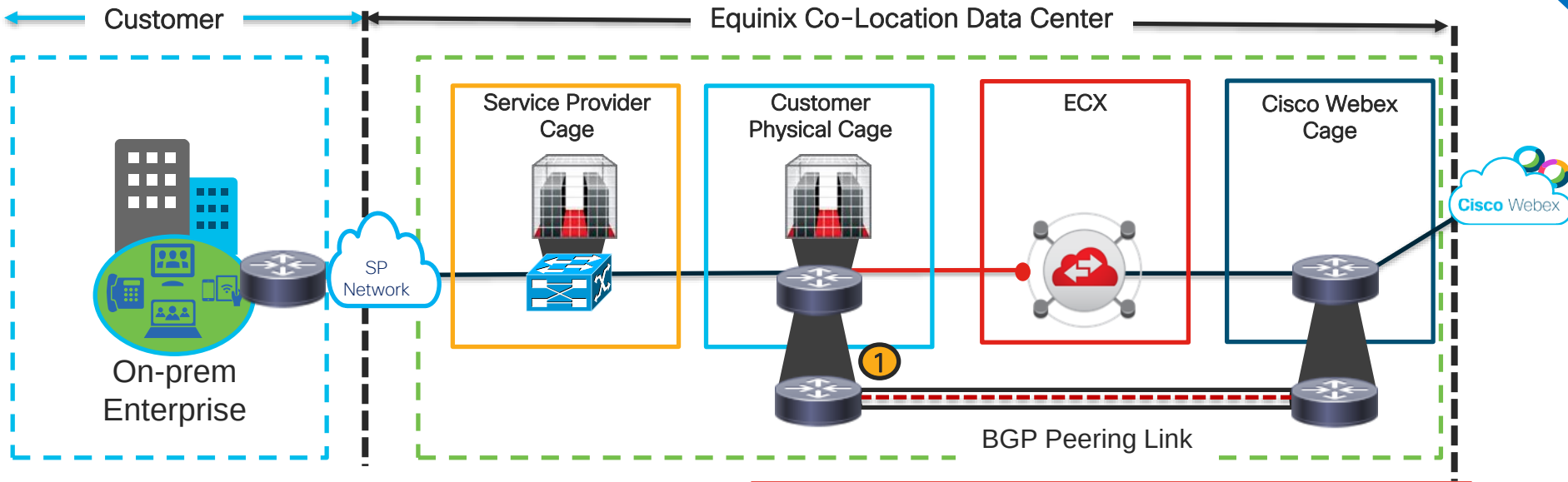


Option 1: Equinix Cloud Exchange (ECX) Direct Peering via Customer Cage 'Remote Port'



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

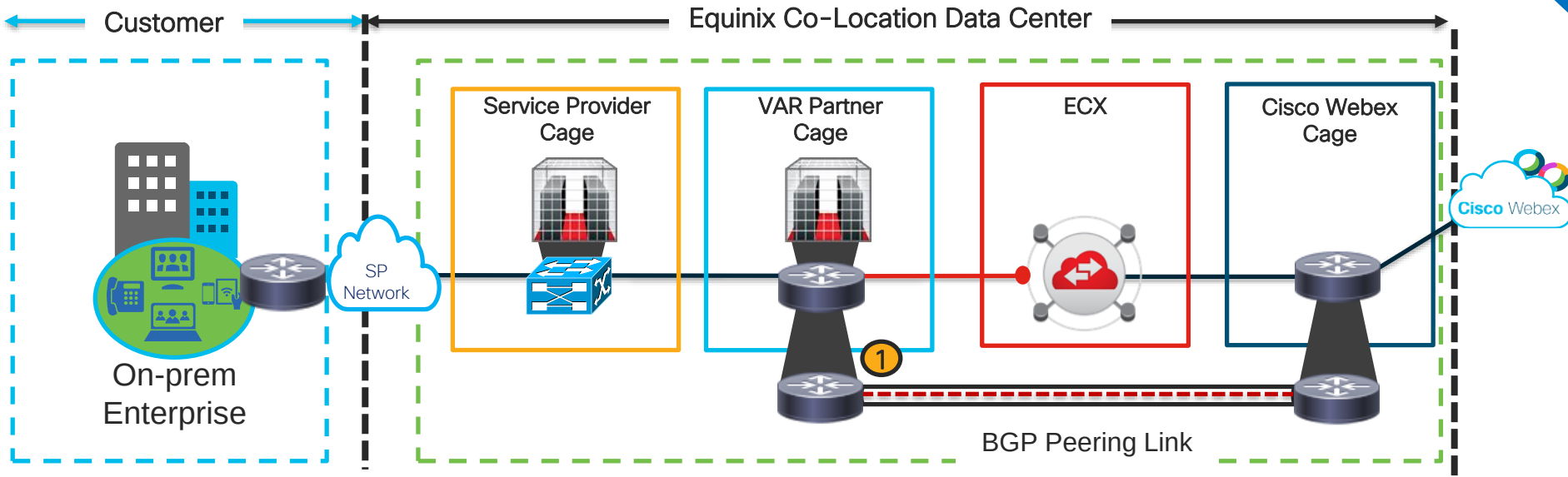
IN EFT TRIALS



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

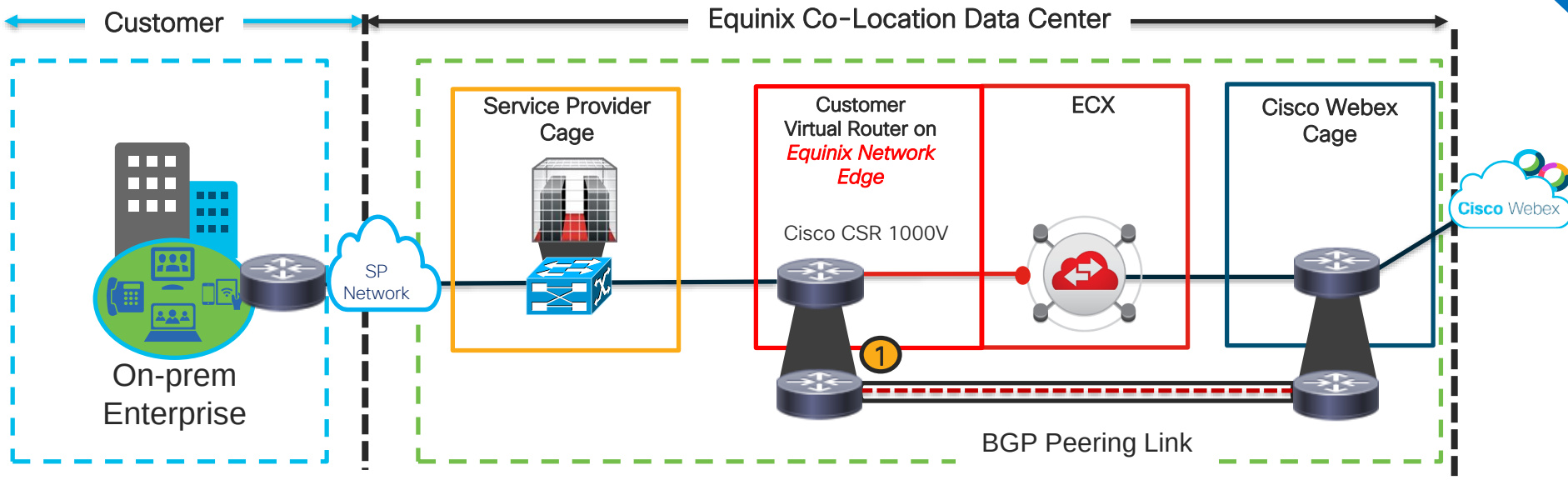
IN EFT TRIALS



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

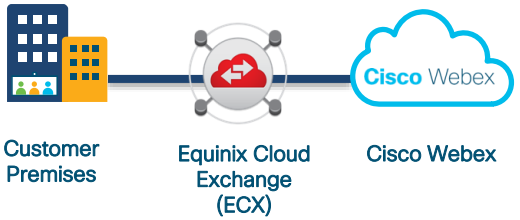


When a customer does not have a cage in Equinix DC, they can consider the new Equinix 'Network Edge' option; however, the the ECX connection will be considered a 'Remote Port' with additional monthly fees from Equinix.

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



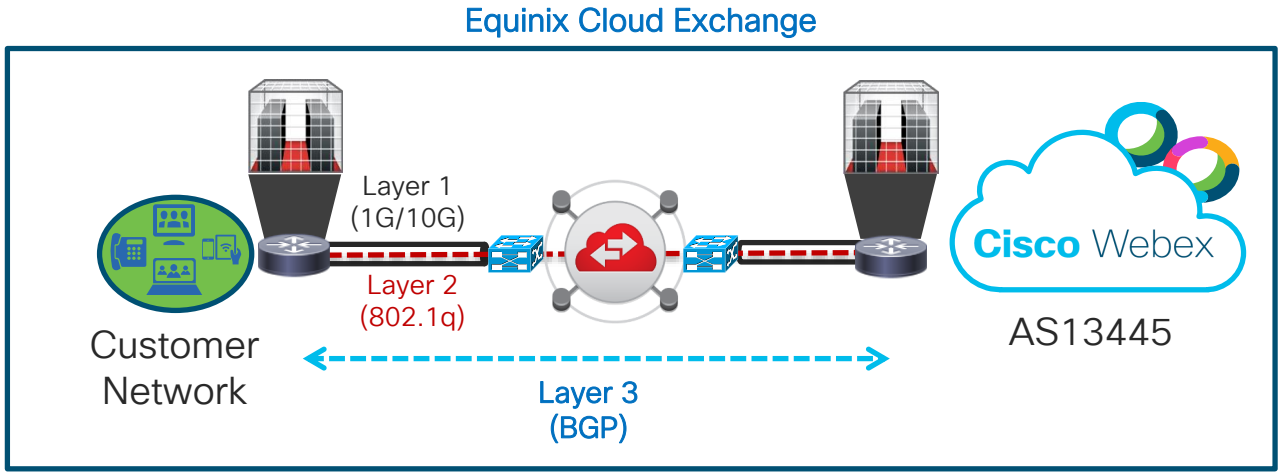
- IP Addressing
  - Public IP – /30 or /31 supported
  - Max length prefix that Webex advertises is /24
  - The maximum length prefix that Webex accepts is /29
  - The maximum number of routes Webex accepts is 100
  - We recommend that customers allow 50 routes from Webex on the BGP peering as the number 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



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
2. Layer 2 – Ethernet Connectivity

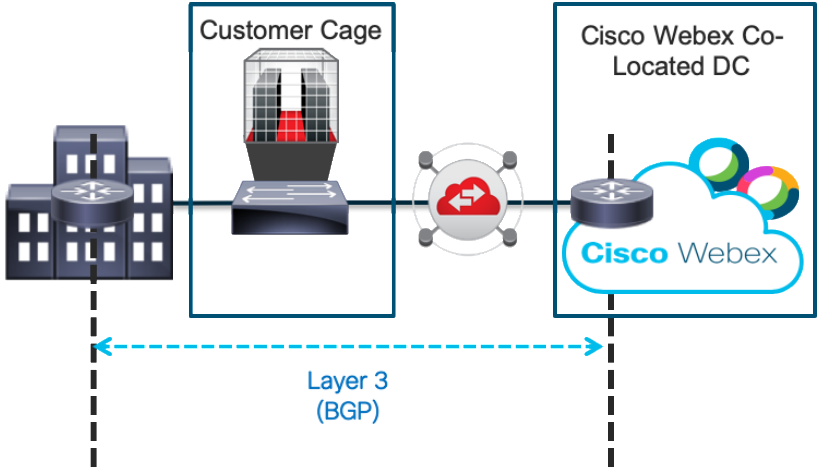
Equinix responsibility:
- ✓ Physical link provisioning (cross connects)
- ✓ Virtual circuit monitoring reports & support

3. Layer 3 – IP connectivity

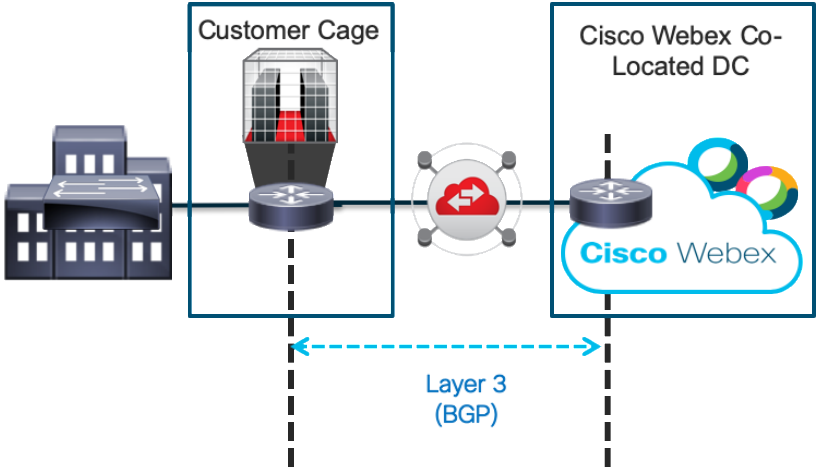
Cisco responsibility
- ✓ peering provisioning and support

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

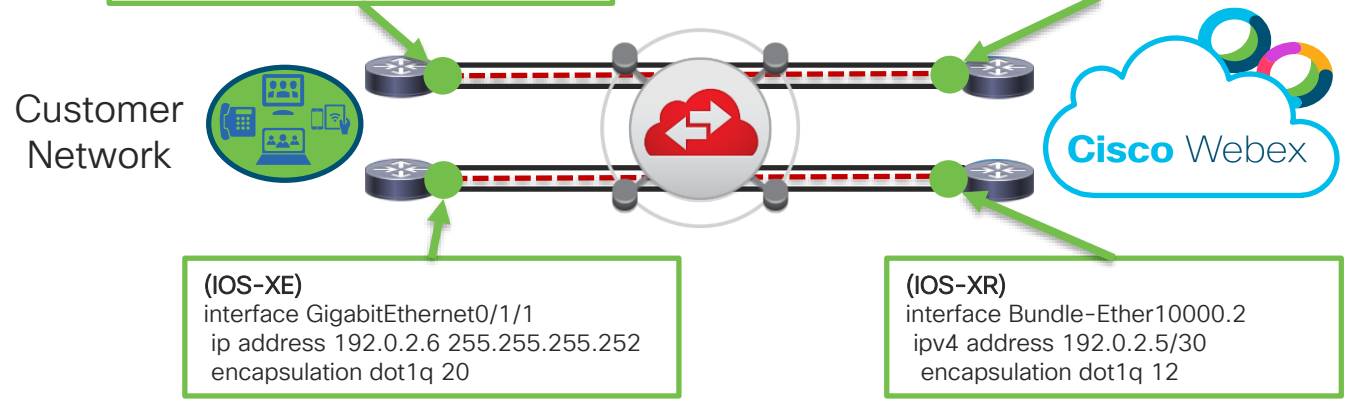
BGP Peering Configuration – high level

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

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

(IOS-XE)
```
interface GigabitEthernet0/1/1
 ip address 192.0.2.2 255.255.255.252
 encapsulation dot1q 10
```

(IOS-XR)
```
interface Bundle-Ether10000.2
 ipv4 address 192.0.2.1/30
  encapsulation dot1q 11
```

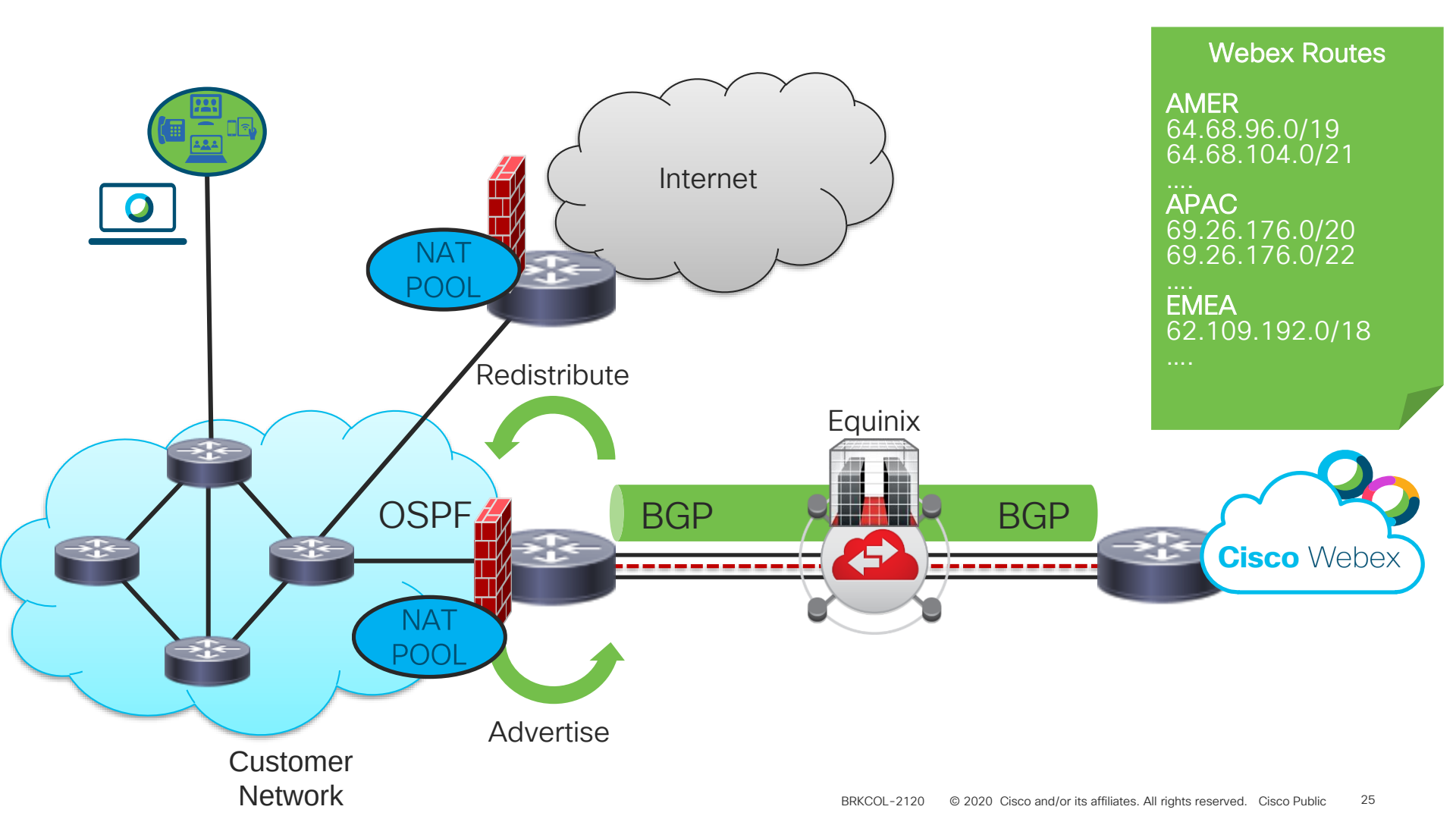


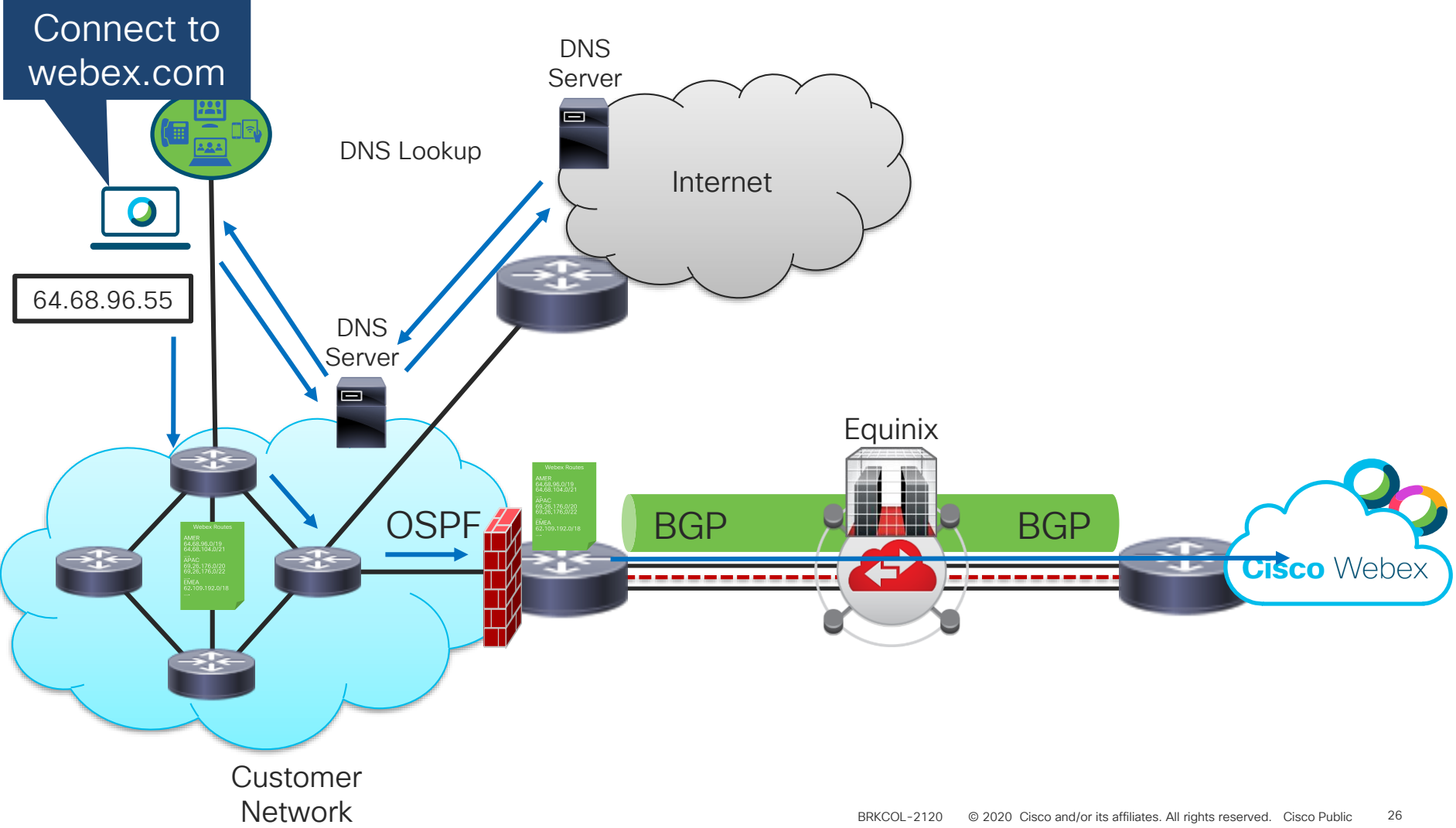
Cisco Recommends Dual peering links for high availability

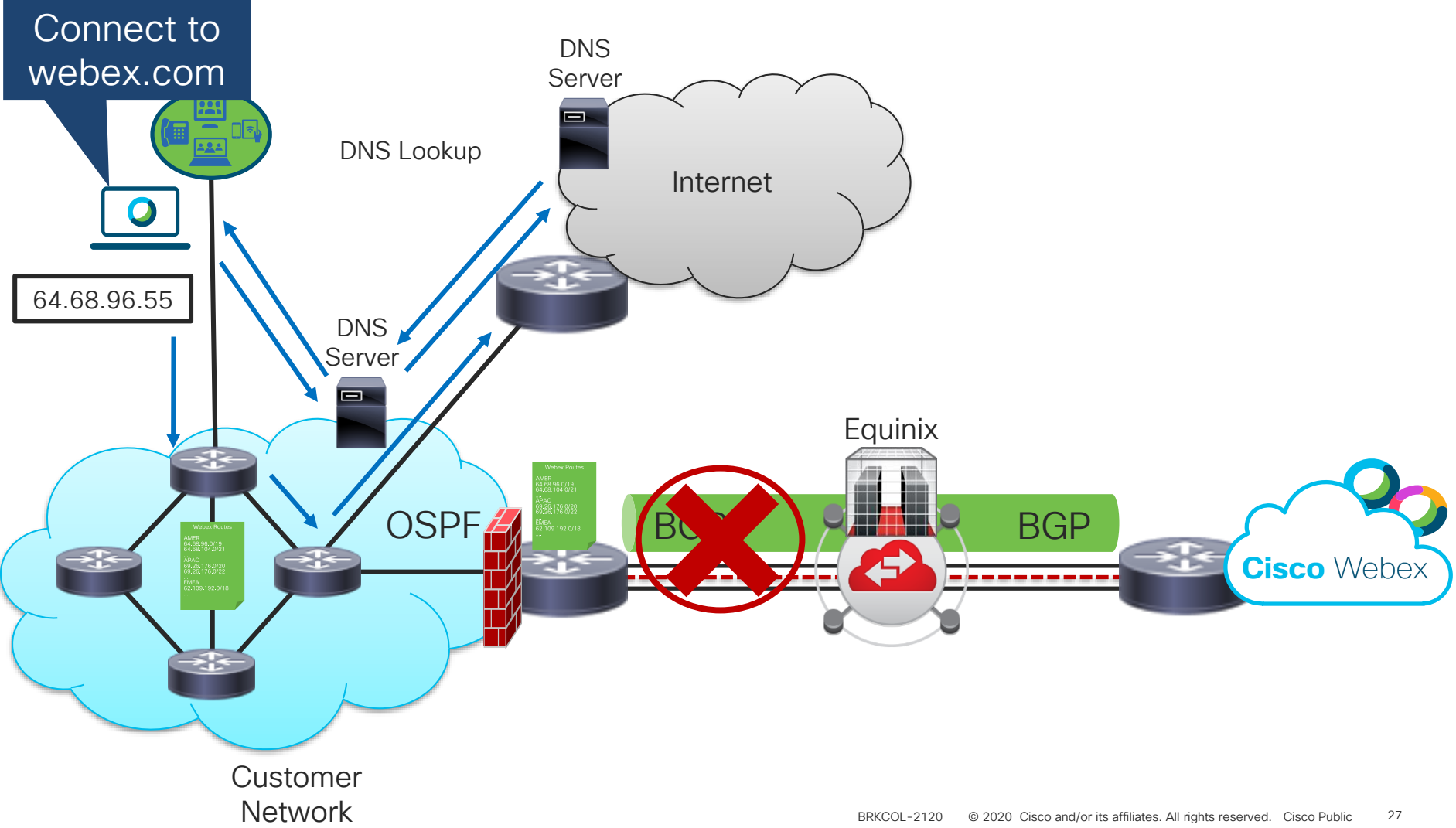
(IOS-XE)
```
interface GigabitEthernet0/1/1
 ip address 192.0.2.6 255.255.255.252
 encapsulation dot1q 20
```

(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







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)

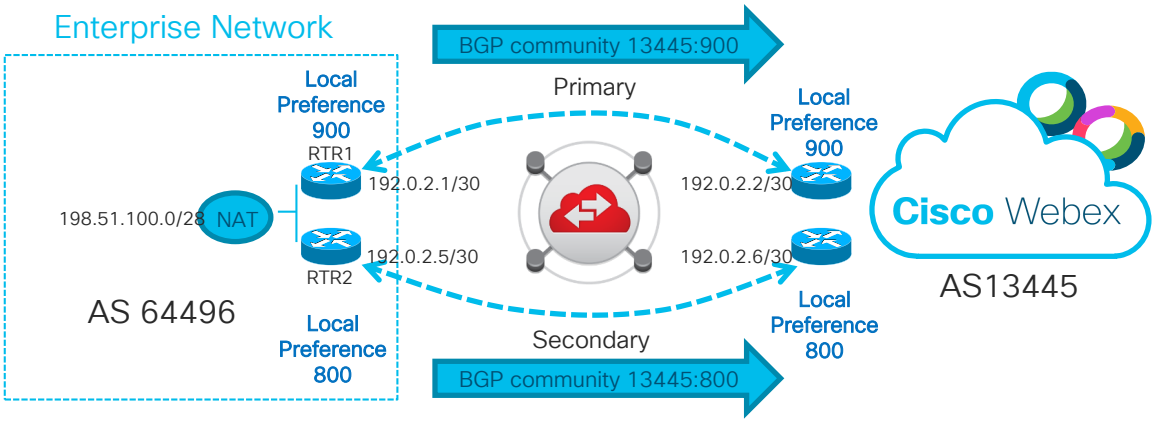
Webex Prefix BGP Origin communities
- **13445:10000** – AMER
- **13445:10010** – EMEA
- **13445:10020** – APAC

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.



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.

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
```

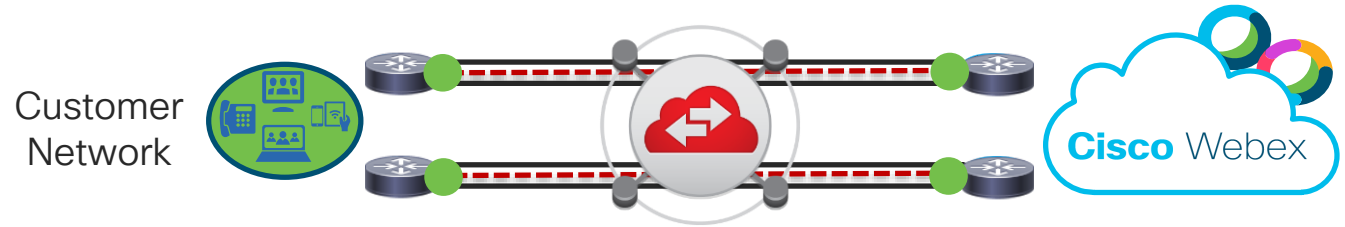
RTR2 Example BGP Configuration

```
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 Prefix BGP Origin communities

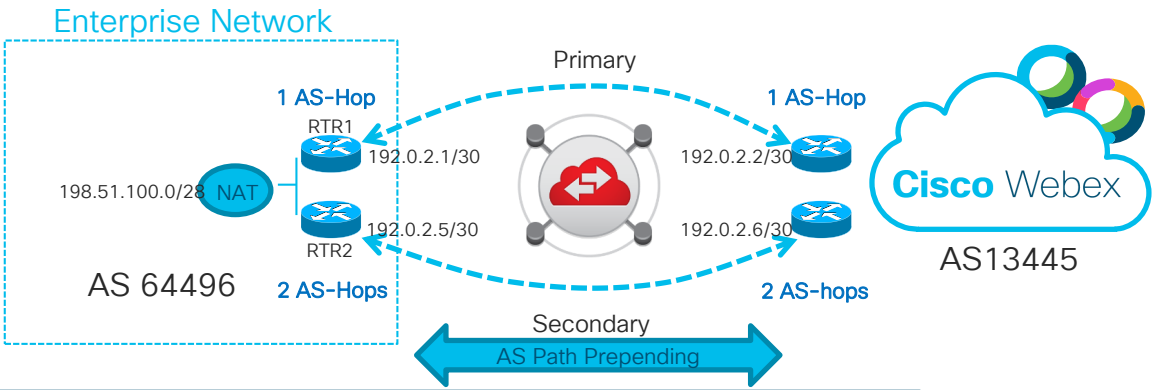
Filter routes by Origin Community (per Theater)

- 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.

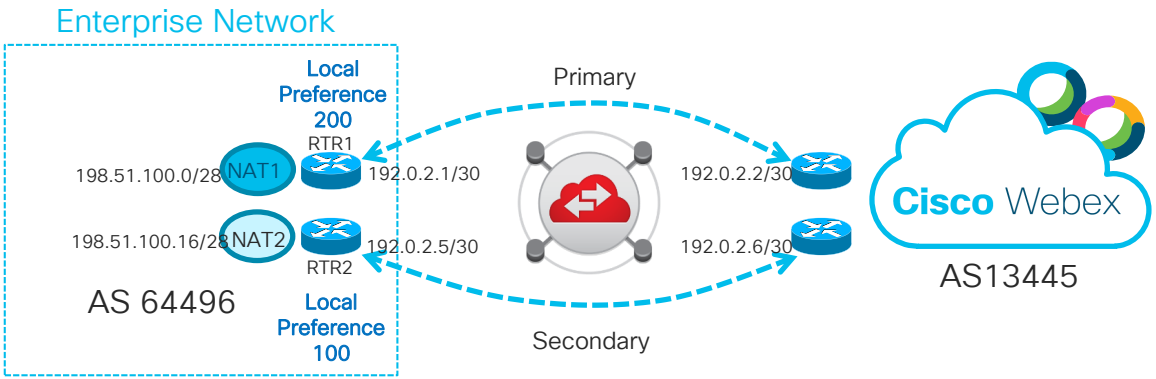
IOS XE

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

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:
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.

IOS XE

RTR1 Example BGP Configuration

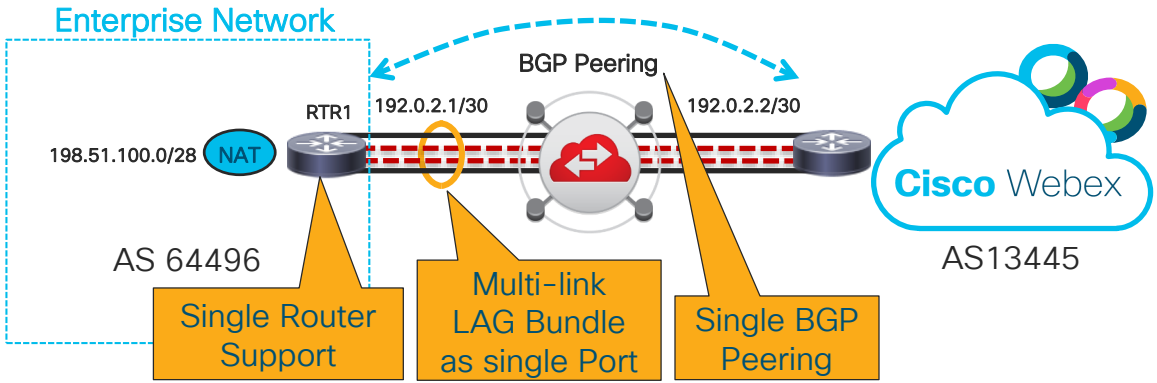
```
router bgp 64496
 neighbor 192.0.2.2 remote-as 13445
!
 address-family ipv4
  neighbor 192.0.2.2 activate
  neighbor 192.0.2.2 send-community both
  neighbor 192.0.2.2 route-map PRIMARY-OUT out
  neighbor 192.0.2.2 route-map PRIMARY-IN in
exit-address-family
!
ip prefix-list ADVERTISE-NAT1-TO-WEBEX 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

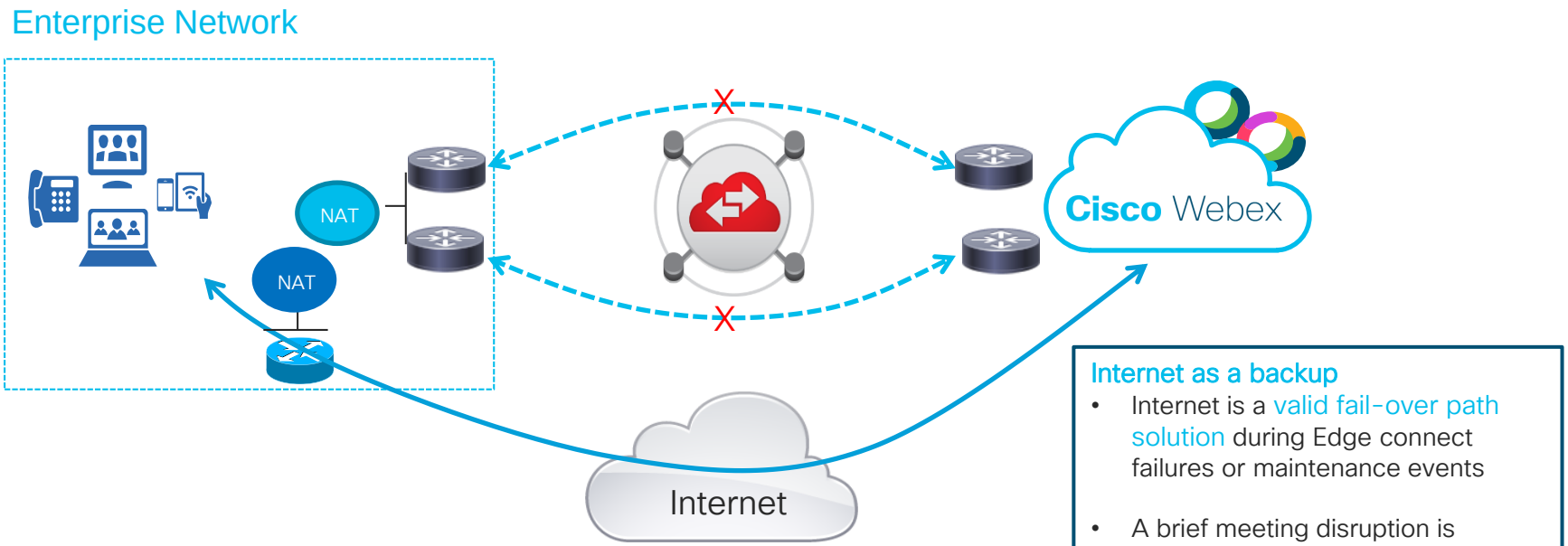
```
router bgp 64496
neighbor 192.0.2.6 remote-as 13445
 !
 address-family ipv4
  neighbor 192.0.2.6 activate
  neighbor 192.0.2.6 send-community both
  neighbor 192.0.2.6 route-map SECONDARY-OUT out
  neighbor 192.0.2.6 route-map SECONDARY-IN in
exit-address-family
!
ip prefix-list ADVERTISE-NAT2-TO-WEBEX 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
```

High Availability and Redundancy

Equinix Circuit



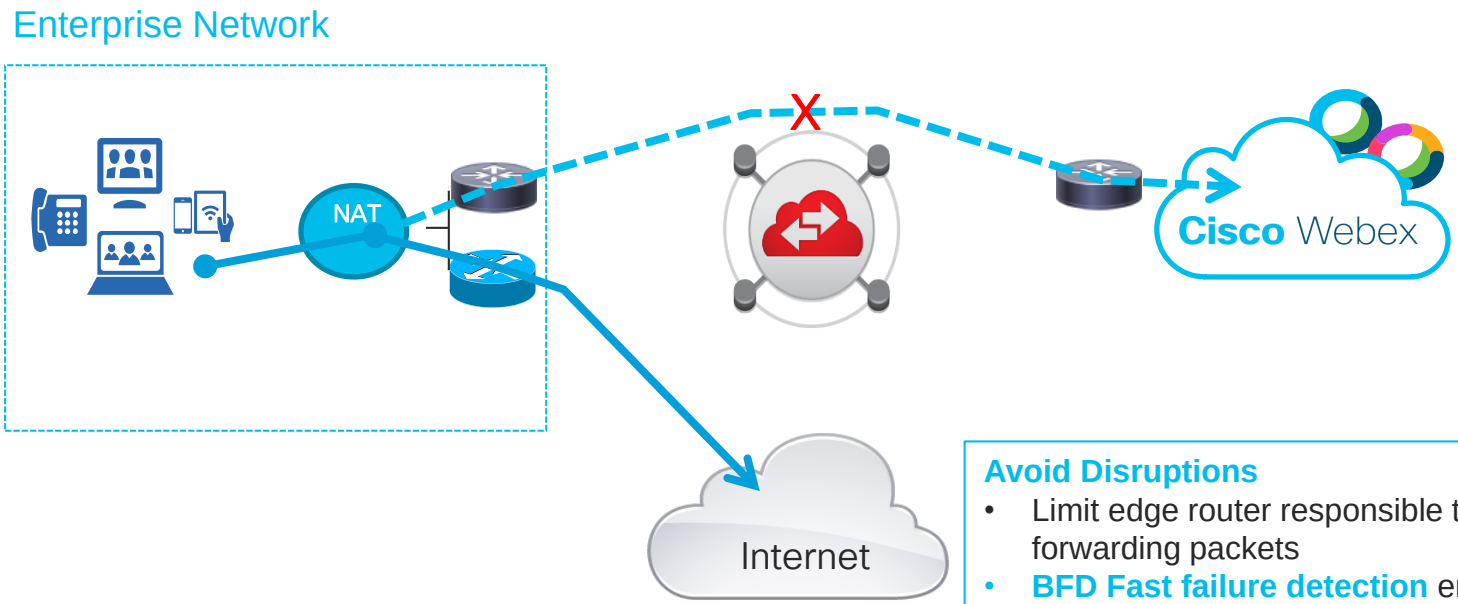
Internet as a backup



Internet as a backup

- Internet is a valid fail-over path solution during Edge connect failures or maintenance events
- A brief meeting disruption is expected if the client IP address changes due to NAT pool change

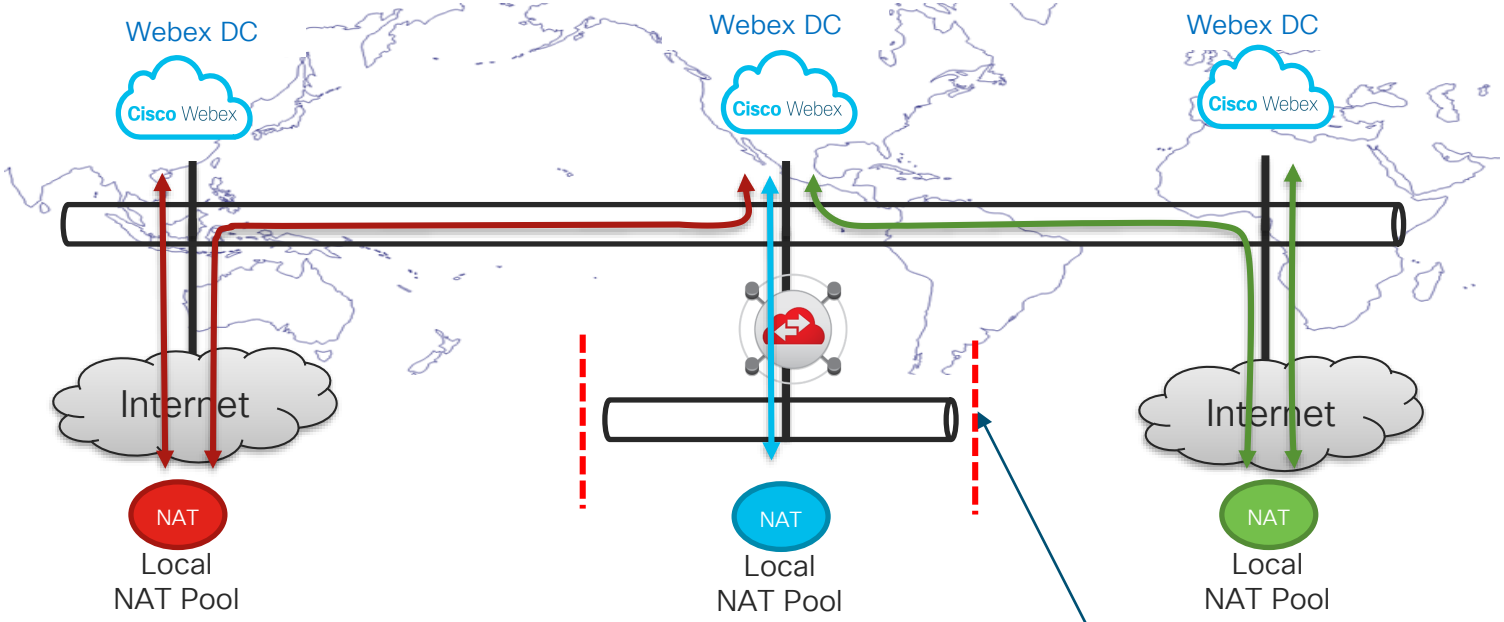
Internet as a backup



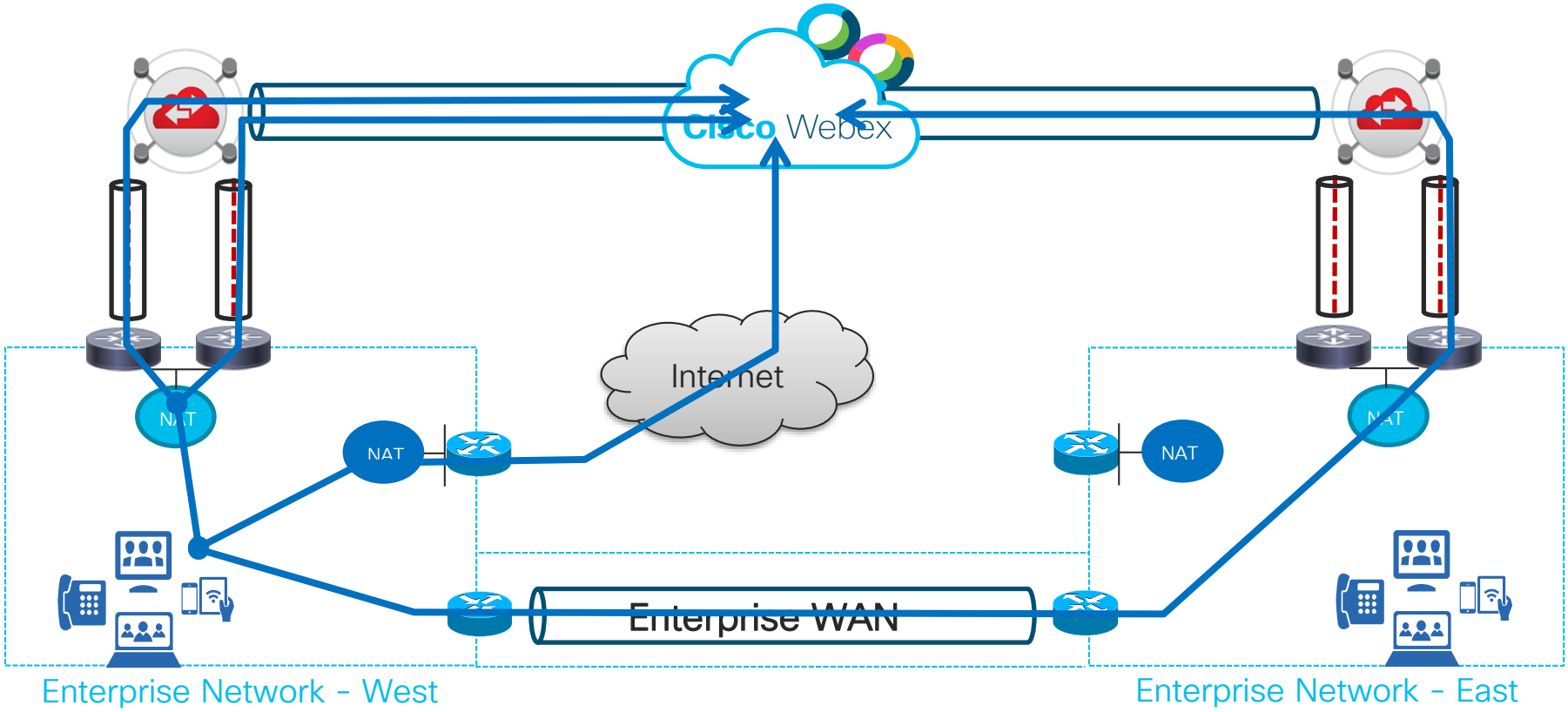
Avoid Disruptions

- 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**

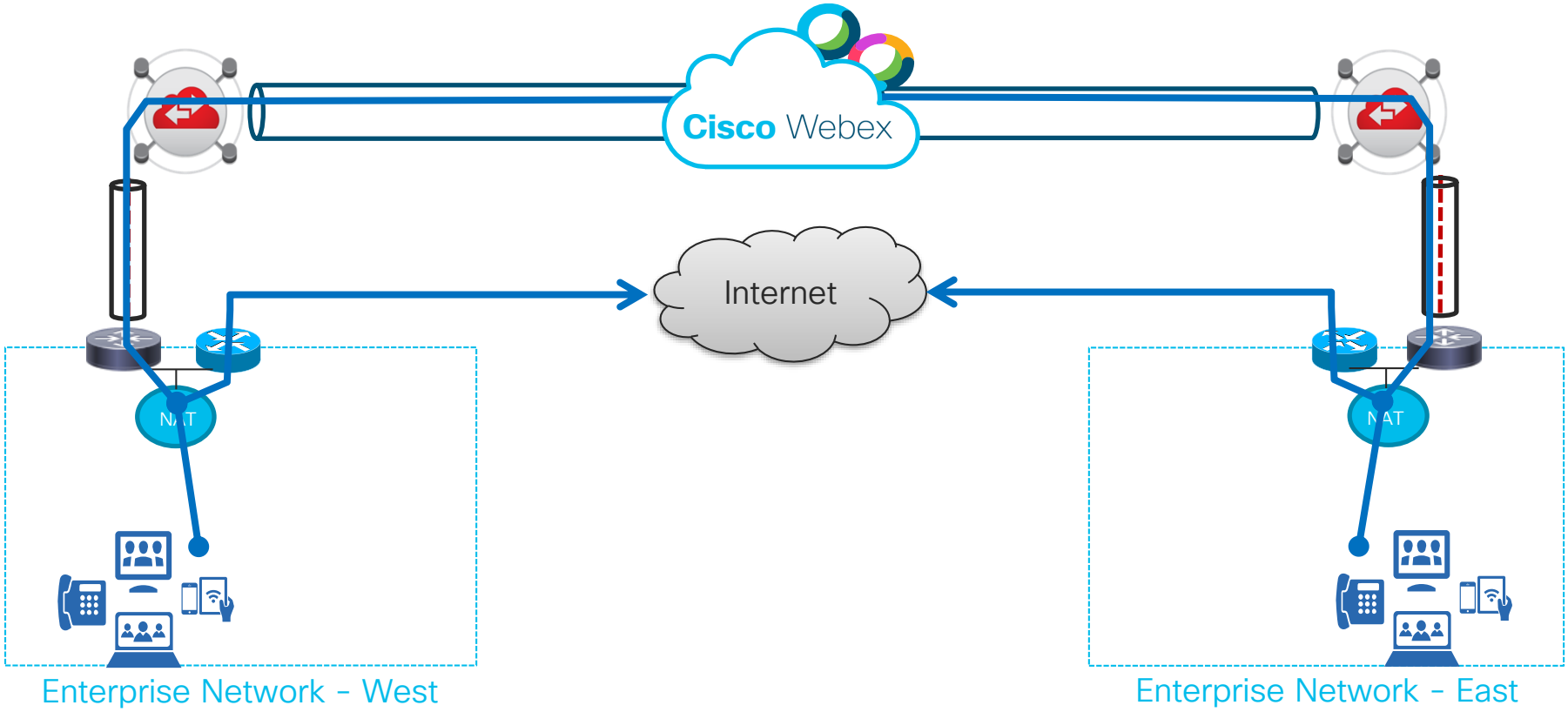
Hybrid Peering: Edge Connect and Direct Internet Access



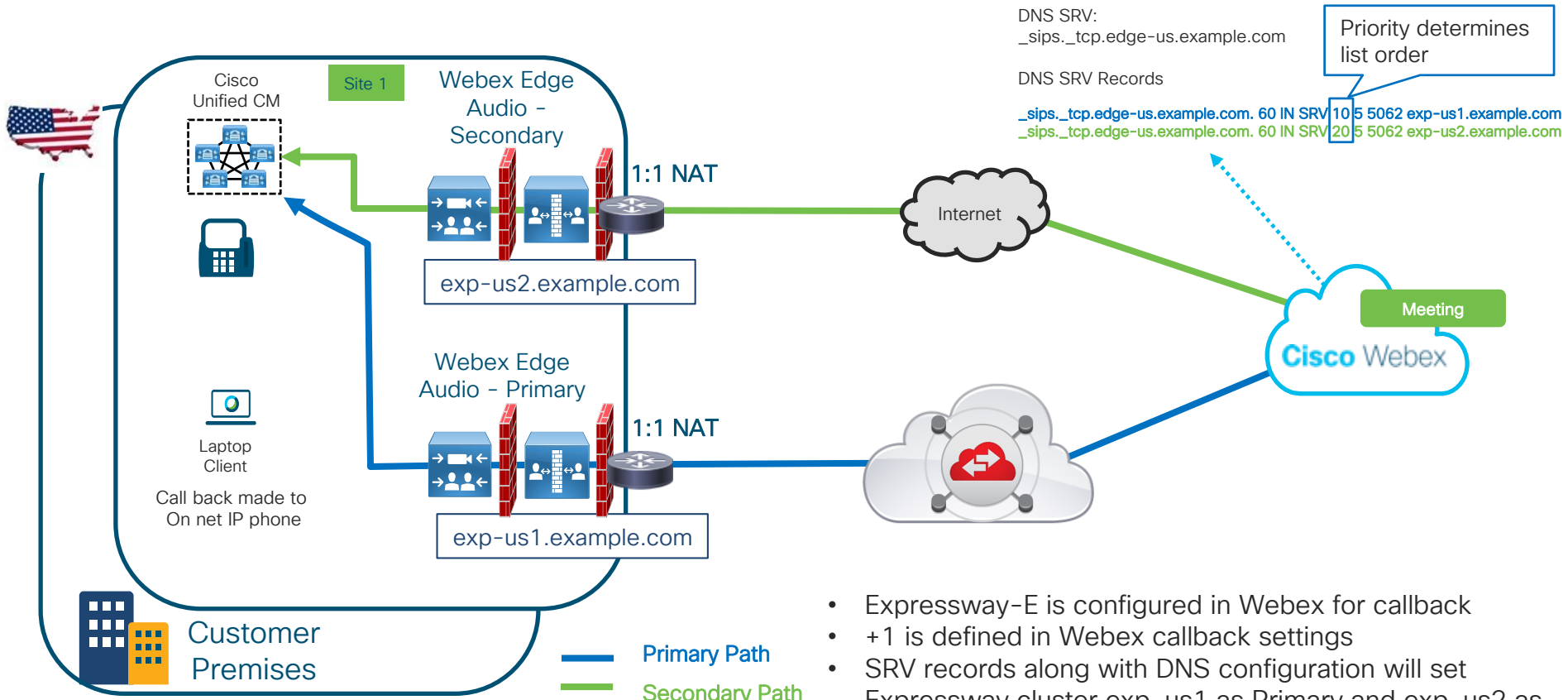
Link Redundancy and Site Redundancy



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

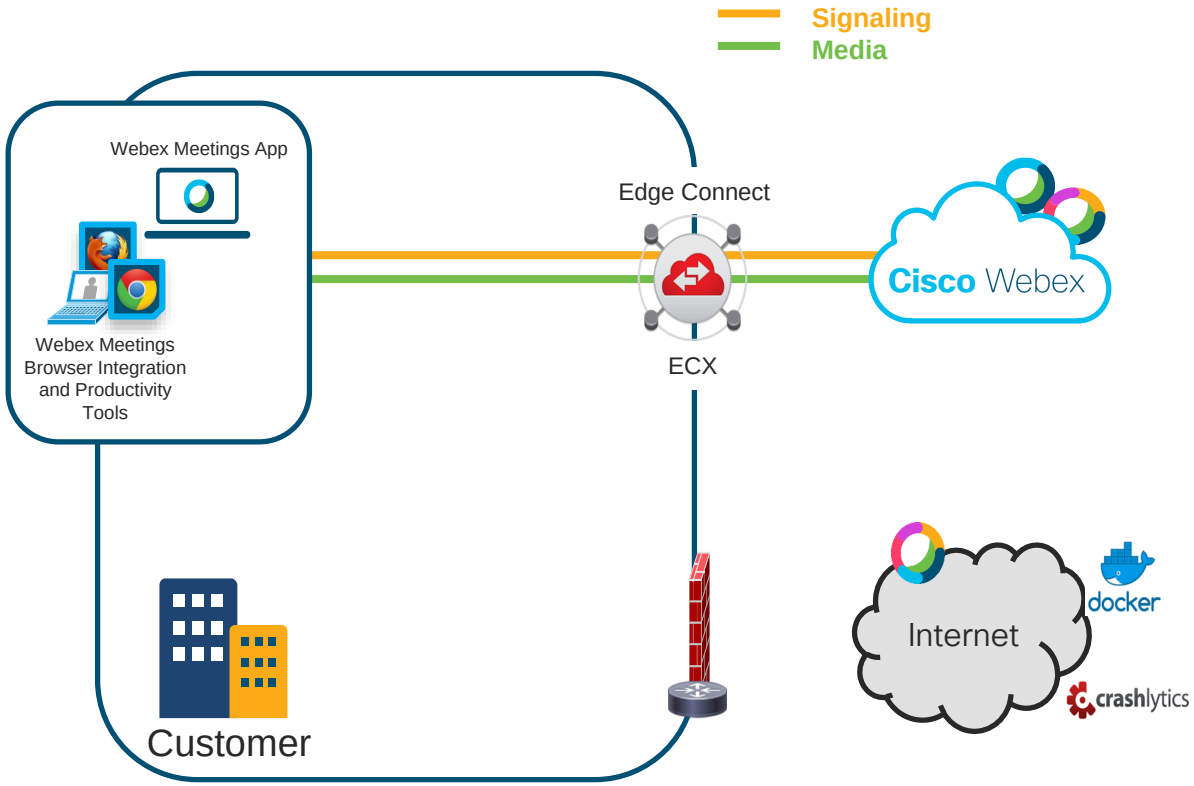
Webex Edge Connect – Traffic

Signaling and Media

Edge Connect Peering Link

Webex Meetings App Signaling and Media

Public Internet



Webex Edge Connect – Traffic

Signaling and Media

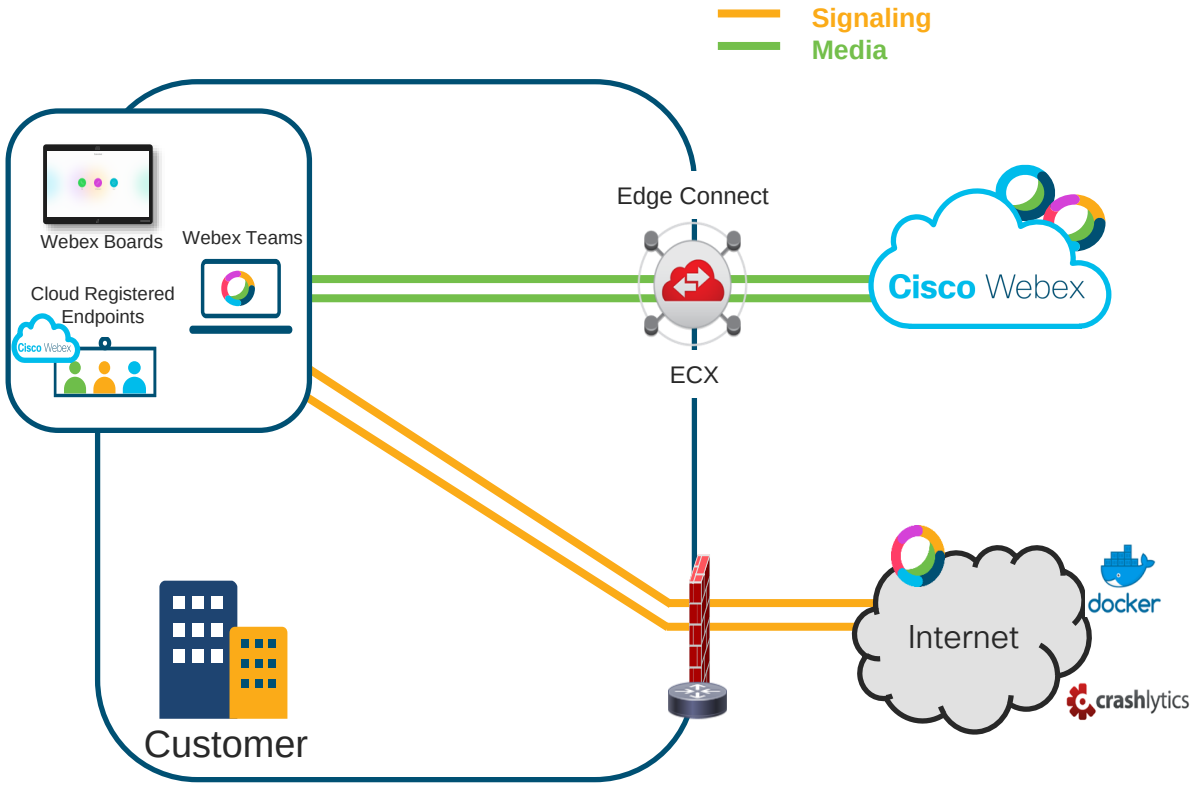
Edge Connect Peering Link

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

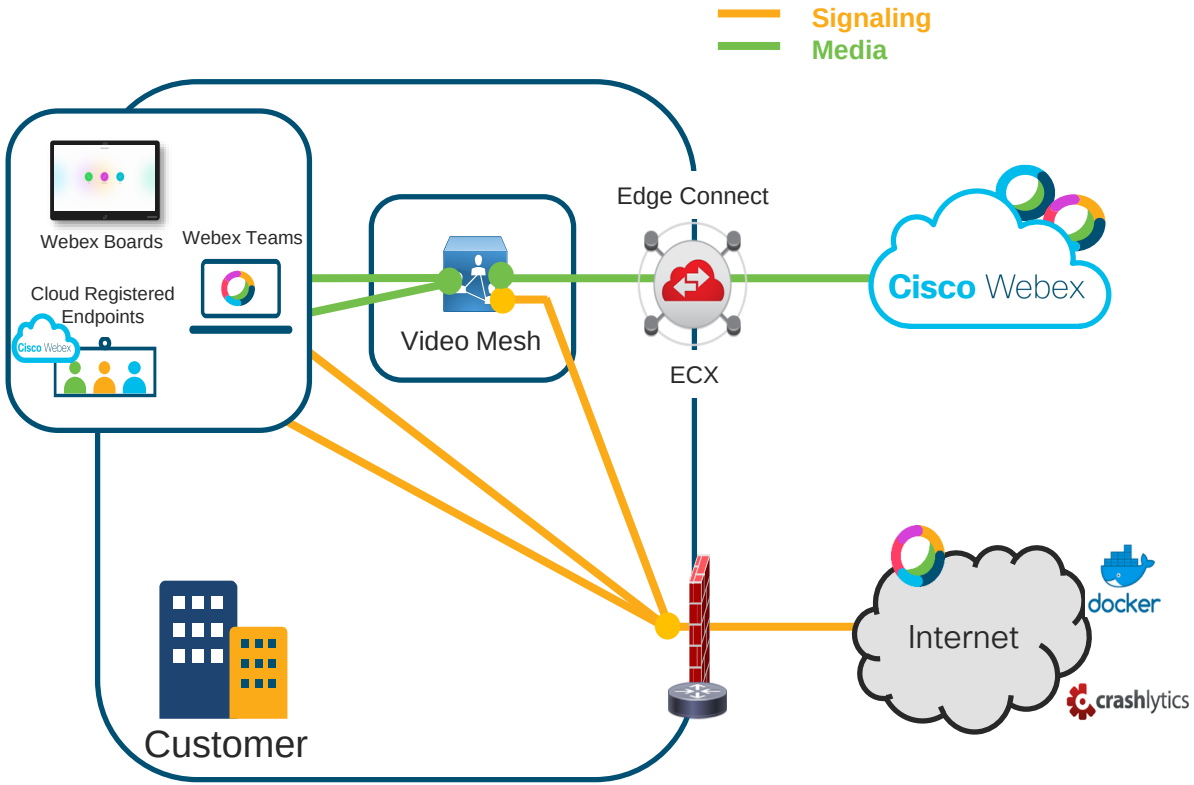
Webex Teams, Board and Endpoint's Media

Video Mesh Cascade Media

Public Internet

Webex Teams, Board and Endpoint's Signaling

Video Mesh Signaling



Unified CM integration – Video Mesh

Signaling and Media

Webex Enablement

Video Mesh

Edge Connect Peering Link

Webex Meetings App Signaling and Media

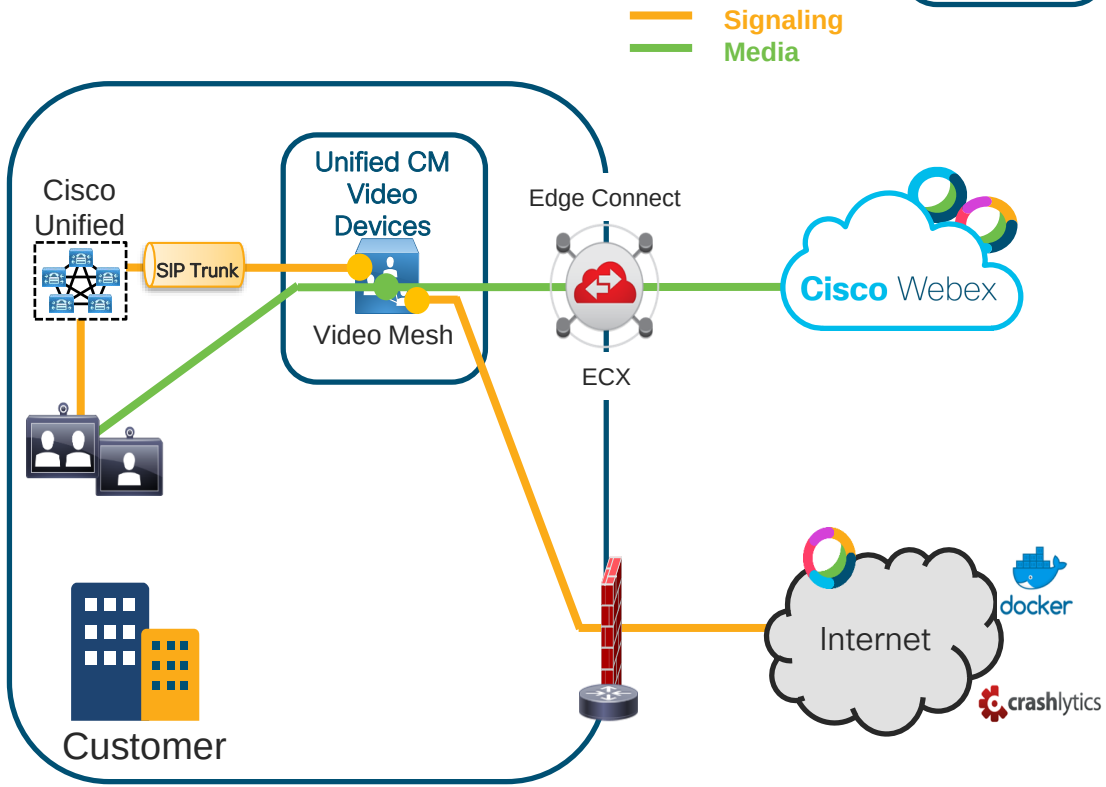
Webex Teams, Board and Endpoint's Media

Video Mesh Cascade Media

Public Internet

Webex Teams, Board and Endpoint's Signaling

Video Mesh Signaling



cisco Live!

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

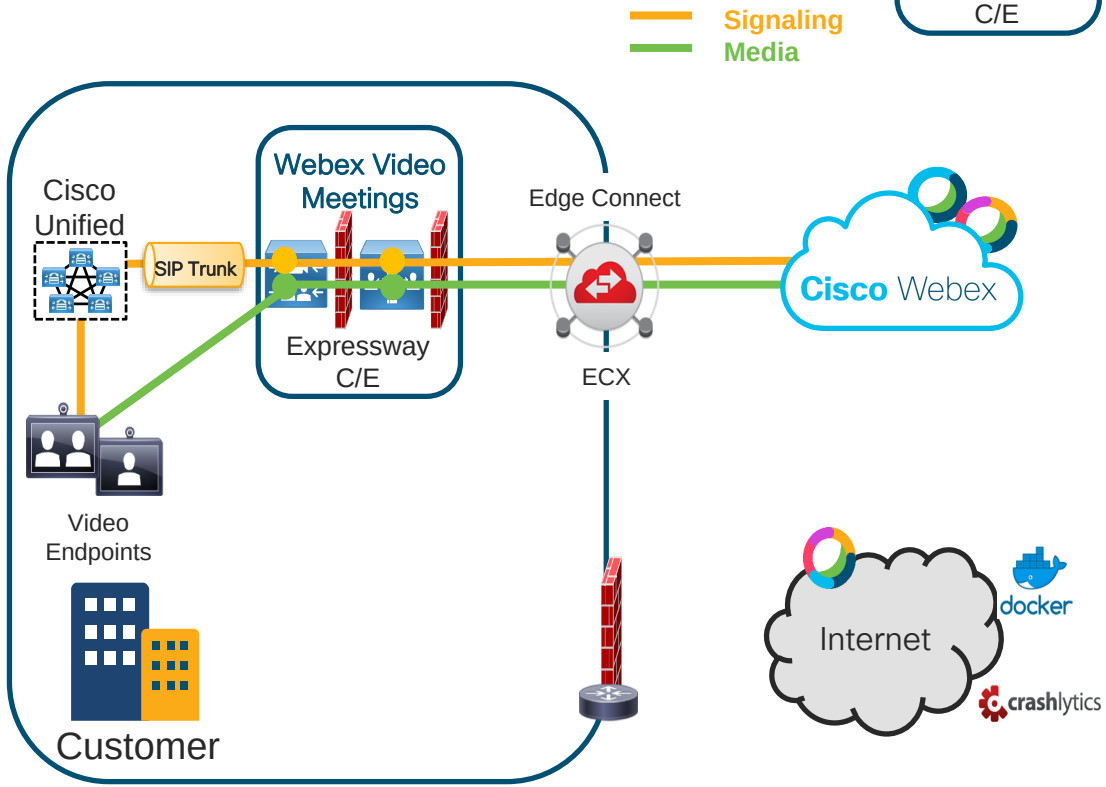
Video Mesh Cascade Media

Expressway Signaling and Media

Public Internet

Webex Teams, Board and Endpoint's Signaling

Video Mesh Signaling



Unified CM Integration – Webex Edge Audio

Edge Connect Peering Link

Webex Meetings App Signaling and Media

Webex Teams, Board and Endpoint's Media

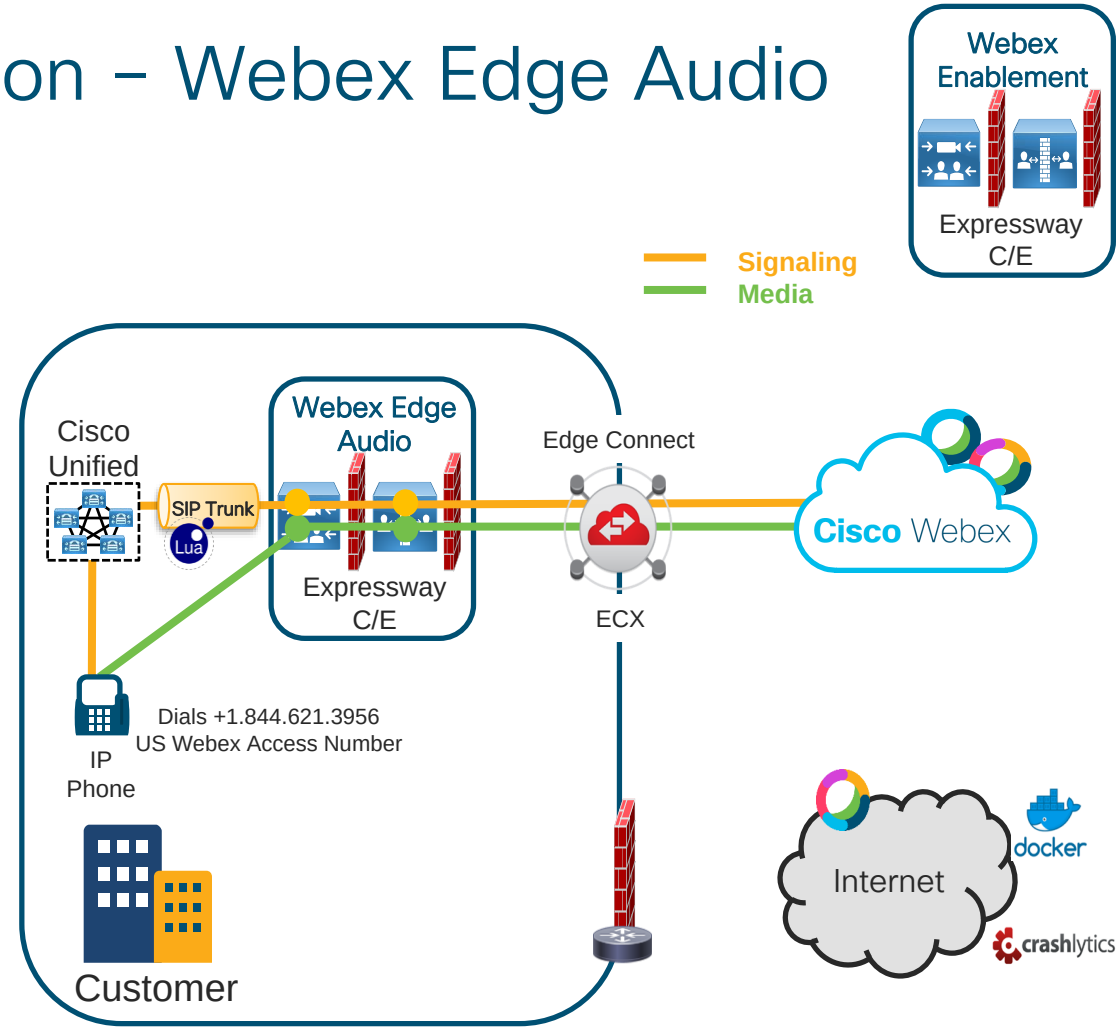
Video Mesh Cascade Media

Expressway Signaling and Media

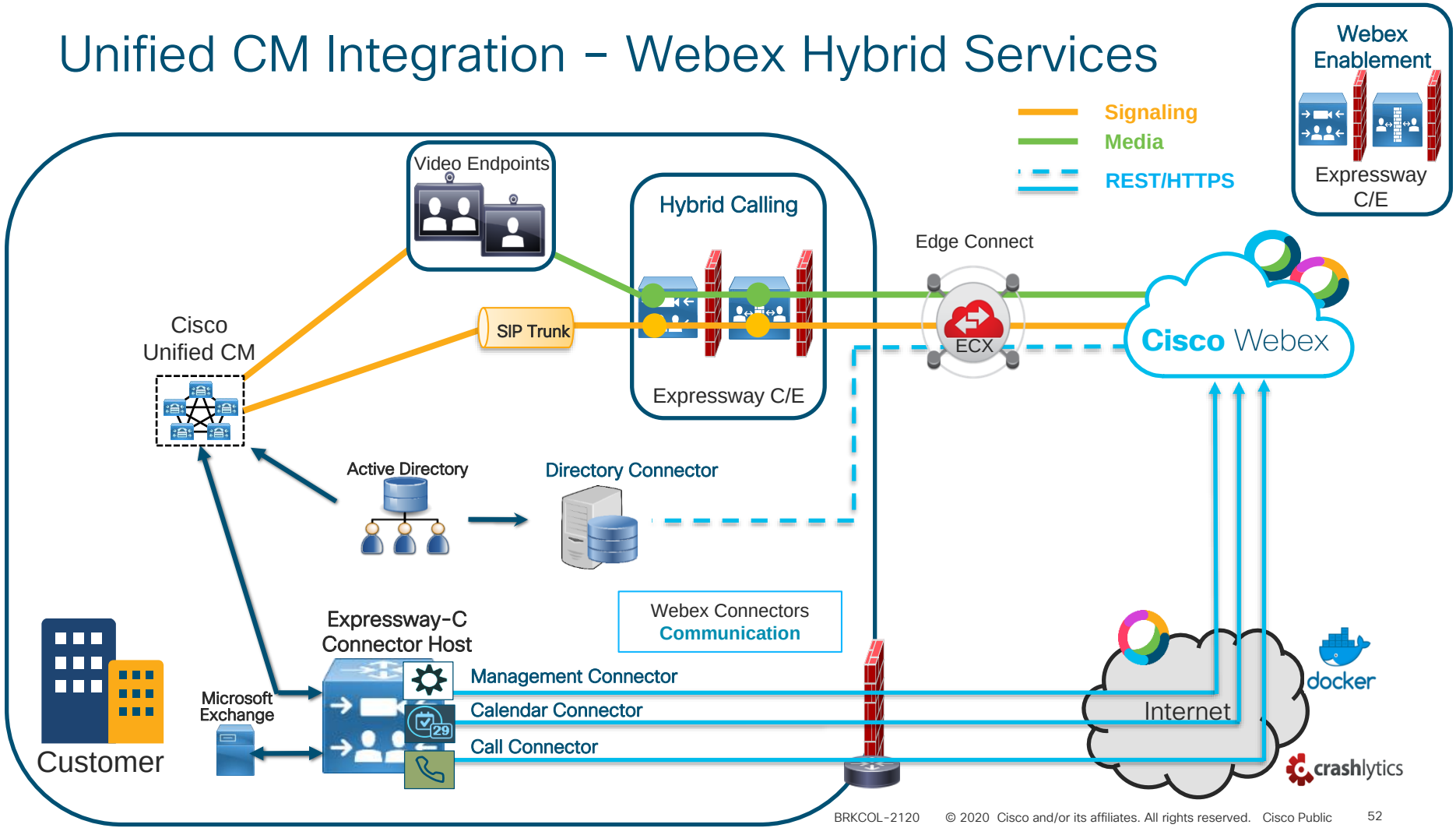
Public Internet

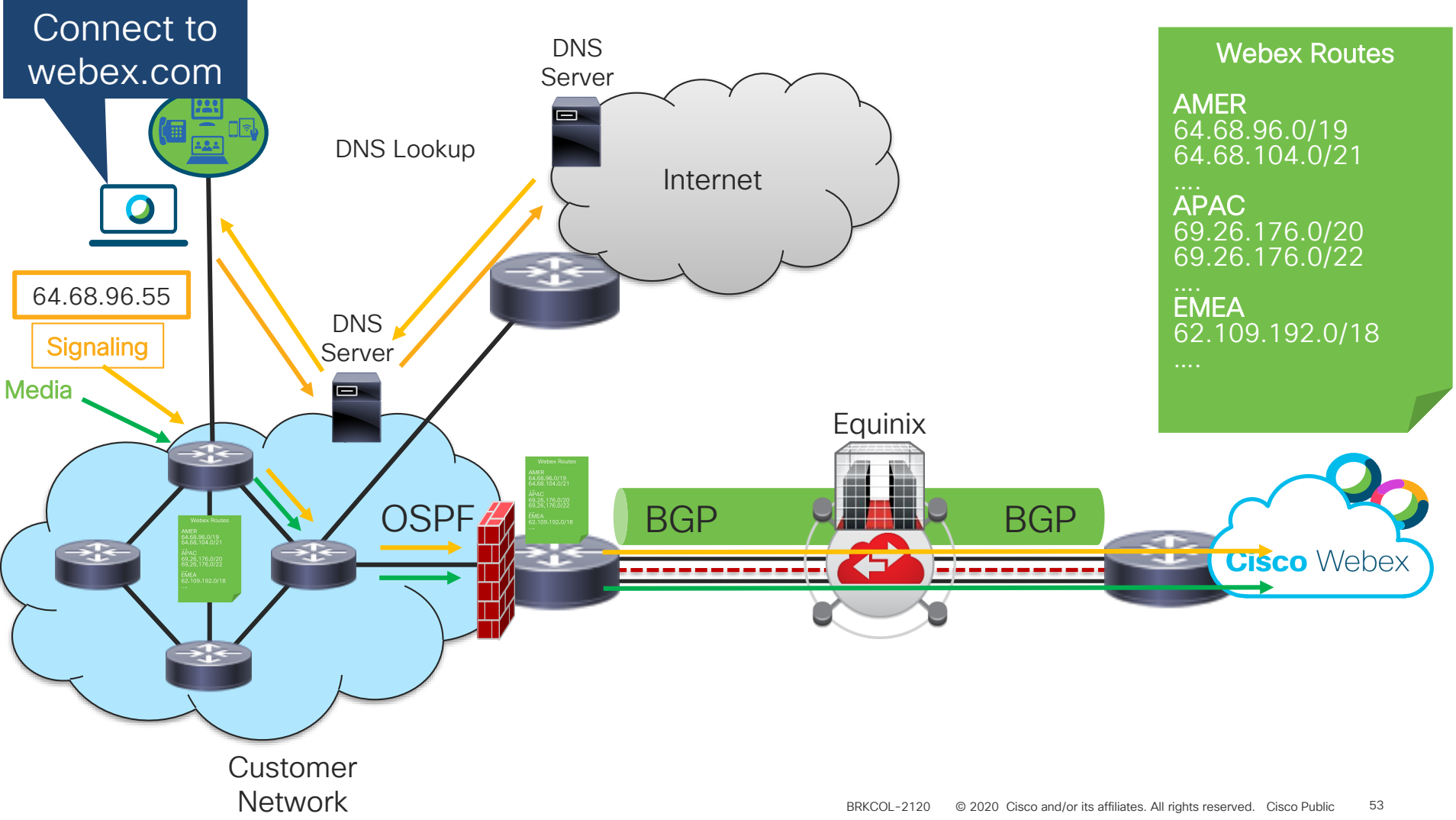
Webex Teams, Board and Endpoint's Signaling

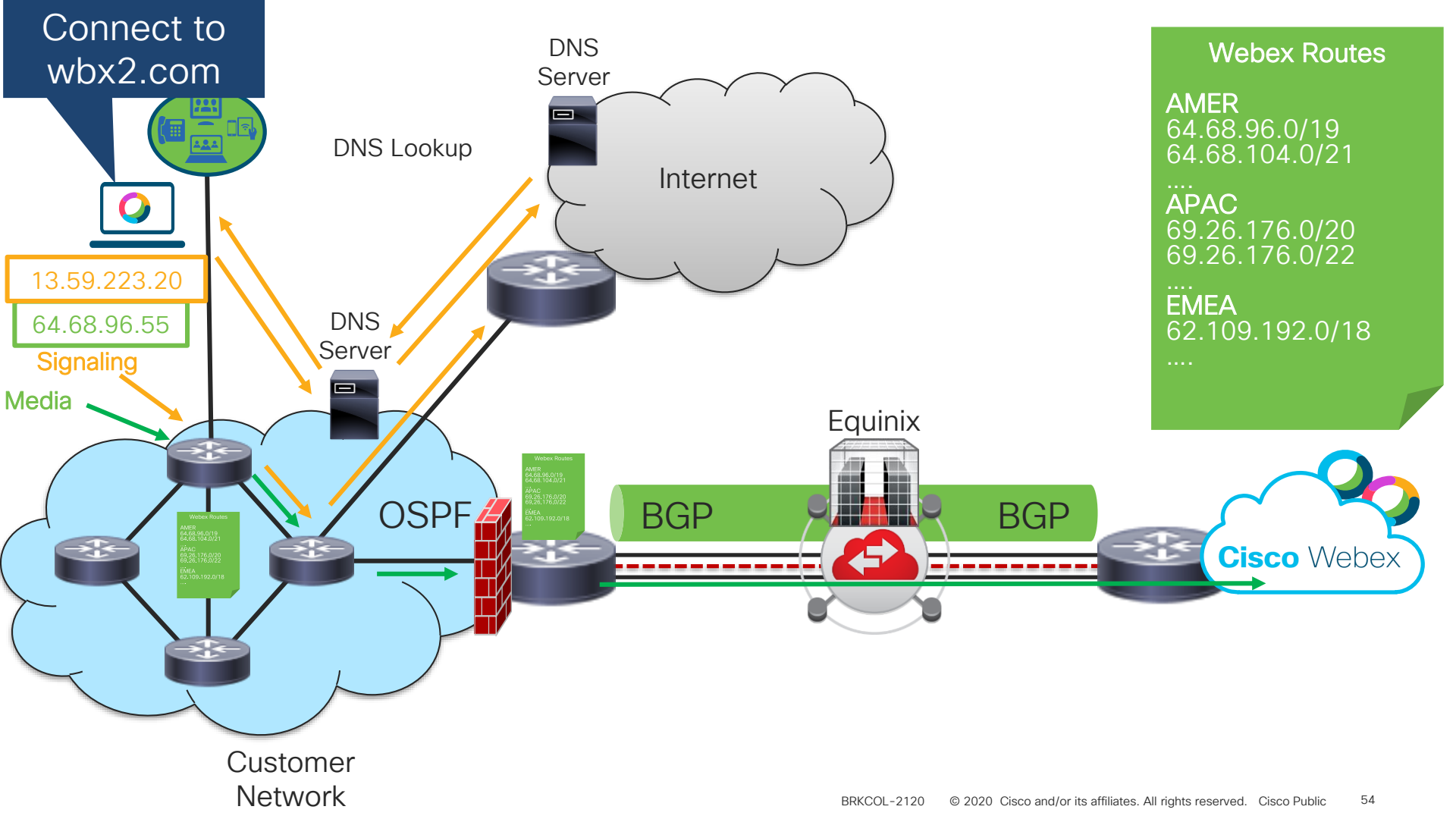
Video Mesh Signaling



Unified CM Integration – Webex Hybrid Services







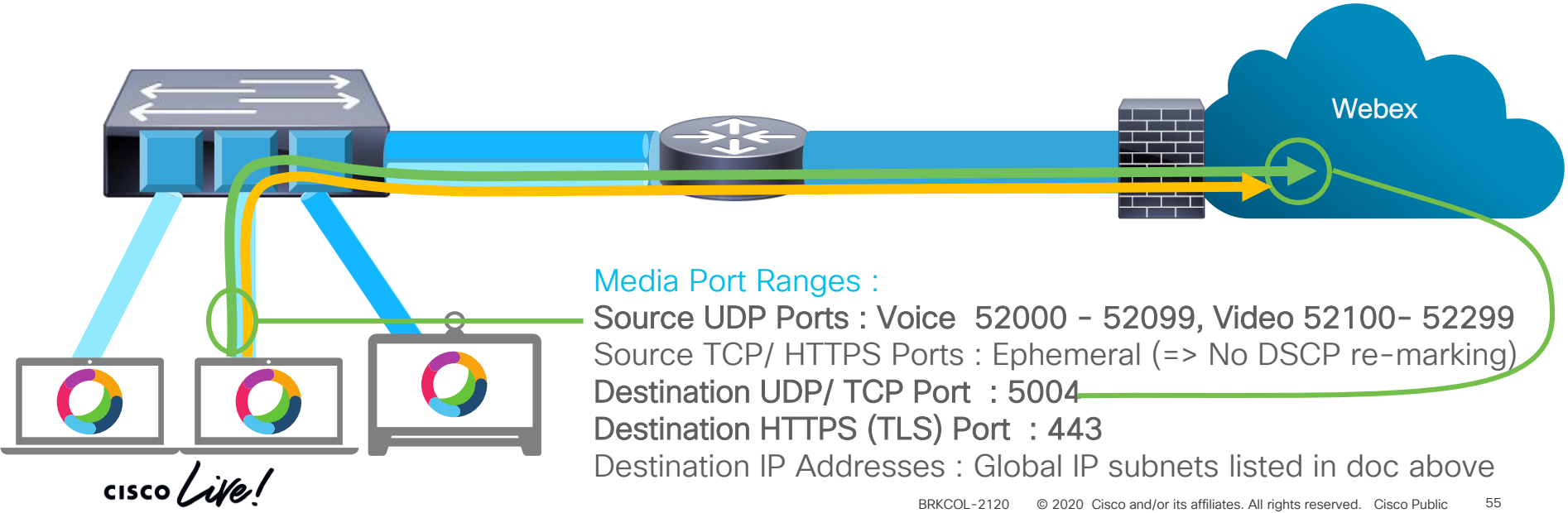
Connecting to Webex through Enterprise Firewalls: Webex Teams Apps and Devices

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

cisco Live!

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.

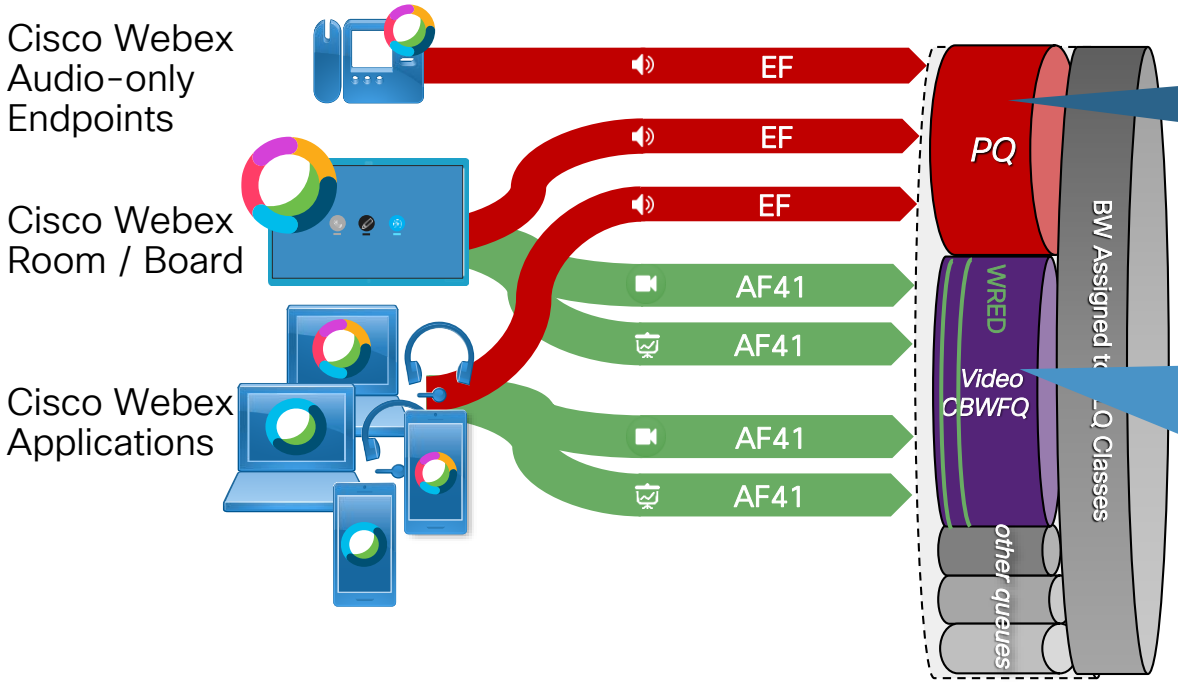
Internet access required

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

QoS Marking for Webex Media

Cisco Webex Teams Media

Assigning Cisco Webex Teams Media Traffic To Queues



Audio traffic marked PHB EF / DSCP 46 mapped to priority queue

Video traffic marked PHB AF41 / DSCP 34 mapped to a class-based weighted fair queue with DSCP-based WRED

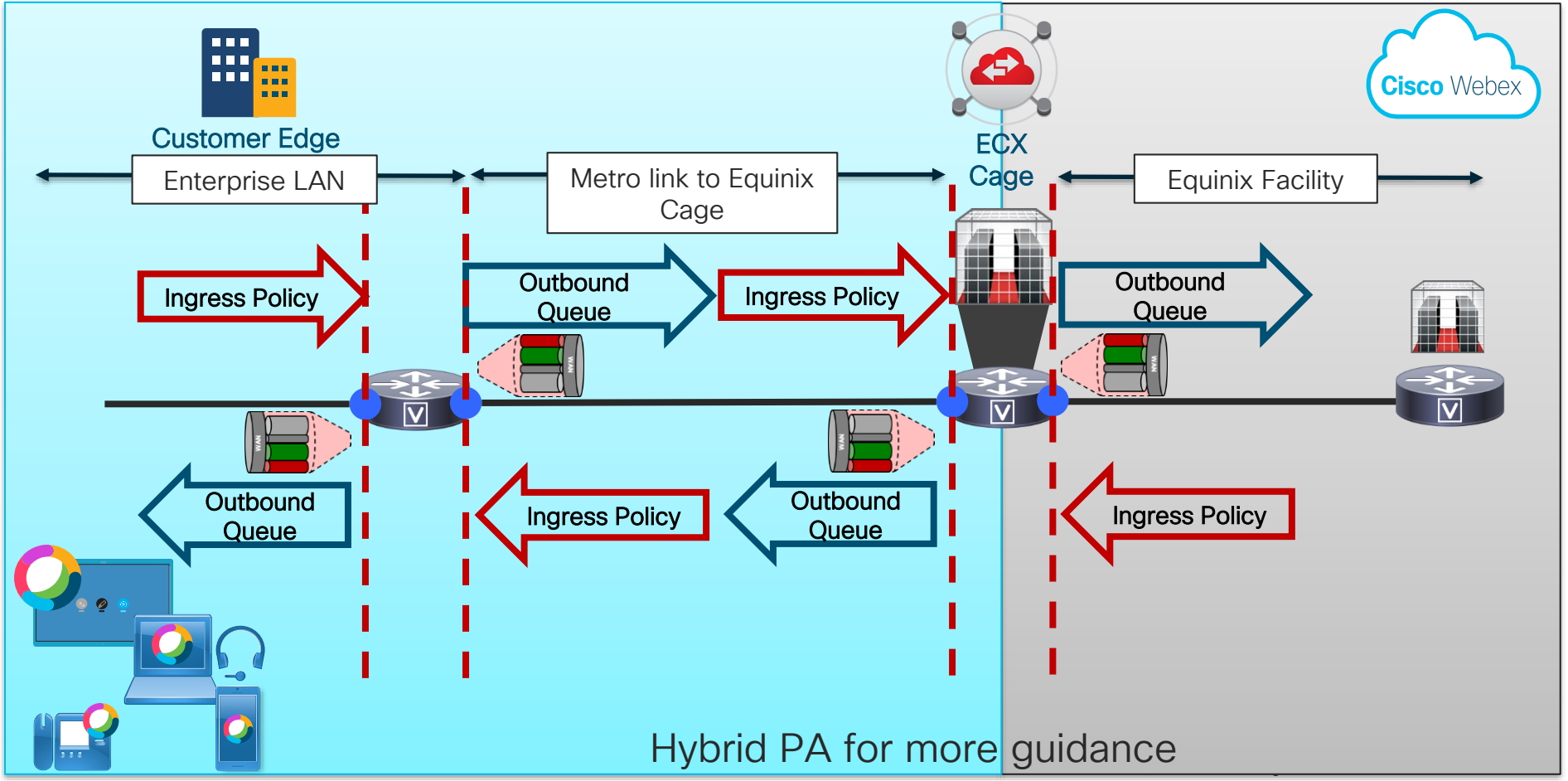
Cisco Webex Teams Media

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)

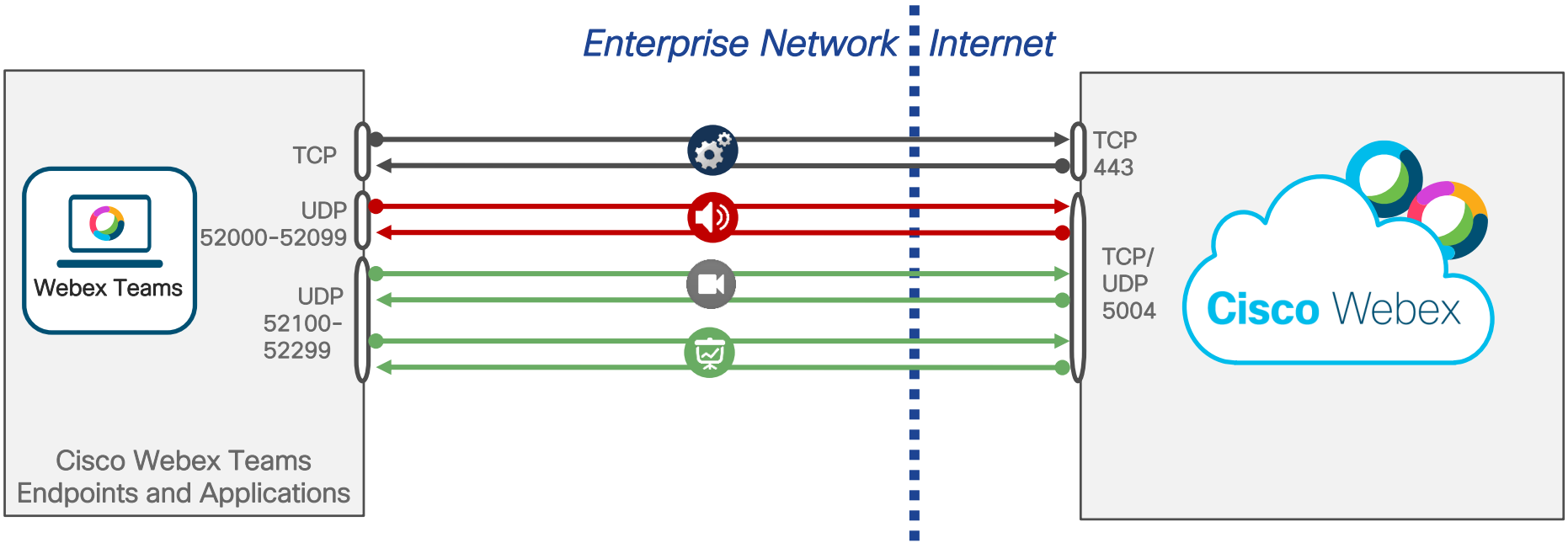
Source IP	Destination IP	Source UDP Ports	Destination UDP Ports	Recommended DSCP	Media Type
Cisco Webex Meetings Application	Webex Cloud	Ephemeral	9000	AF41	Audio / Video

Webex Meetings App

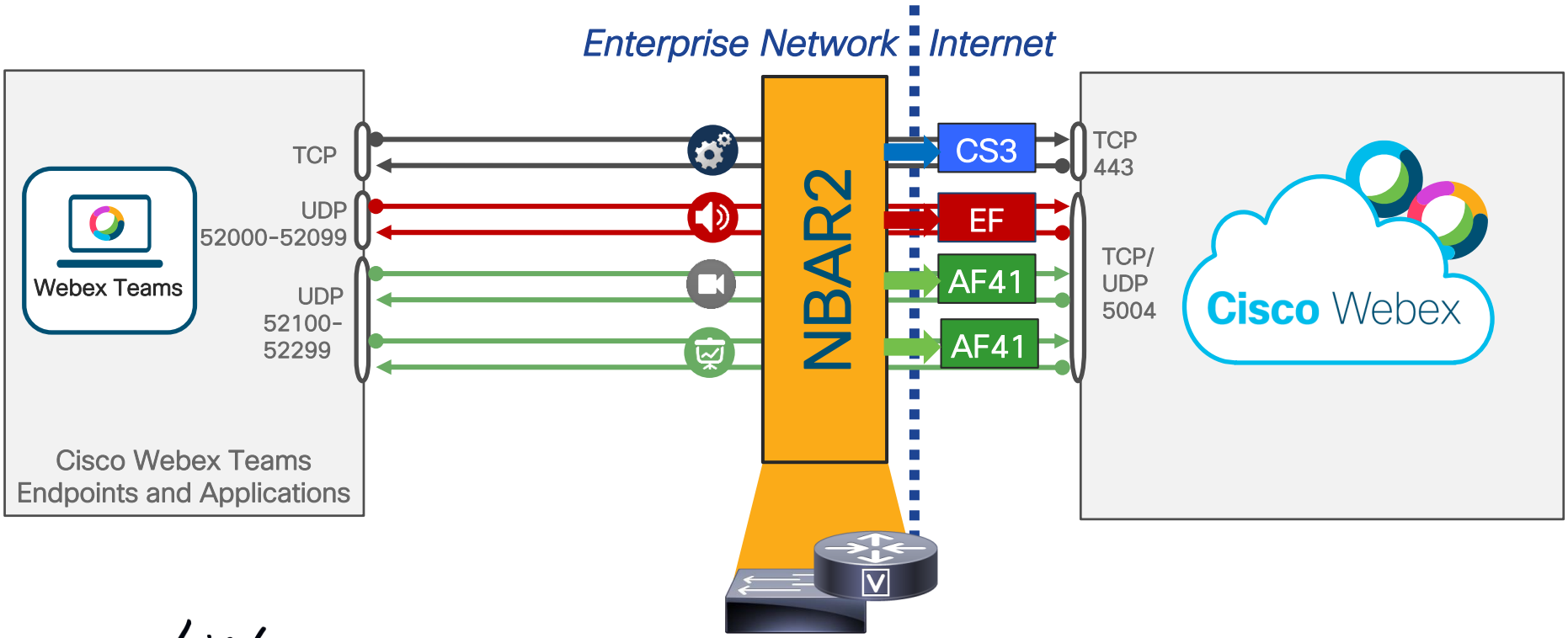
webex-audio = Webex audio streaming
webex-video = Webex video streaming
webex-app-sharing = Webex app sharing traffic
webex-meeting = Webex Signaling Traffic - (non-media – not port based)

NBAR2

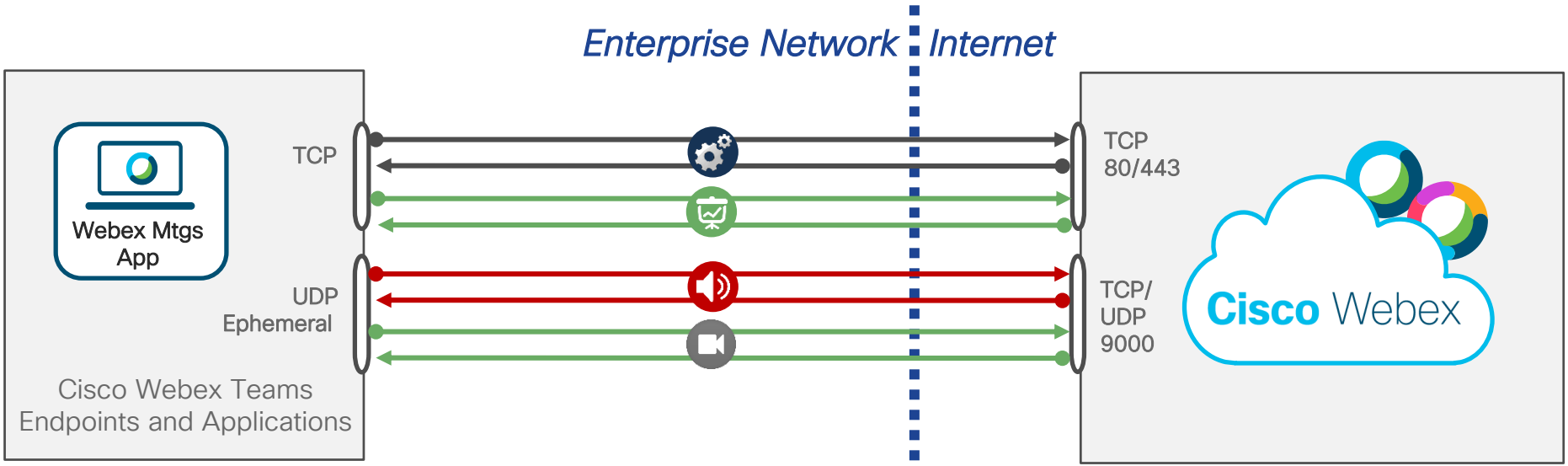
Port Usage Today – Webex Teams



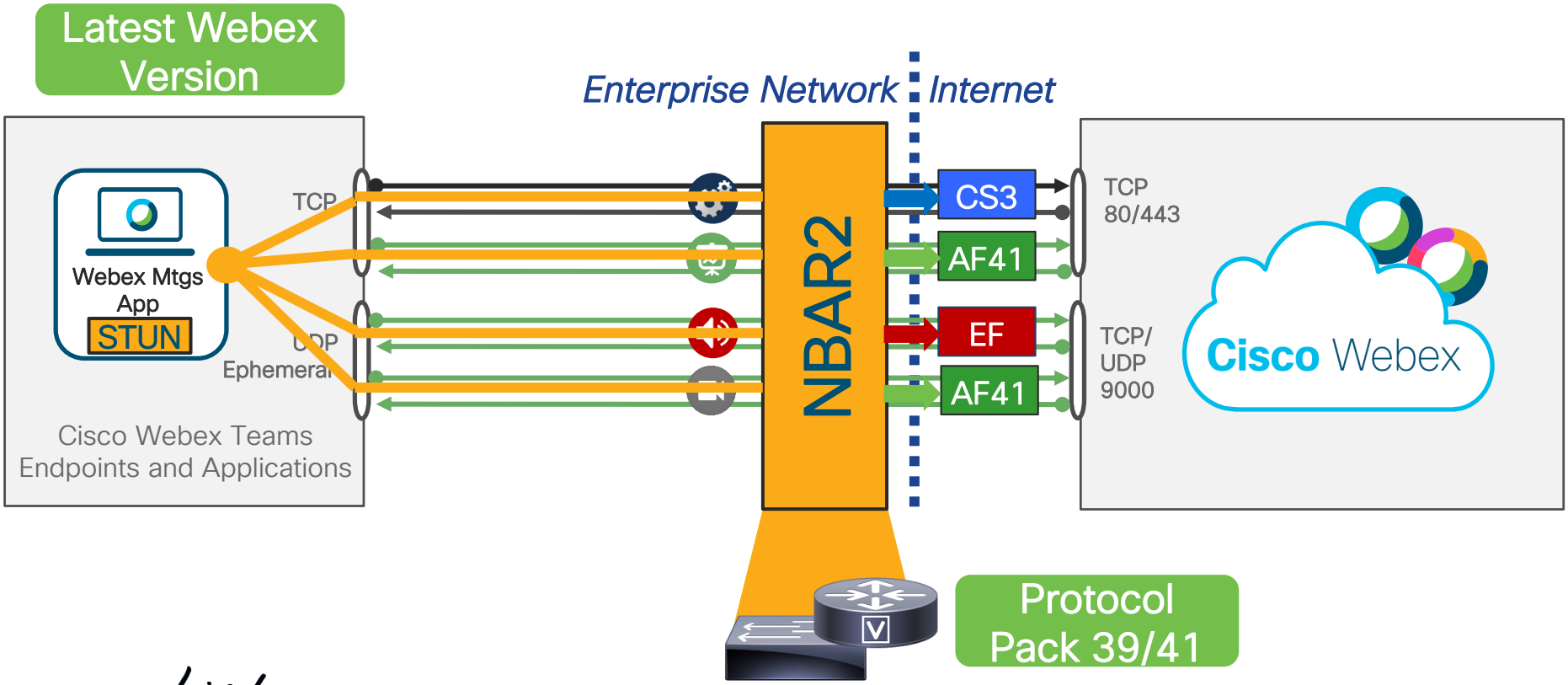
Port Usage Today – Webex Teams



Port Usage Today – Webex Meetings App

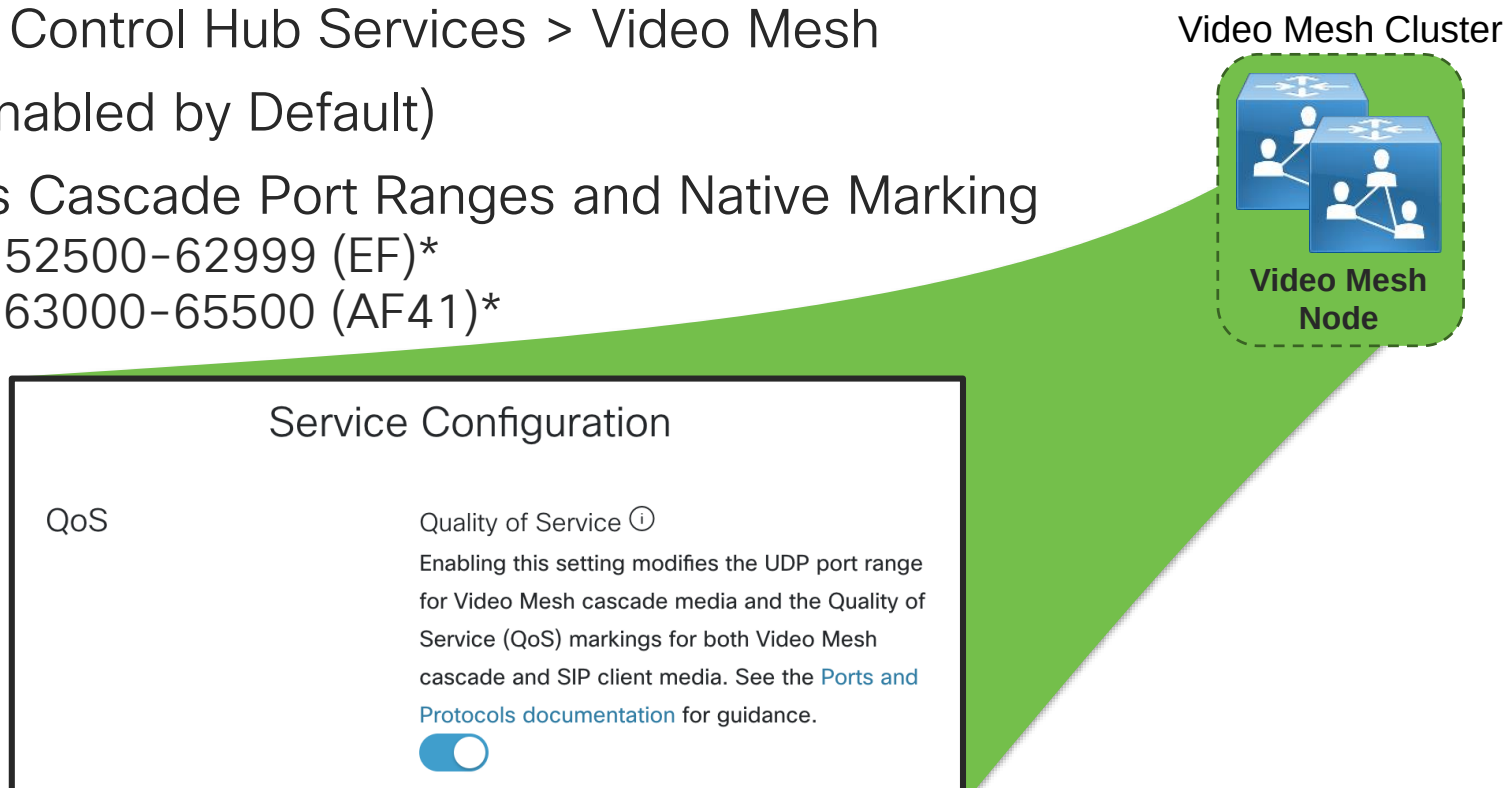


Port Usage Today – Webex Meetings App



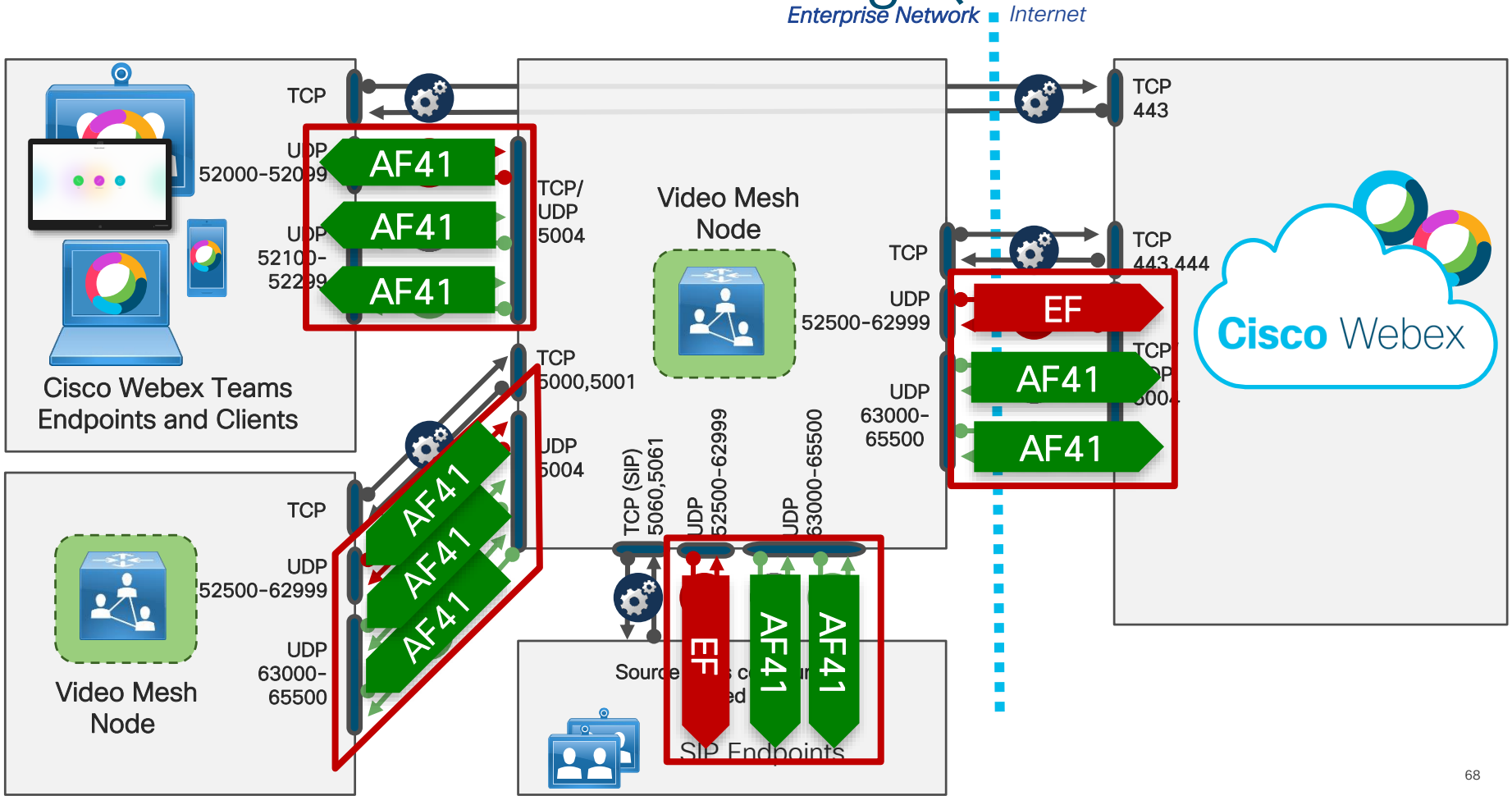
Video Mesh Node – Ports

- 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)*

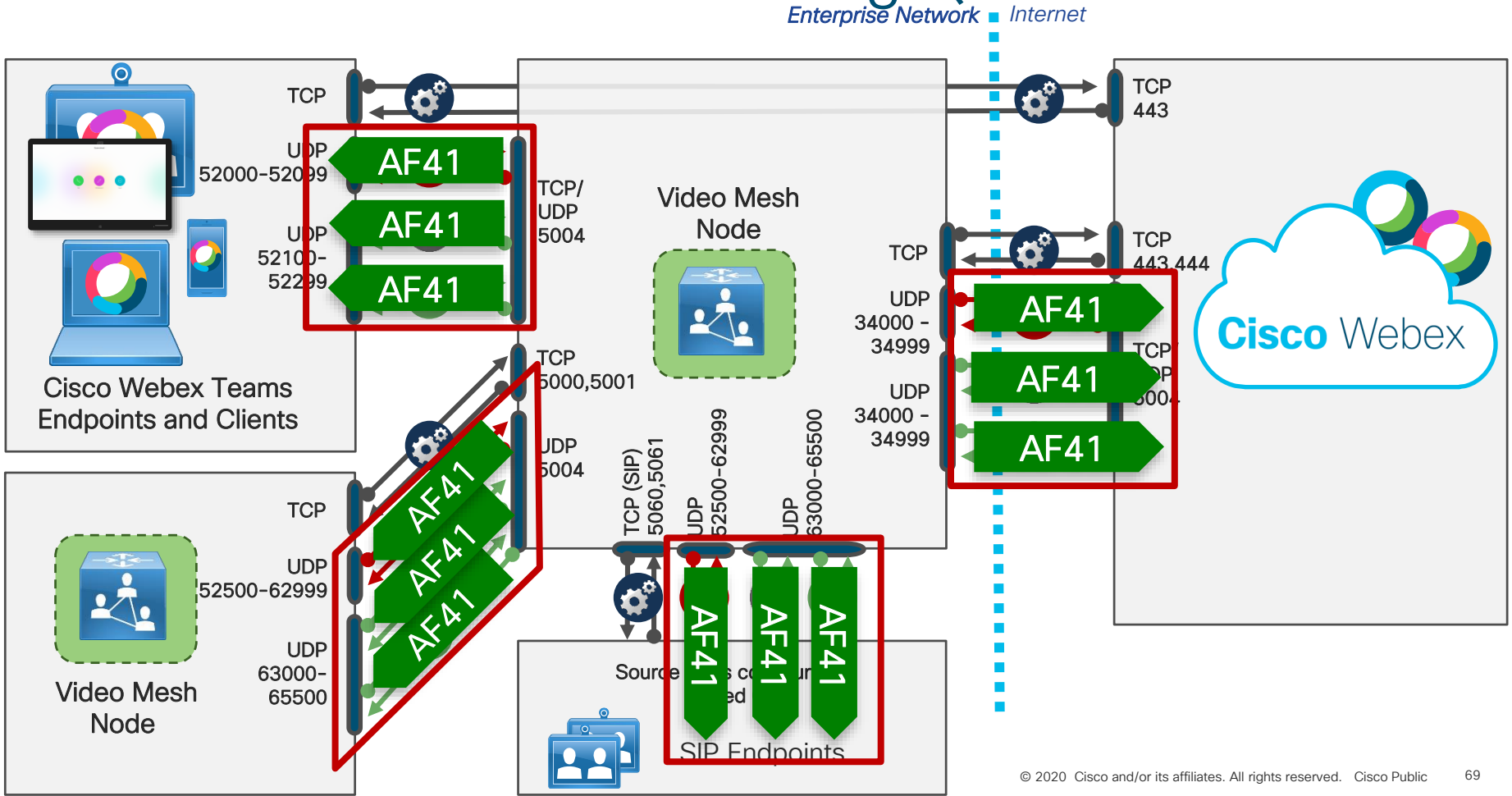


* When disabled changes the source ports that are used for audio, video, and content sharing from the Video Mesh node to the range 34000 to 34999

Video Mesh – Native Marking QoS Enabled



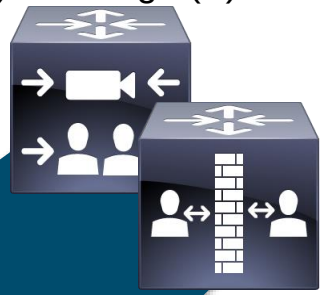
Video Mesh – Native Marking QoS Disabled

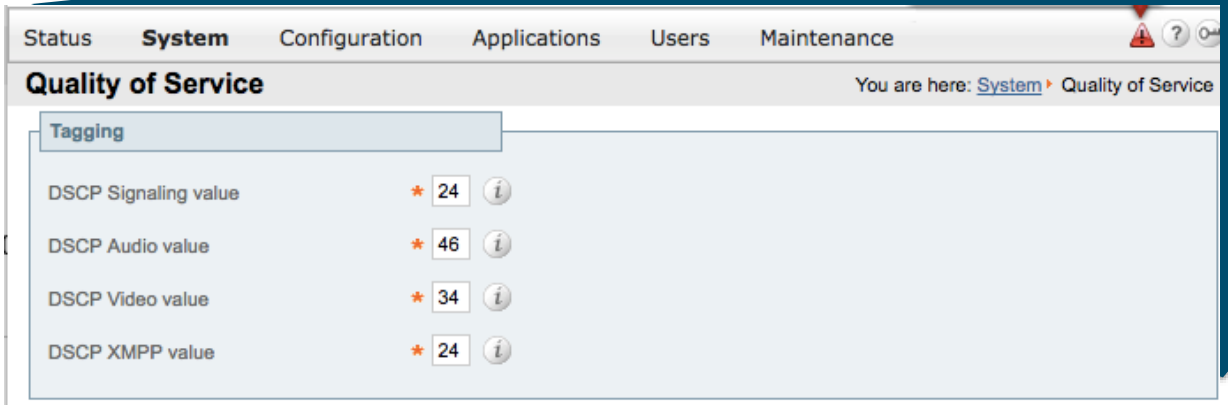


Expressway

- 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

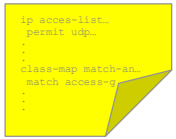
Cisco Expressway Core (C) and Edge (E)

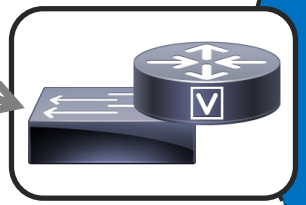




Webex Ingress QoS Policy

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)

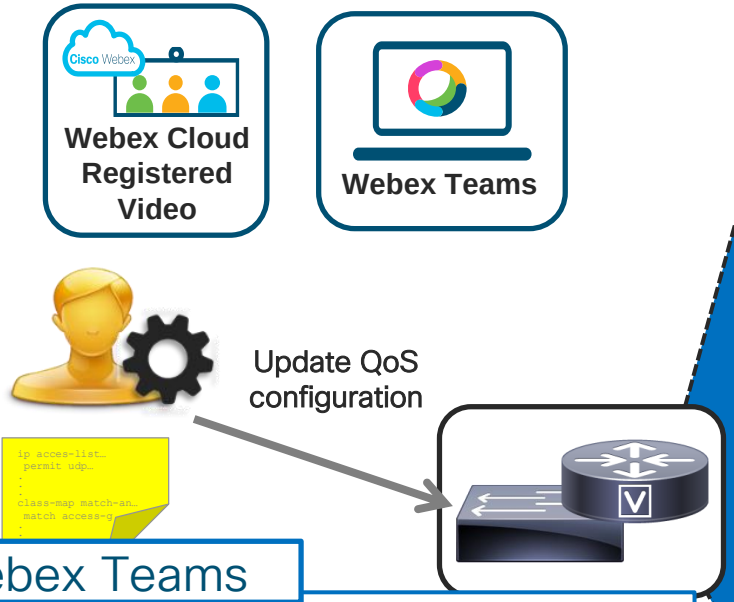
NBAR2

```
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
  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
```

Webex Ingress QoS Policy



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…)

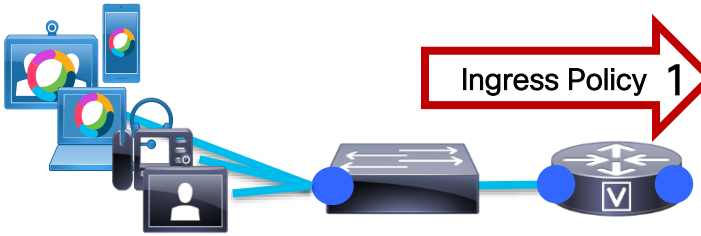
NBAR2

```
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 protocol cisco-spark-audio
  match access-group name QOS_VOICE
  match access-group name QOS_WEBEX_TEAMS_AUDIO

class-map match-any PRIORITIZED_VIDEO
  match protocol cisco-spark-video
  match access-group name QOS_PRIORITIZED_VIDEO
  match access-group name QOS_WEBEX_TEAMS_VIDEO
```

WAN Ingress QoS Marking Policy



Reference

Ingress Policy 1

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

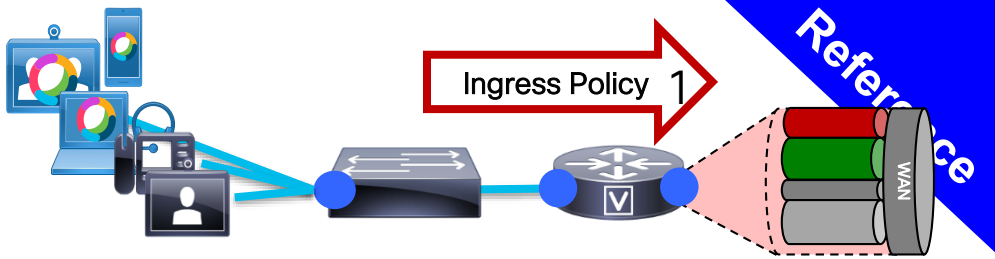
2

```
! 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 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
```



Egress Policy 6

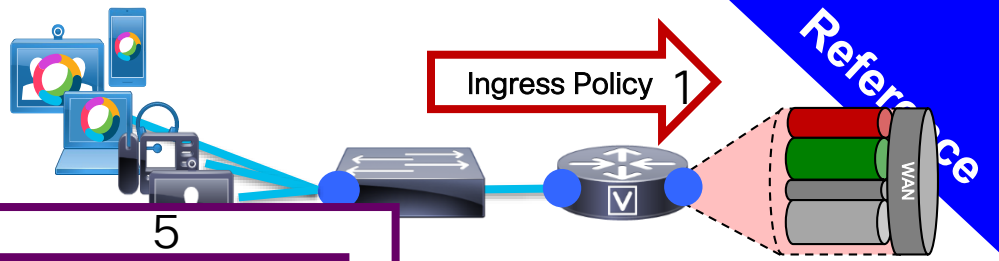
```
! This section configures the classes
class-map match-any VOICE
 match webex-audio
 match access-group QOS_WEBEX_TEAMS_AUDIO
class-map match-any PRIORITIZED-VIDEO
 match webex-video
 match access-group QOS_WEBEX_TEAMS_VIDEO
class-map match-any SIGNALING
 match webex-meeting
 match cisco-spark
 match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

4

3

```
! 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
```



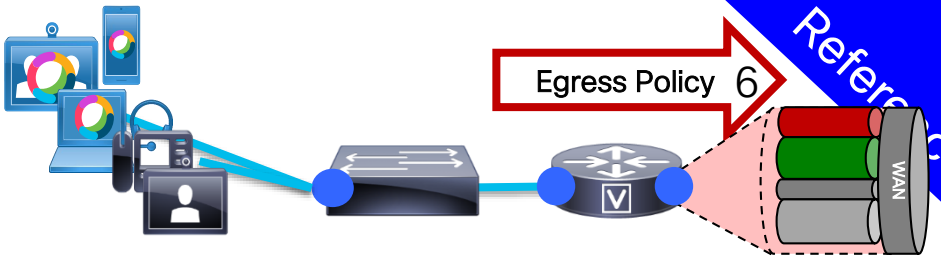

```
! This section configures the ACL's
ip access-list extended QOS_WEBEX_TEAMS_AUDIO
  permit udp any range 52000 to 52099 any 5004
  permit udp eq 5004 any range 52000 to 52099
ip access-list extended QOS_WEBEX_TEAMS_VIDEO
  permit udp any range 52100 52299 any 5004
  permit udp eq 5004 any range 52100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



Reference

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
```

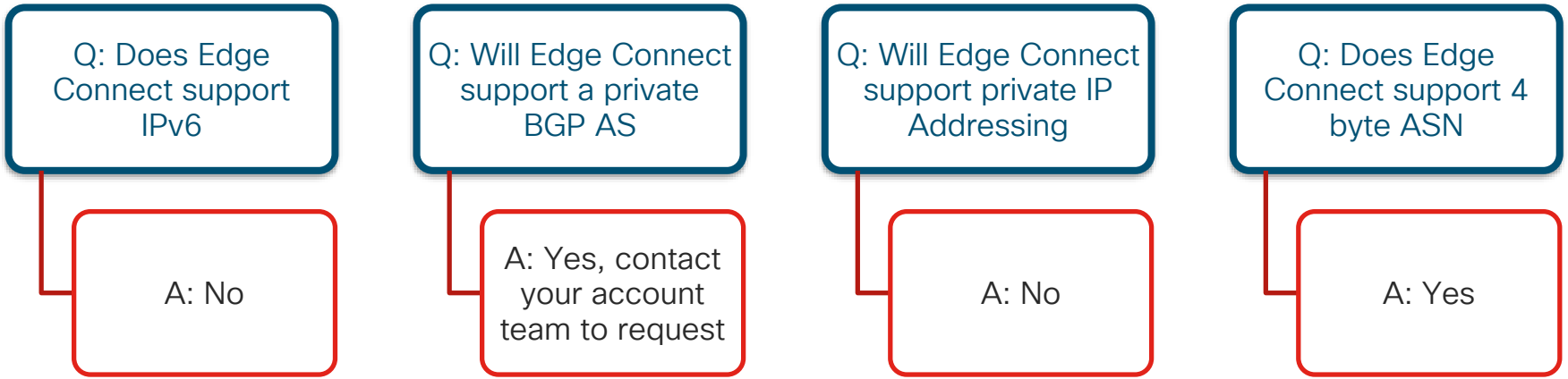
6.3

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



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

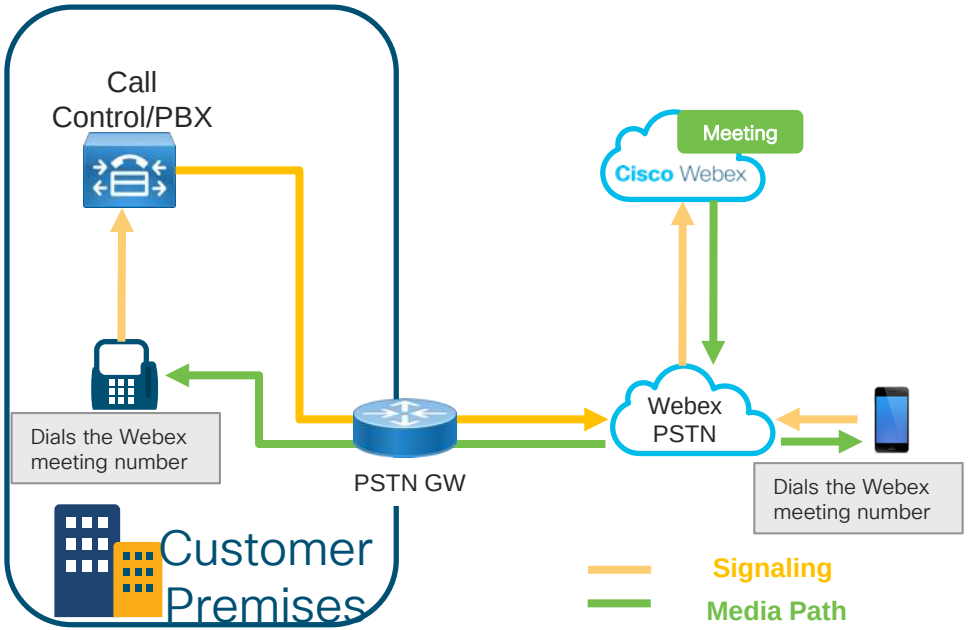
- http://lg.webex.com/lg/

Webex Edge Audio

Components of Webex Edge for Meetings

Cisco Webex PSTN Audio

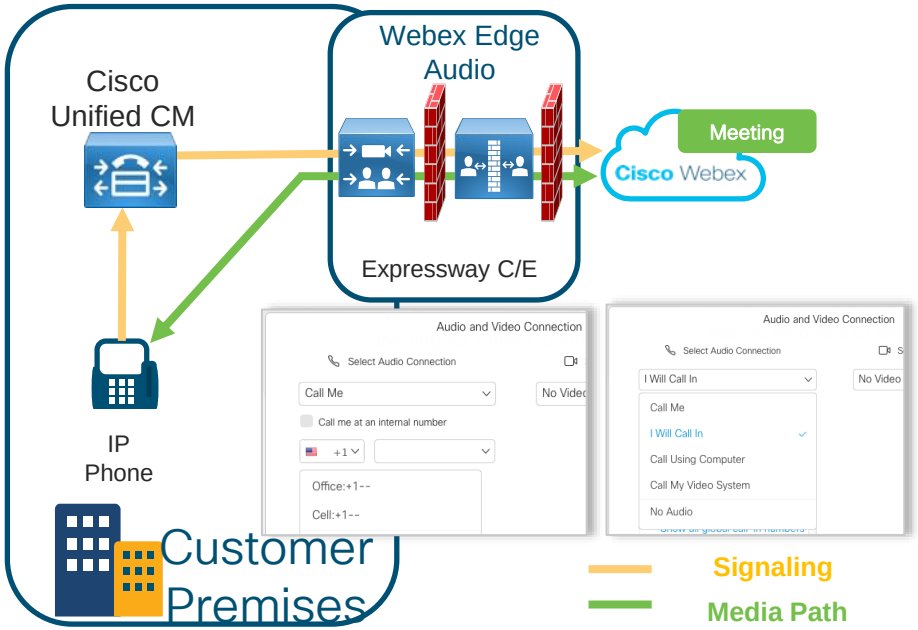
High level overview



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.

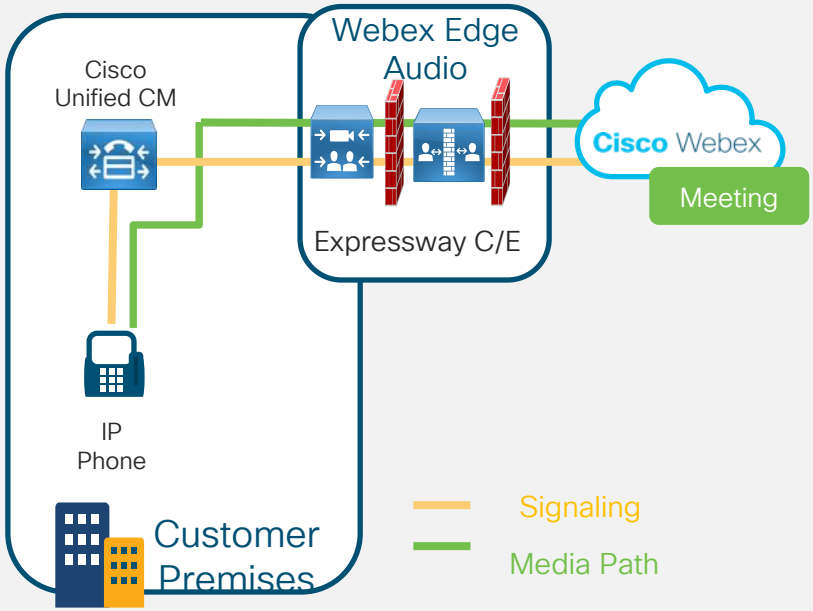
Cisco Webex Edge Audio

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

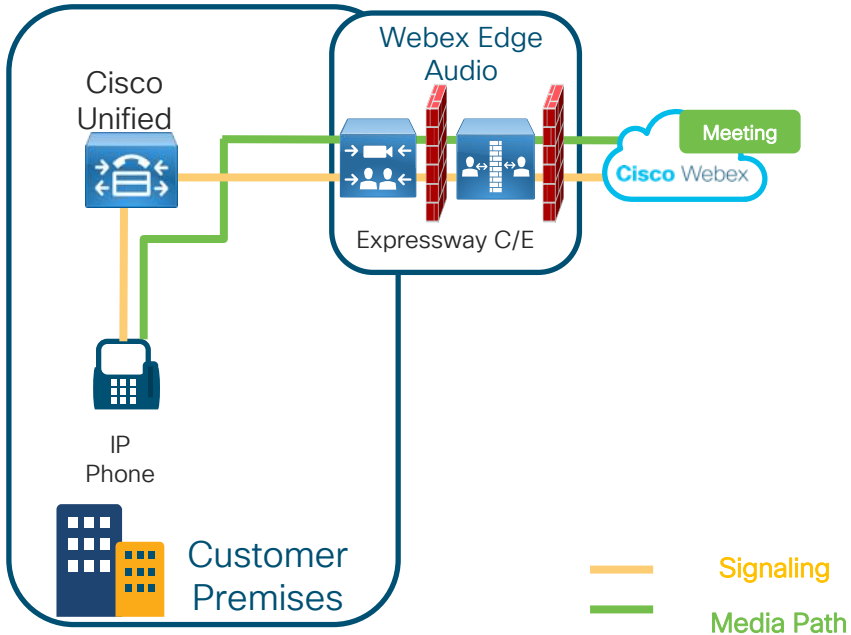


- Intelligent audio routing: integrating Webex with Unified CM
  - Creates end-to-end VoIP path for Unified CM registered devices (callback and dial-in)
  - Uses company's own PSTN for any other device (callback savings)
  - No SIP trunks or peering arrangements required
- Geo-country code configurable
- 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.

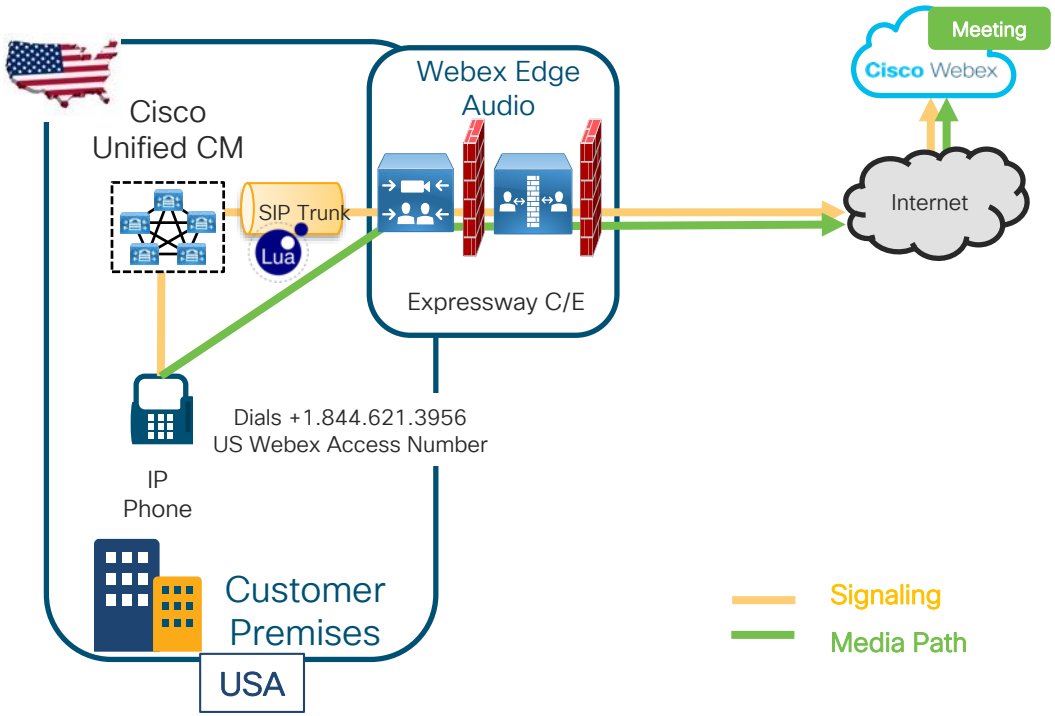
Webex site

- 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

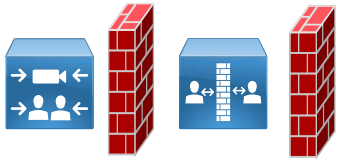
Best Practice



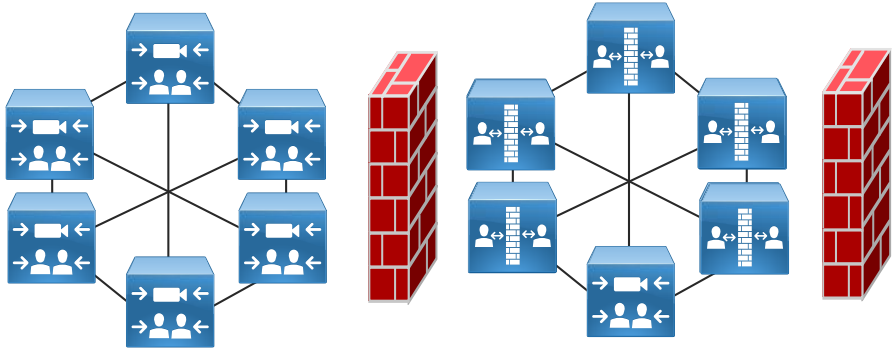
1. Make a new SIP trunk from CUCM to Expressway – C, do not use an existing trunk.
2. Create a new dedicated traversal zone between Expressway C and E for Edge Audio only, do not use an existing zone.
3. MRA and Edge Audio can co-reside on the same Expressway C/E pair.
4. Edge Audio is based on +E.164 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



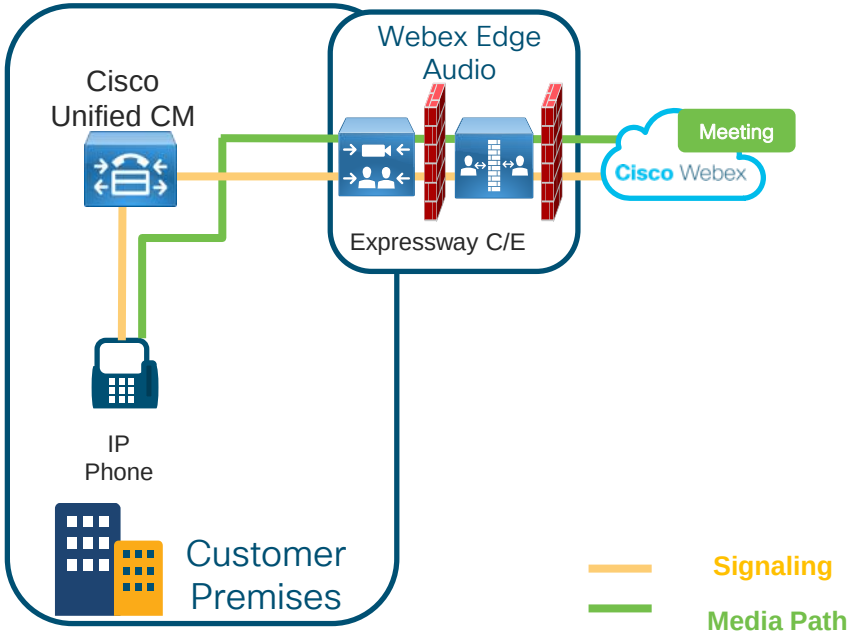
Expressway – C
6 node cluster

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

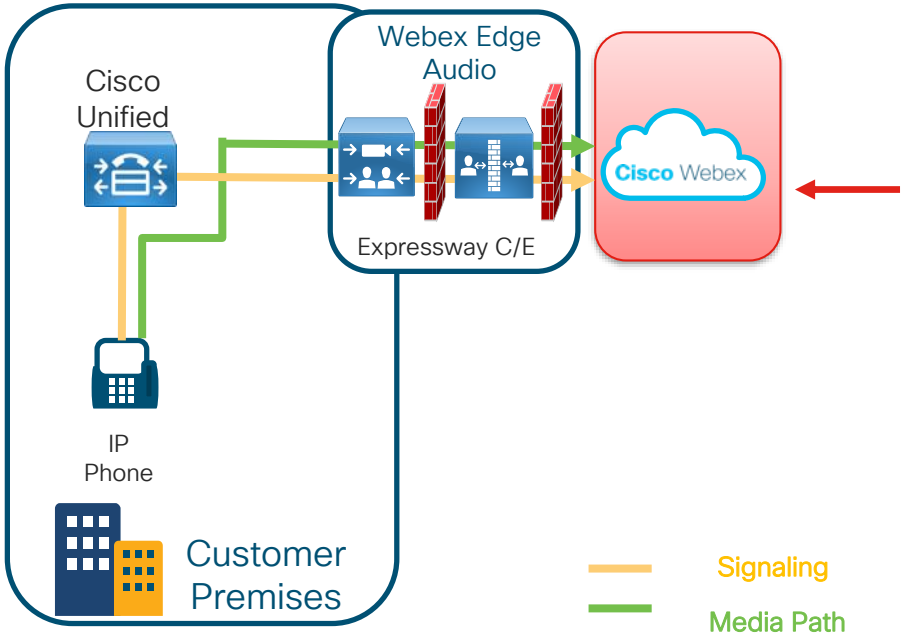


Overview of Webex Edge Audio Configuration Steps:

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

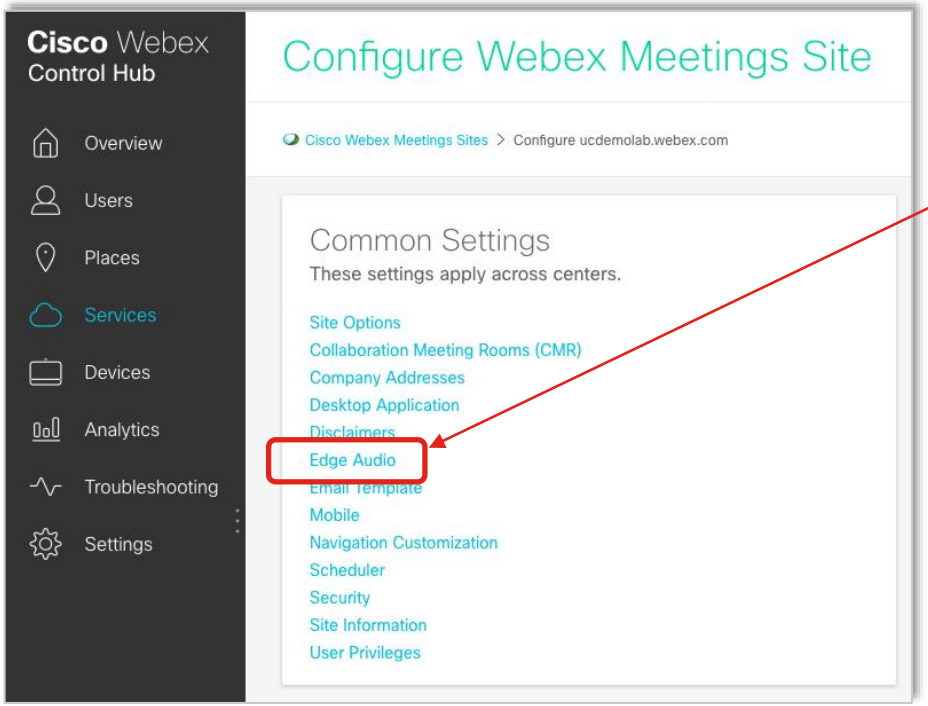


Overview of Webex Edge Audio Configuration Steps:

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

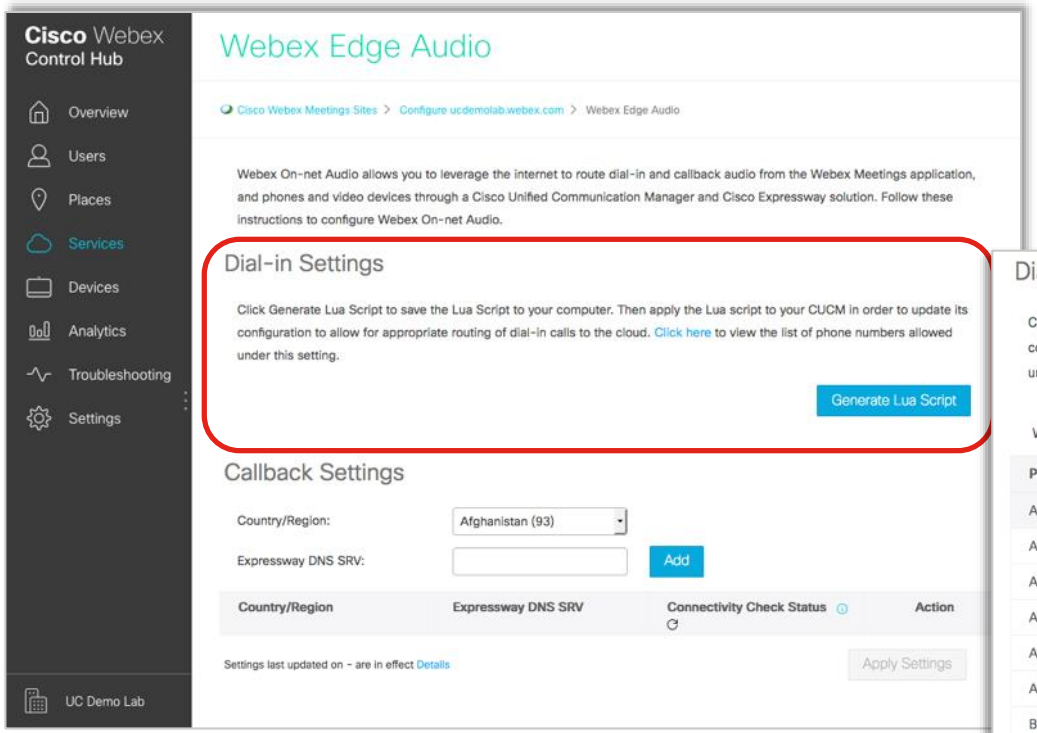


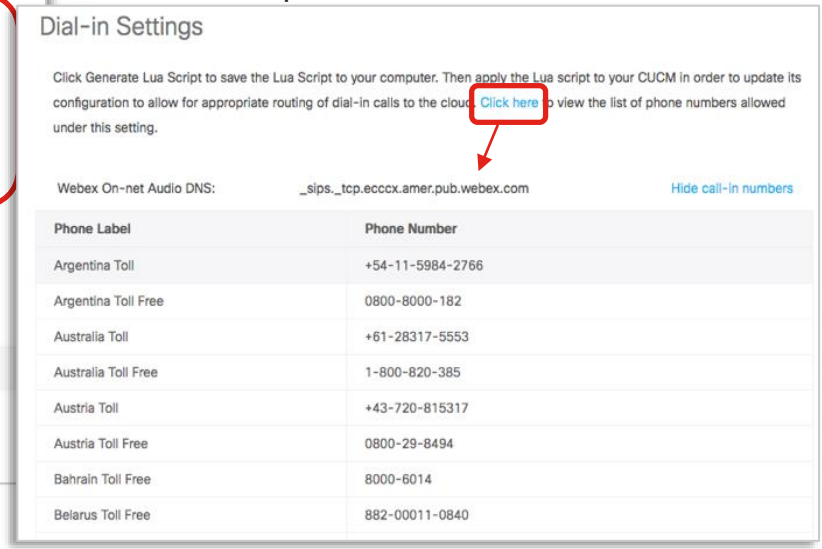
Webex Edge Audio Call-in Set Up Steps:

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

Cisco Webex Edge Audio

Architecture configuration – Dial in



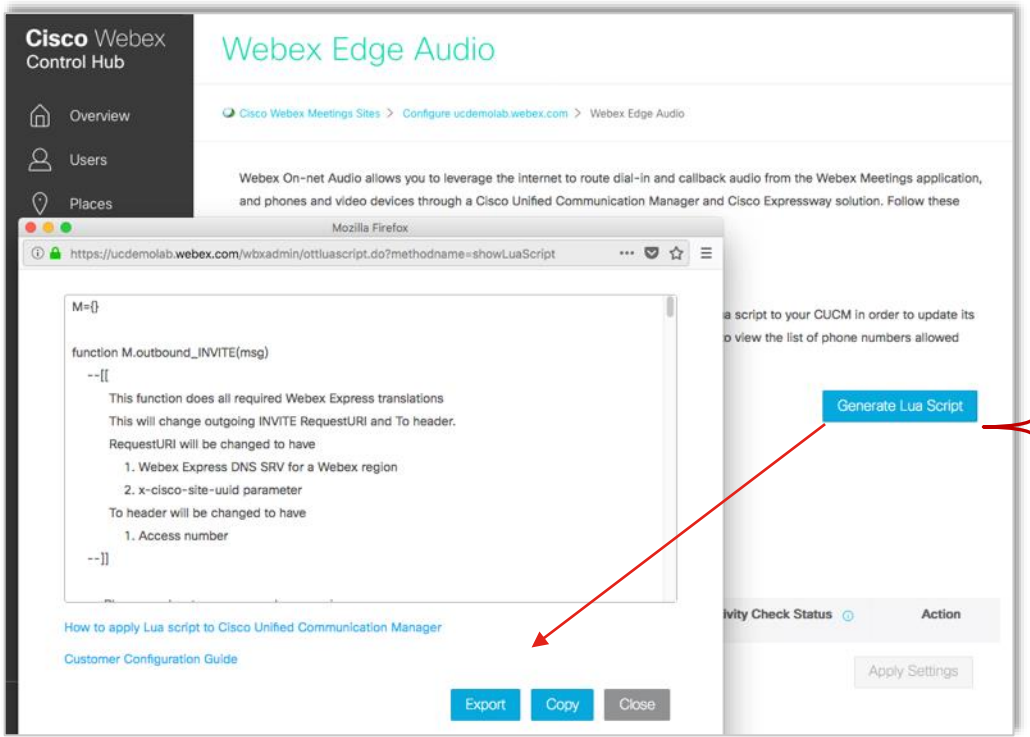


Webex Edge Audio Call-in Set Up Steps:

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

Cisco Webex Edge Audio

Architecture configuration – Dial in



Webex Edge Audio Call-in Set Up Steps:

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

Lua Script

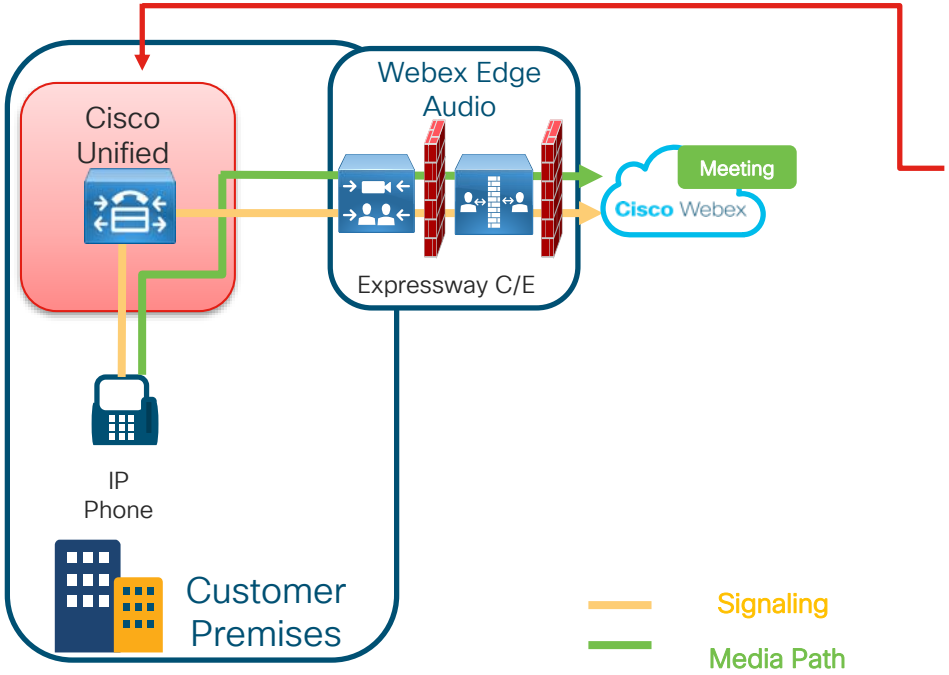
Changes outgoing INVITE RequestURI and To header

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

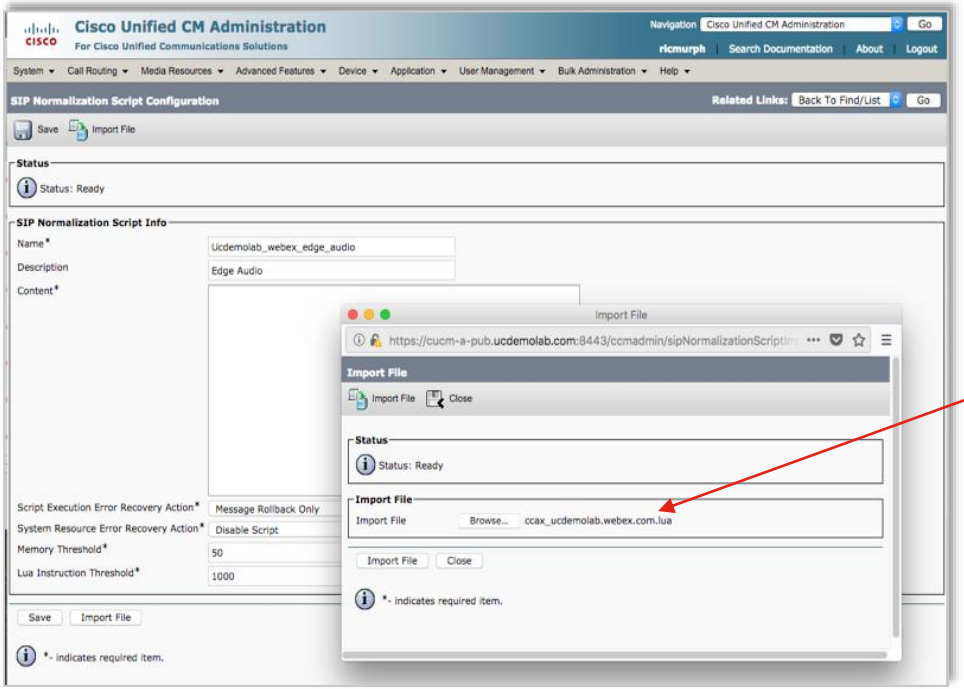


Webex Edge Audio Call-in Set Up Steps:

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



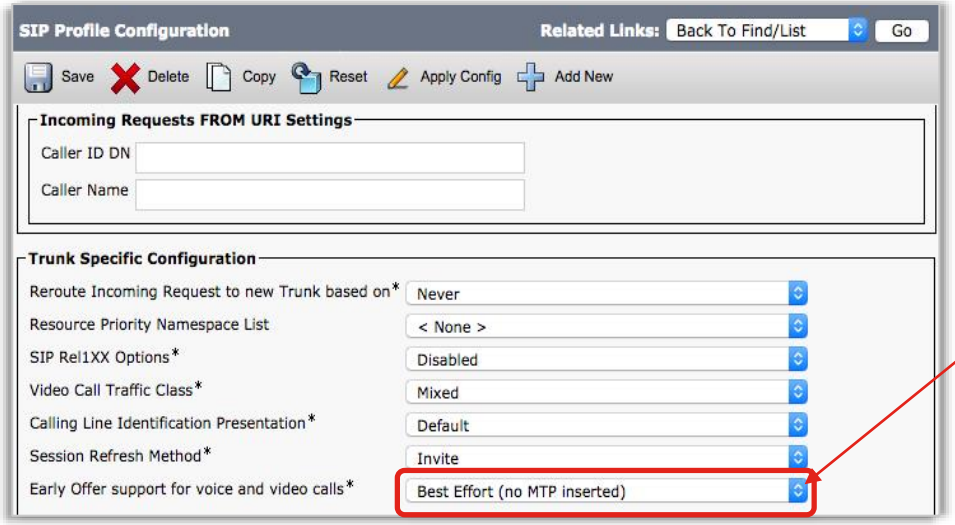
Webex Edge Audio Call-in Set Up Steps:

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



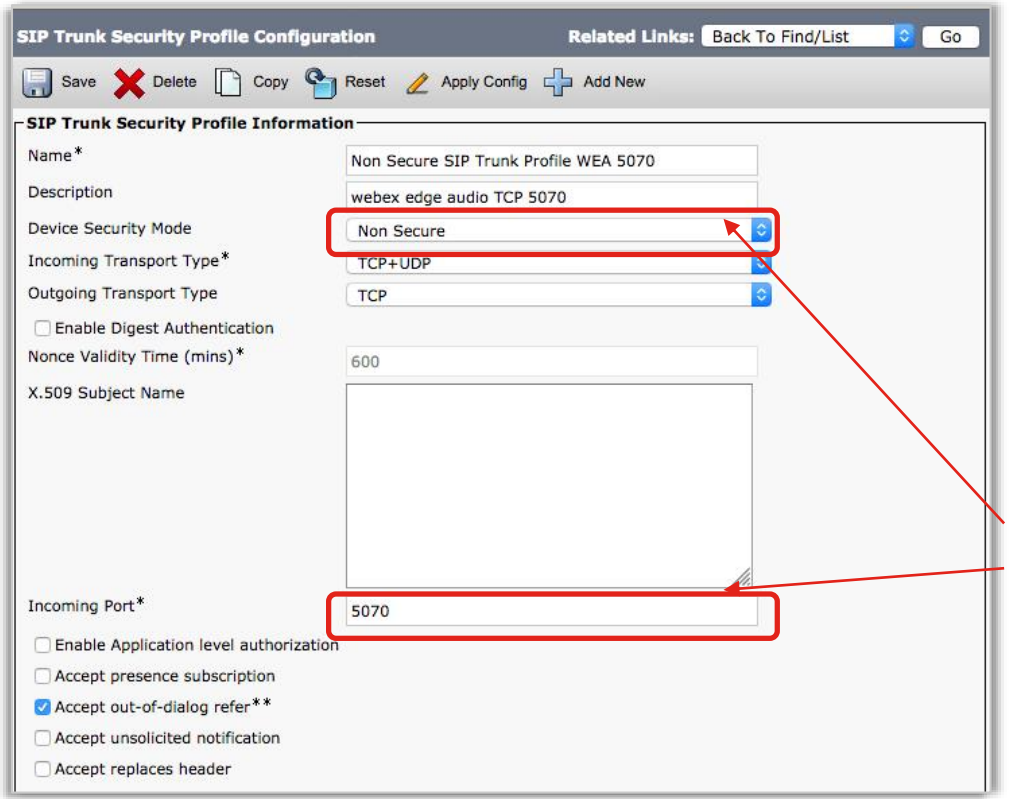
Webex Edge Audio Call-in Set Up Steps:

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



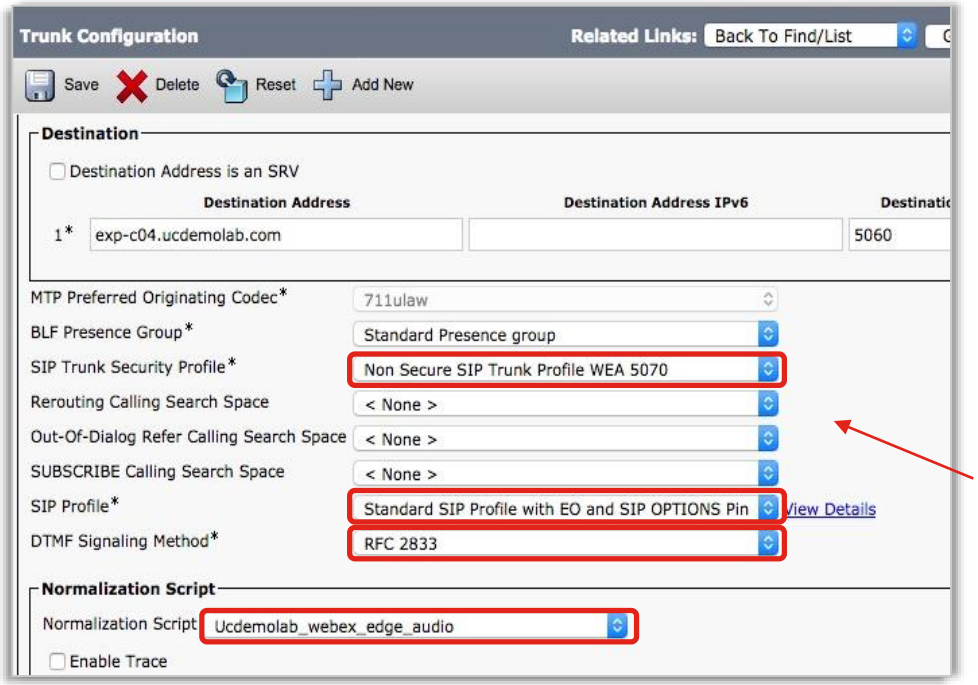
Webex Edge Audio Call-in Set Up Steps:

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



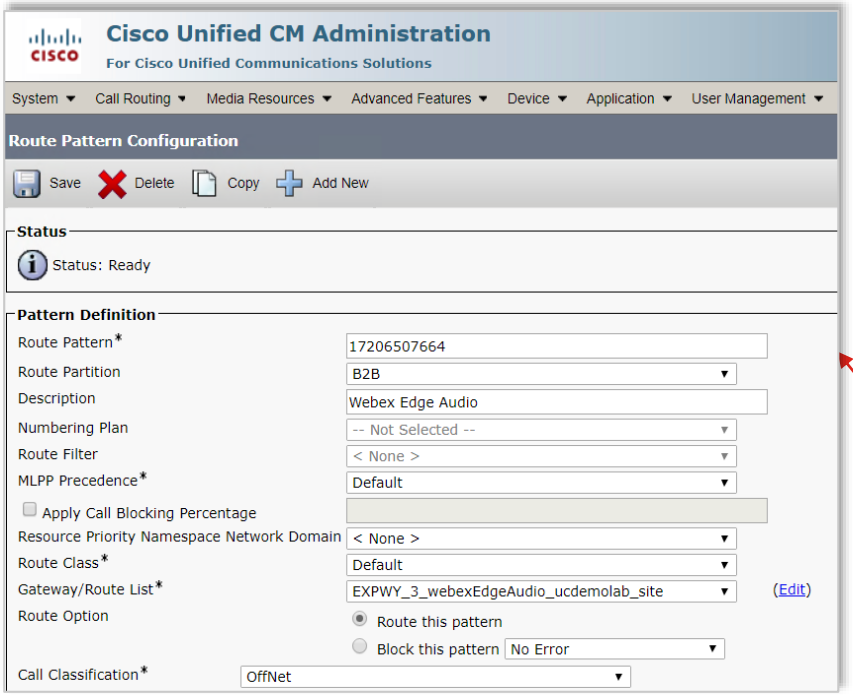
Webex Edge Audio Call-in Set Up Steps:

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

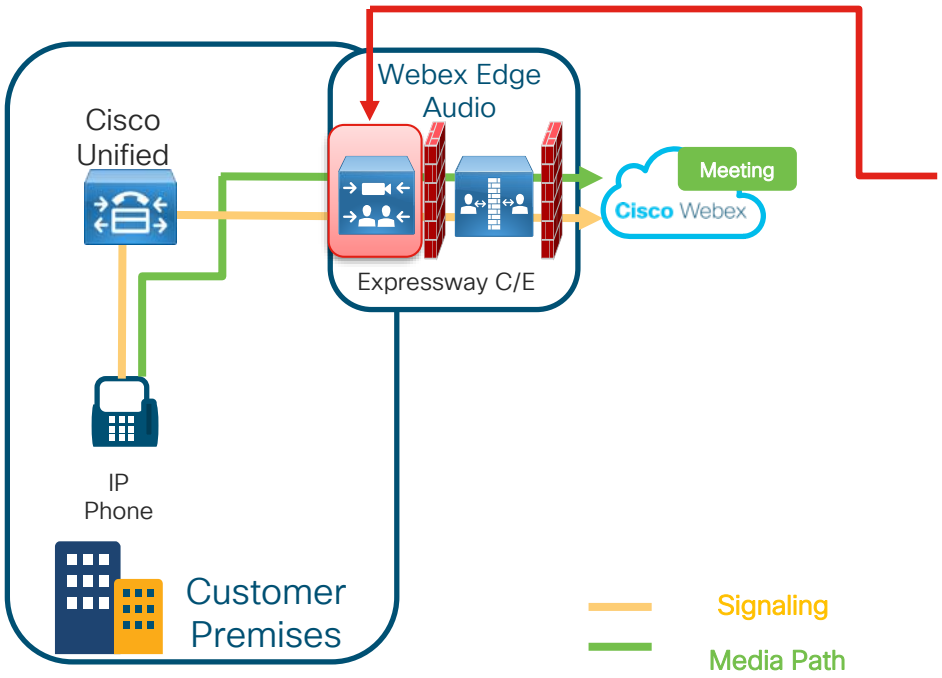


Webex Edge Audio Call-in Set Up Steps:

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

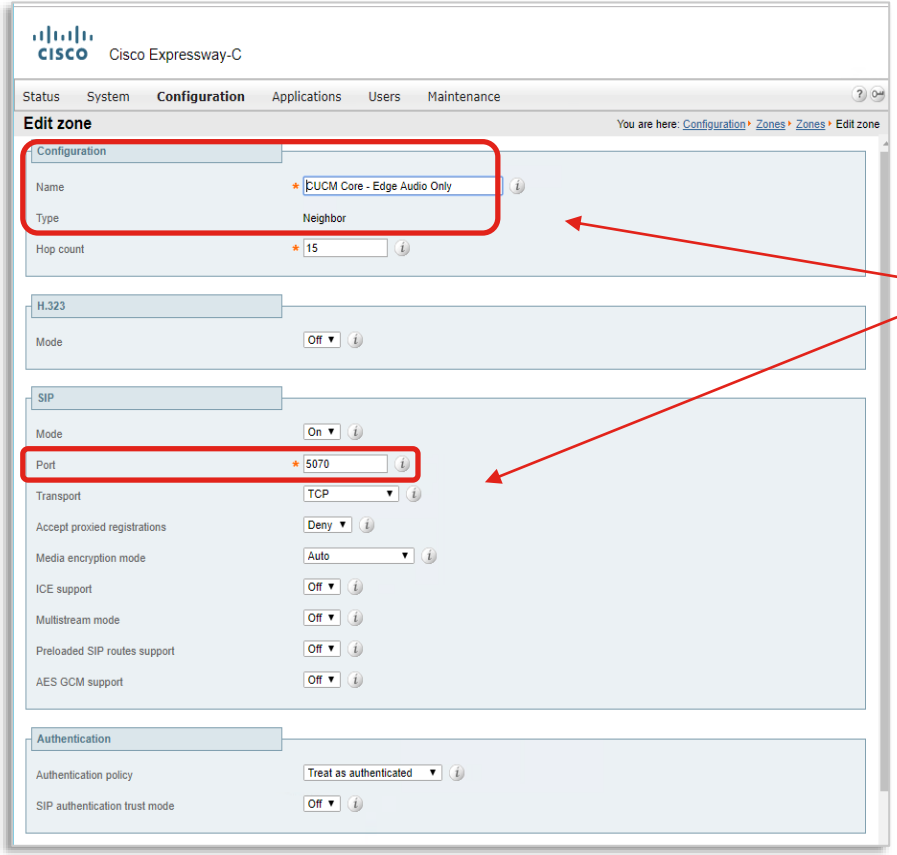


Webex Edge Audio Call-in Set Up Steps:

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

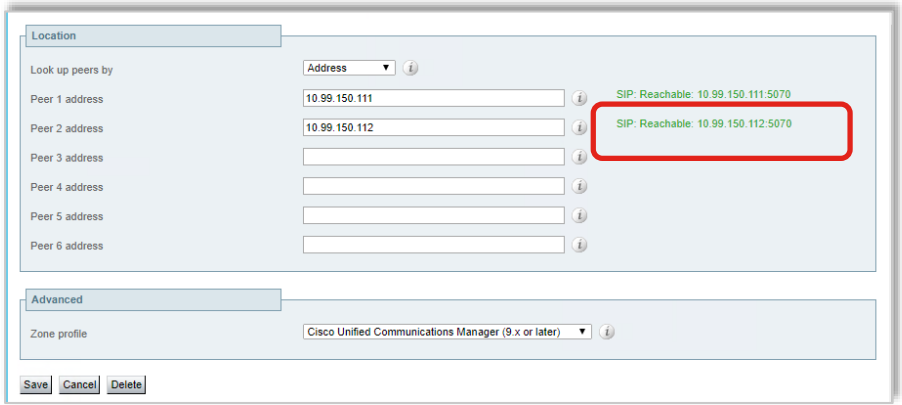
Cisco Webex Edge Audio

Architecture configuration – Dial in



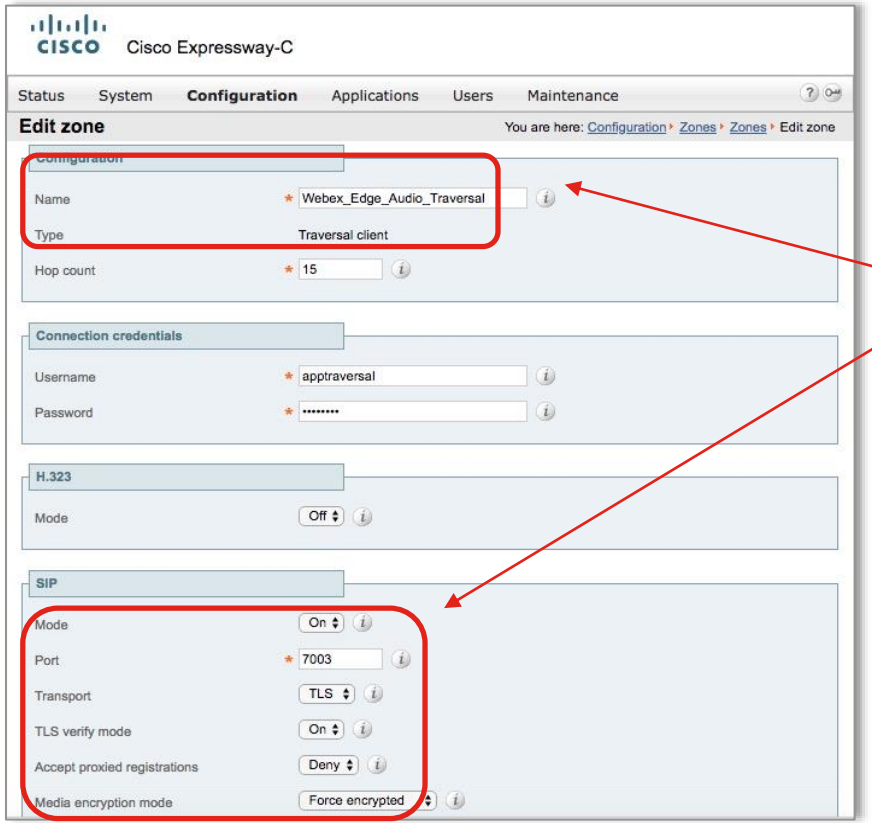
Webex Edge Audio Call-in Set Up Steps:

3. Configure Expressway-C
   - Create Neighbor zone
   - Define secure traversal client zone



Cisco Webex Edge Audio

Architecture configuration – Dial in

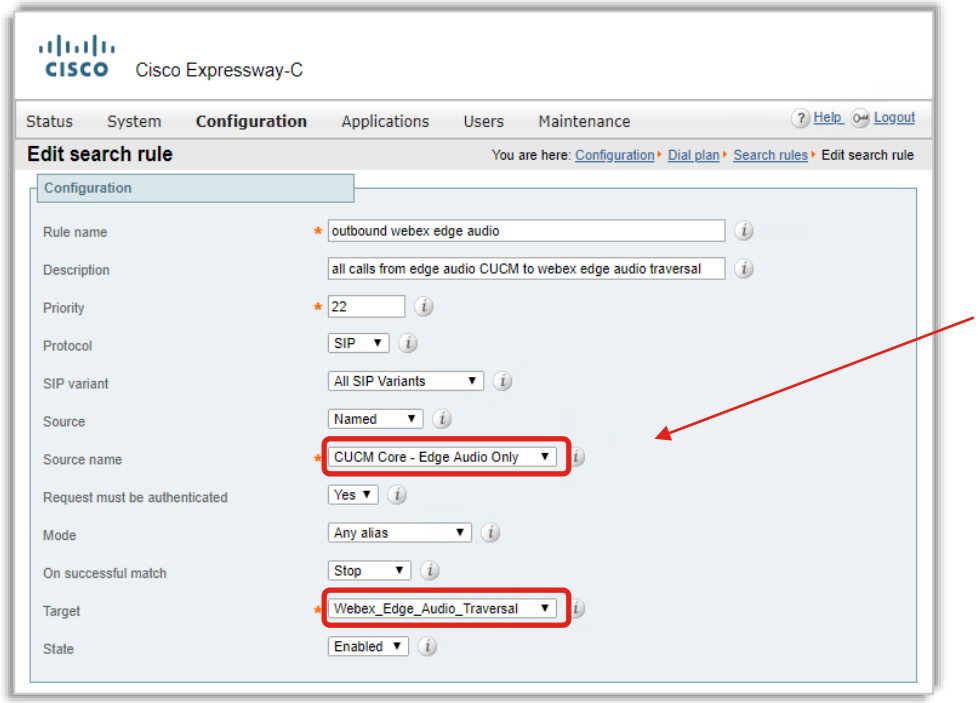


Webex Edge Audio Call-in Set Up Steps:

3. Configure Expressway-C
   - ✓ Create Neighbor zone
   - • Define secure traversal client zone

Cisco Webex Edge Audio

Architecture configuration – Dial in

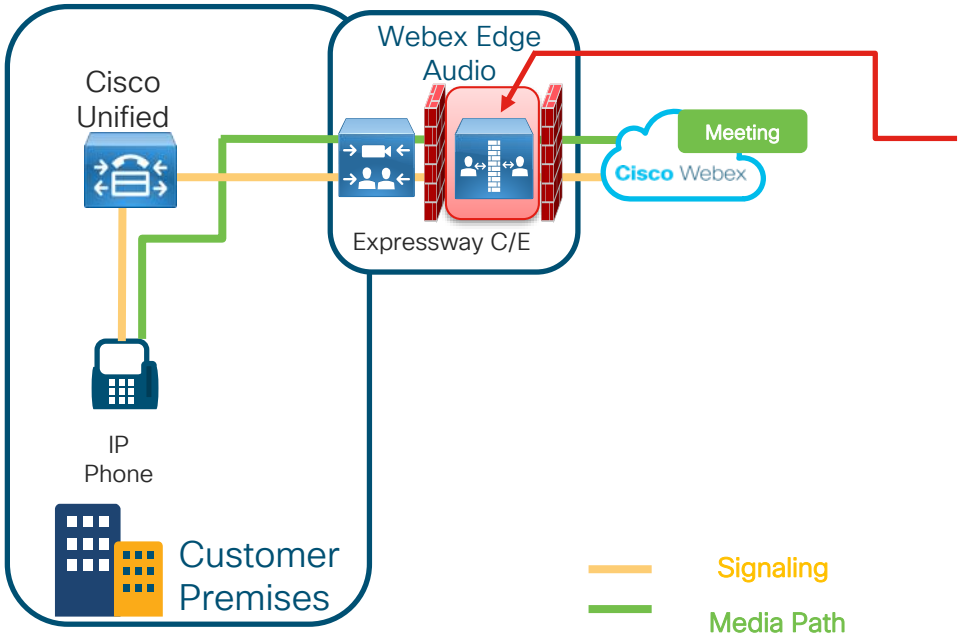


Webex Edge Audio Call-in Set Up Steps:

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



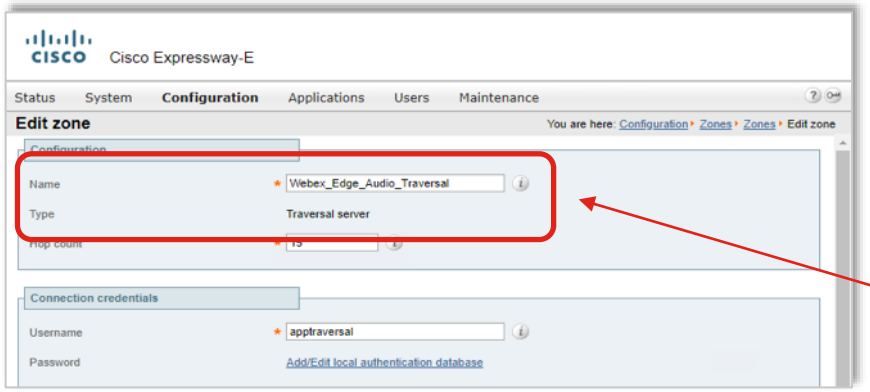
Webex Edge Audio Call-in Set Up Steps:

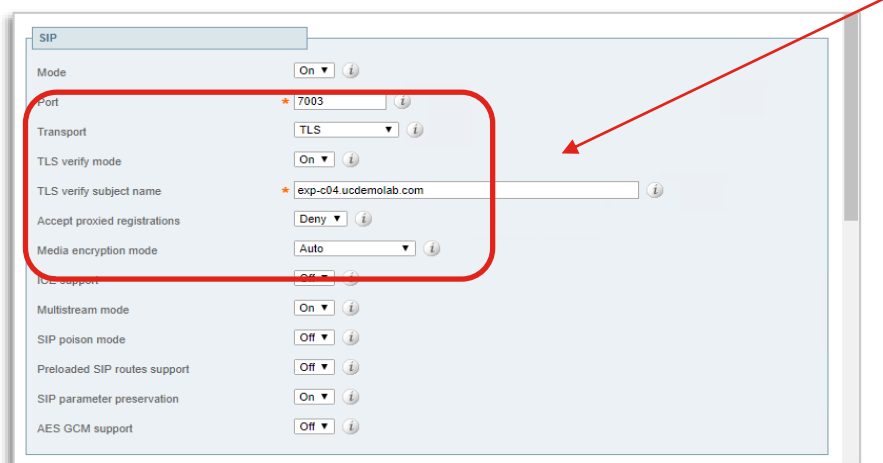
4. Configure Expressway-E

- 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





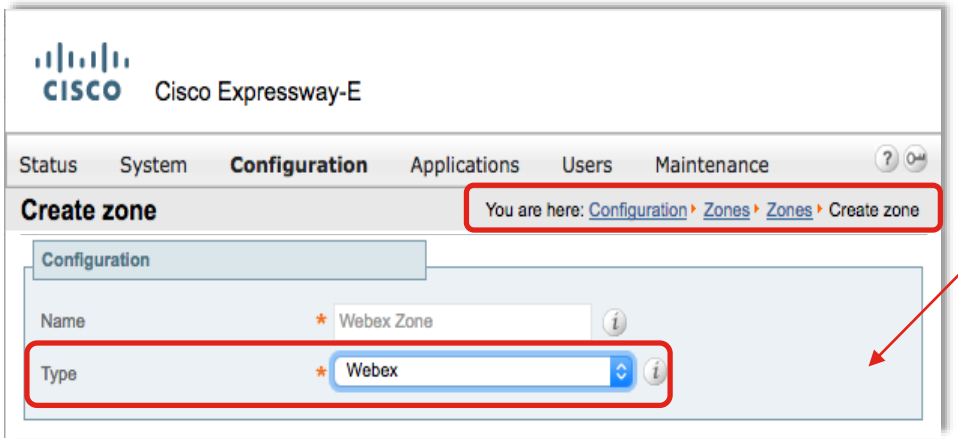
Webex Edge Audio Call-in Set Up Steps:

4. Configure Expressway-E

- Set up Secure Traversal Server Zone.

Cisco Webex Edge Audio

Architecture configuration – Dial in

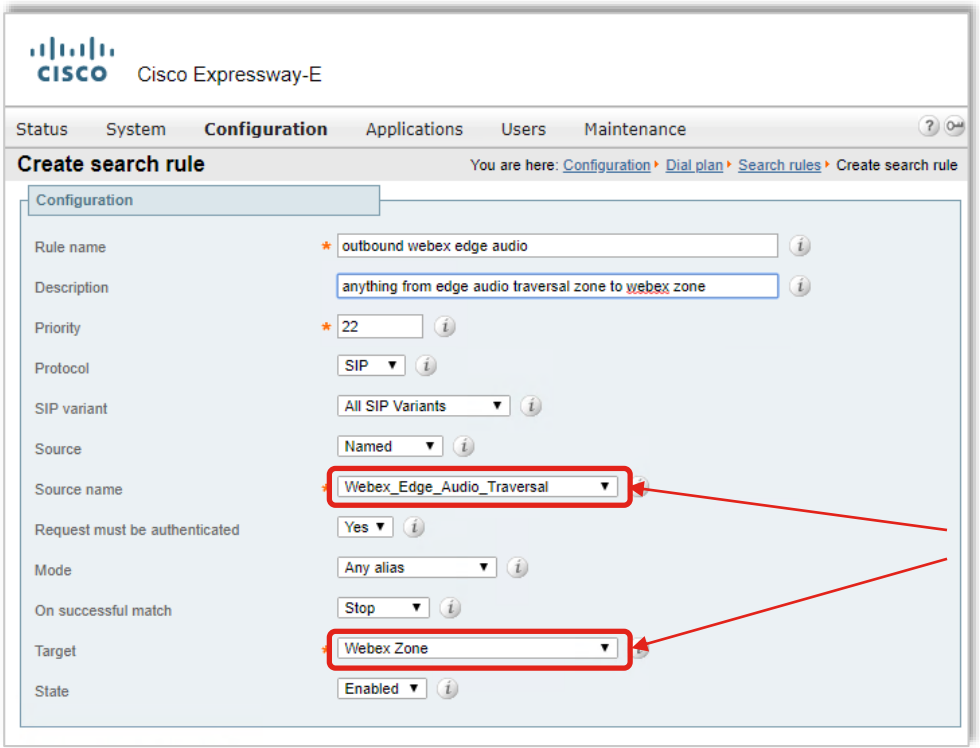


Webex Edge Audio Call-in Set Up Steps:

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



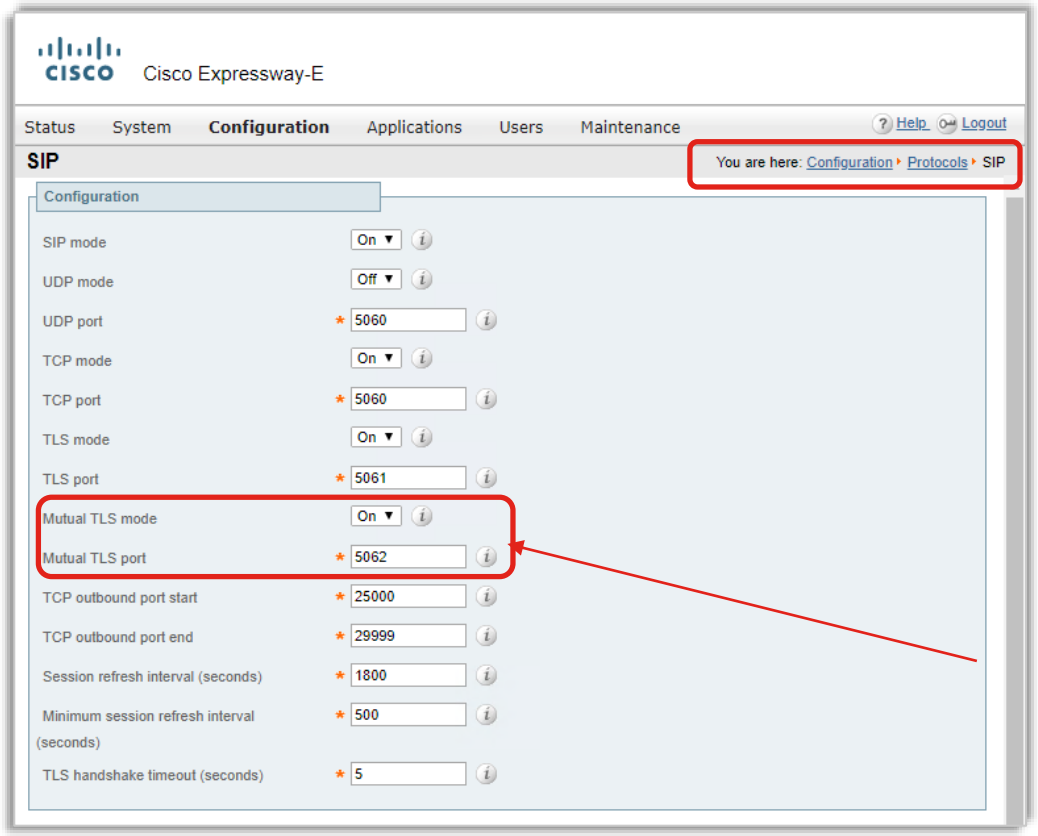
Webex Edge Audio Call-in Set Up Steps:

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



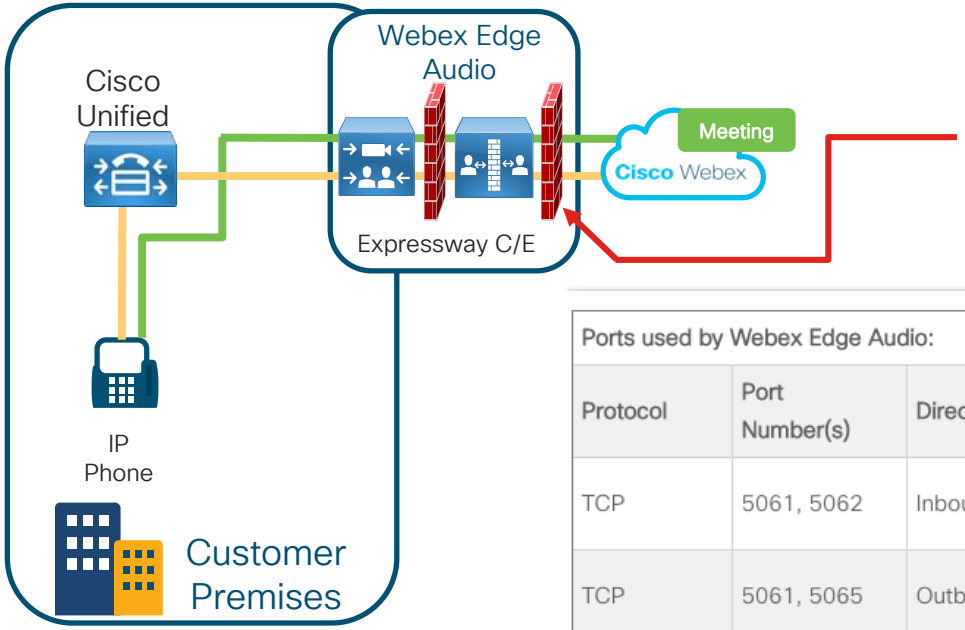
Webex Edge Audio Call-in Set Up Steps:

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



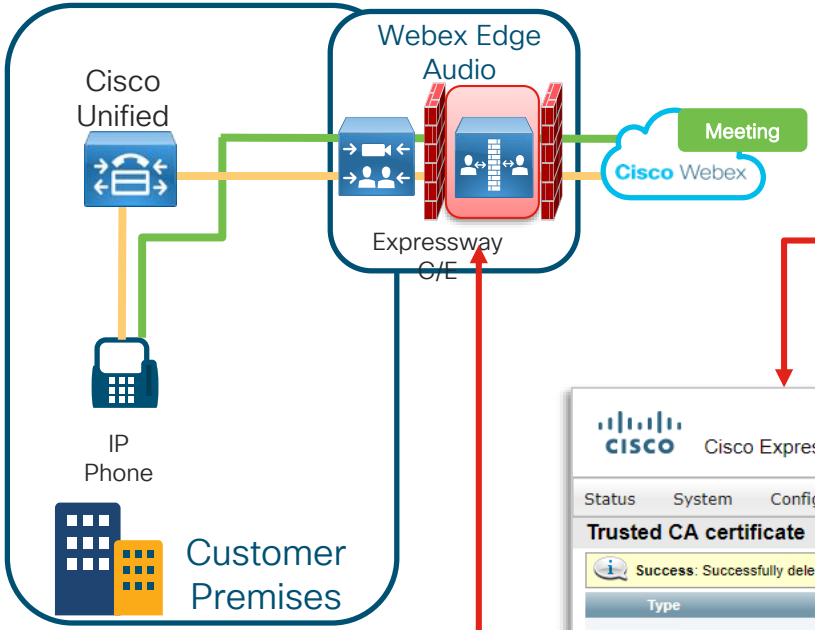
Webex Edge Audio Call-in Set Up Steps:

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

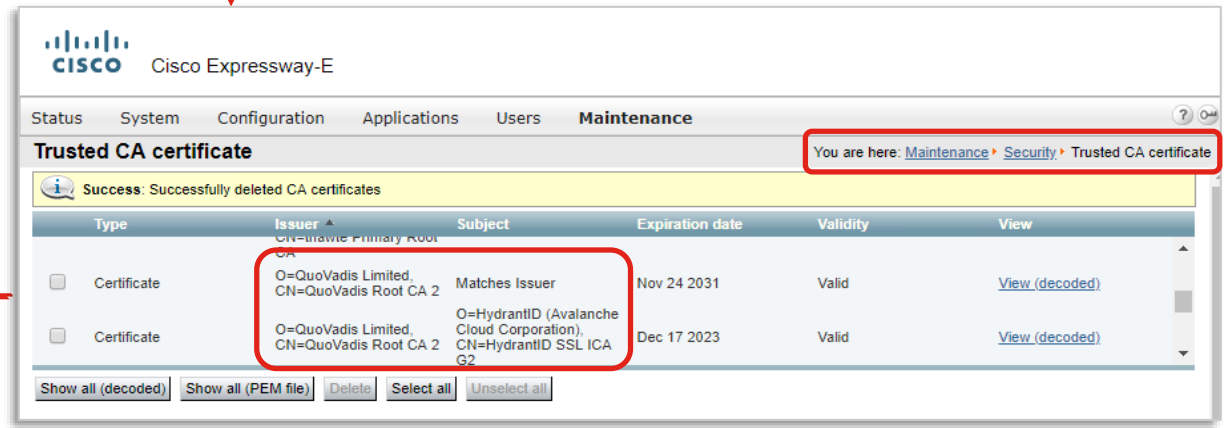
Cisco Webex Edge Audio

Architecture configuration – Dial in



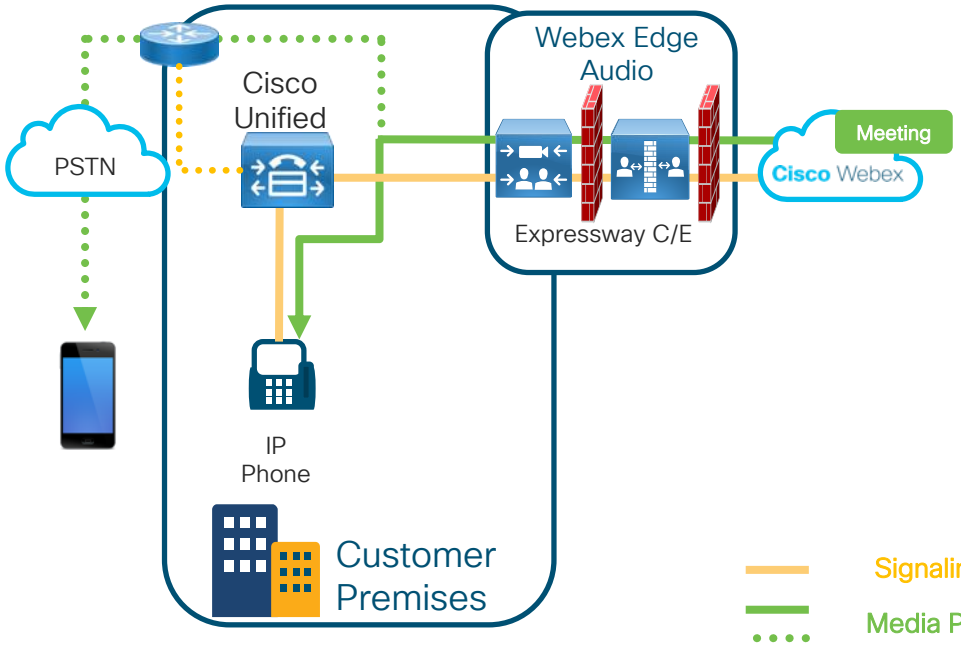
Webex Edge Audio Call-in Set Up Steps:

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



Cisco Webex Edge Audio

Overview Architecture configuration – Call Back

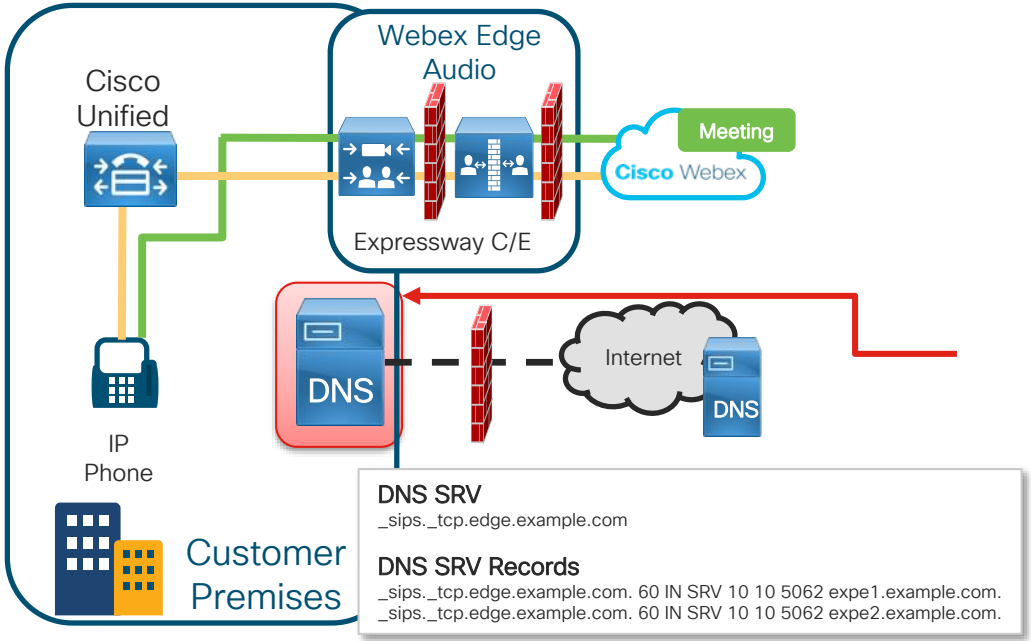


Overview of the Webex Edge Audio Callback Set Up Steps:

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.

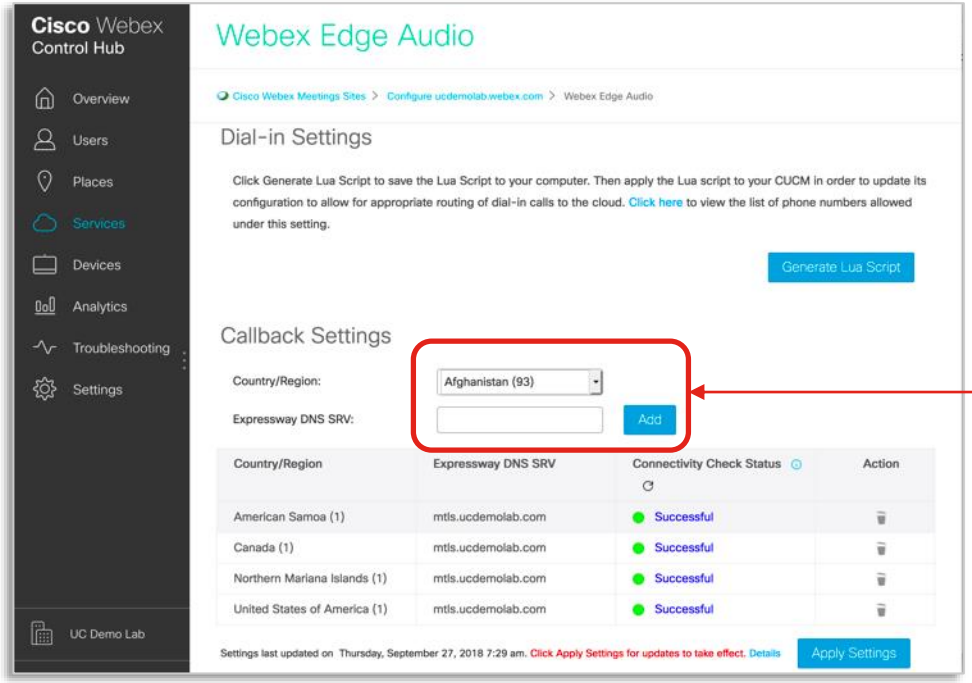
2. The DNS SRV records must refer to the mutual TLS port (the default mutual TLS port is 5062). You cannot reuse existing MRA (_collab-edge._tcp), or B2B (_sips._tcp) SRV records, because Edge Audio requires that the SRV records resolve to the Expressway-E cluster's mutual TLS port. Both MRA and B2b 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

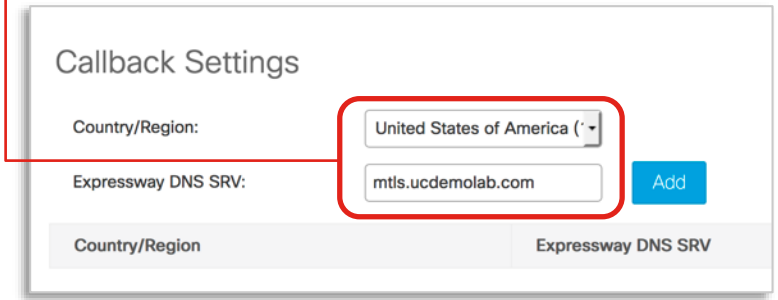
Cisco Webex Edge Audio

Architecture configuration – Call Back

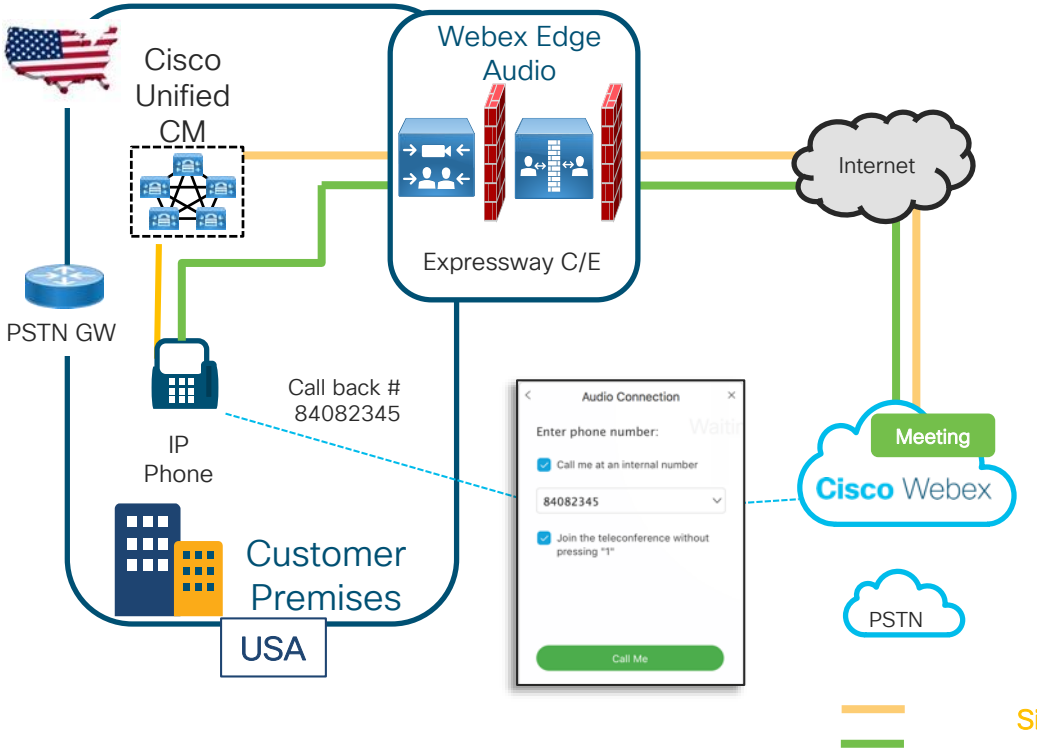


Overview of the Webex Edge Audio Callback Set Up Steps:

1. Apply Webex Edge Audio Callback Settings
   - Define country callback parameters in Control Hub
   - 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.



Extension callback



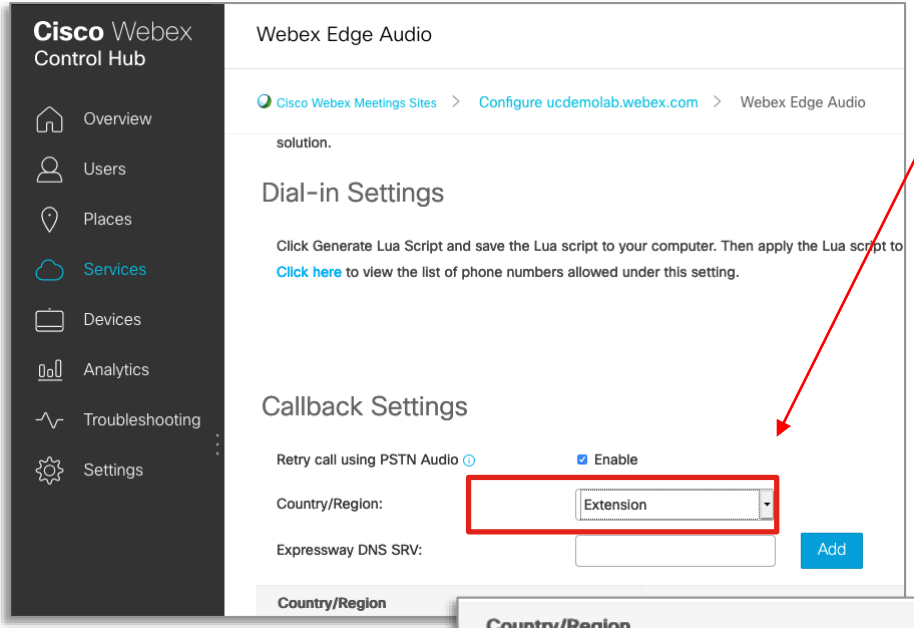
Edge Audio Extension Callback:

- 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:

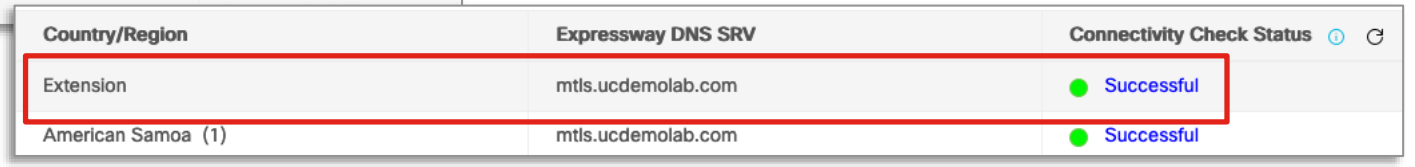
- There will be no PSTN fallback support for extension based call routing.
- It will take a maximum of 30 mins for the extension callback settings to apply

Extension callback configuration

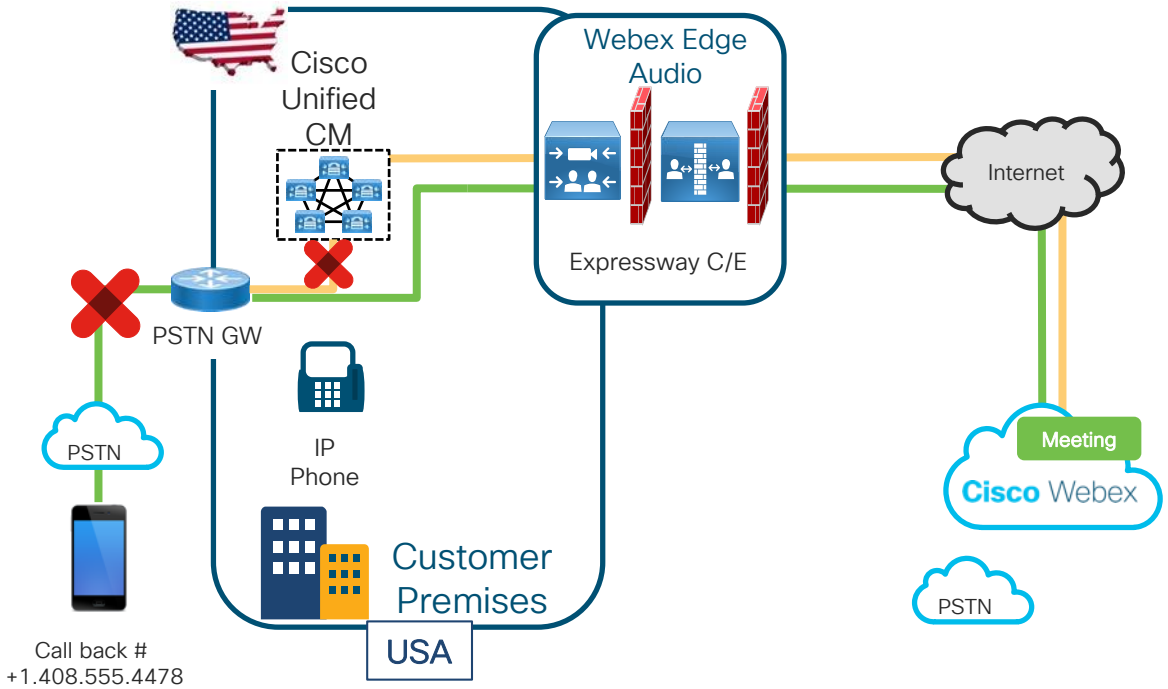


- Select ”Extension from the drop down list
- Add SRV and click “Apply Settings” button
- A single SRV can be configured for callback

- Webex 33.x or higher required



PSTN Fall Back



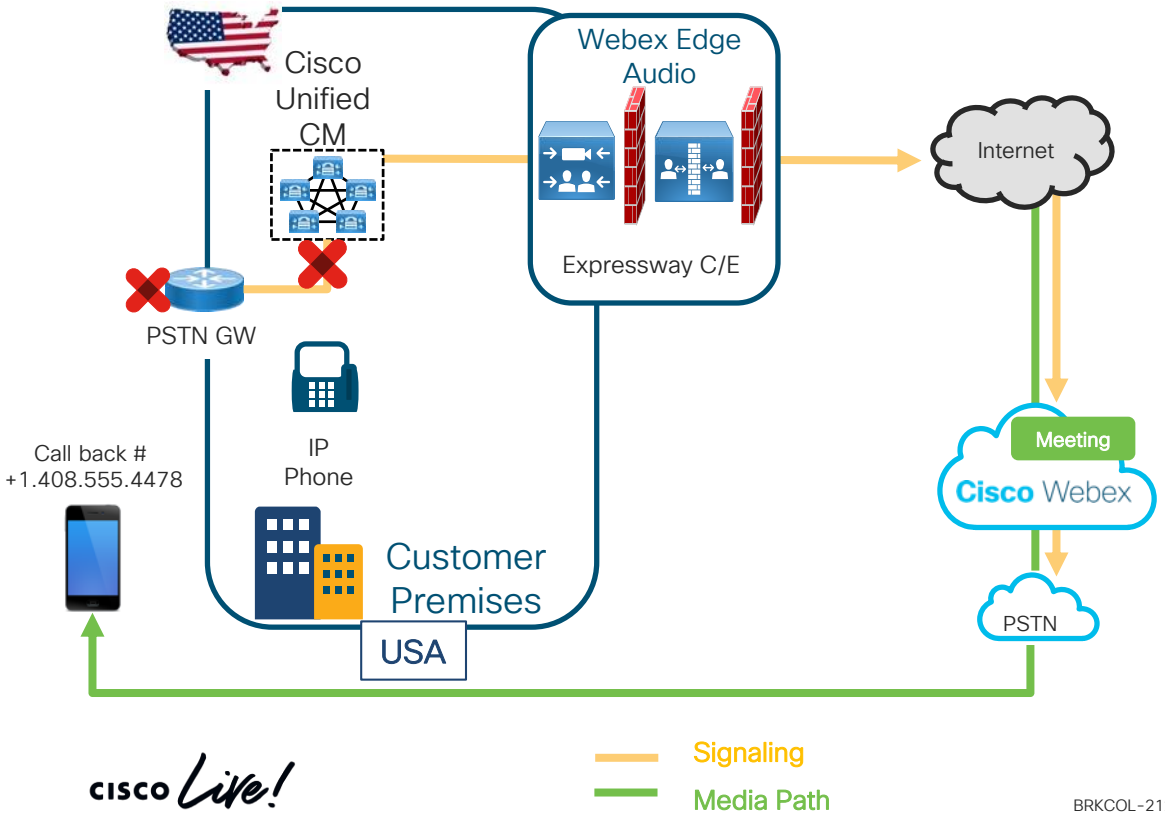
What if any of these happen?

- 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

Signaling

Media Path

PSTN Fall Back



When PSTN fallback will be triggered?

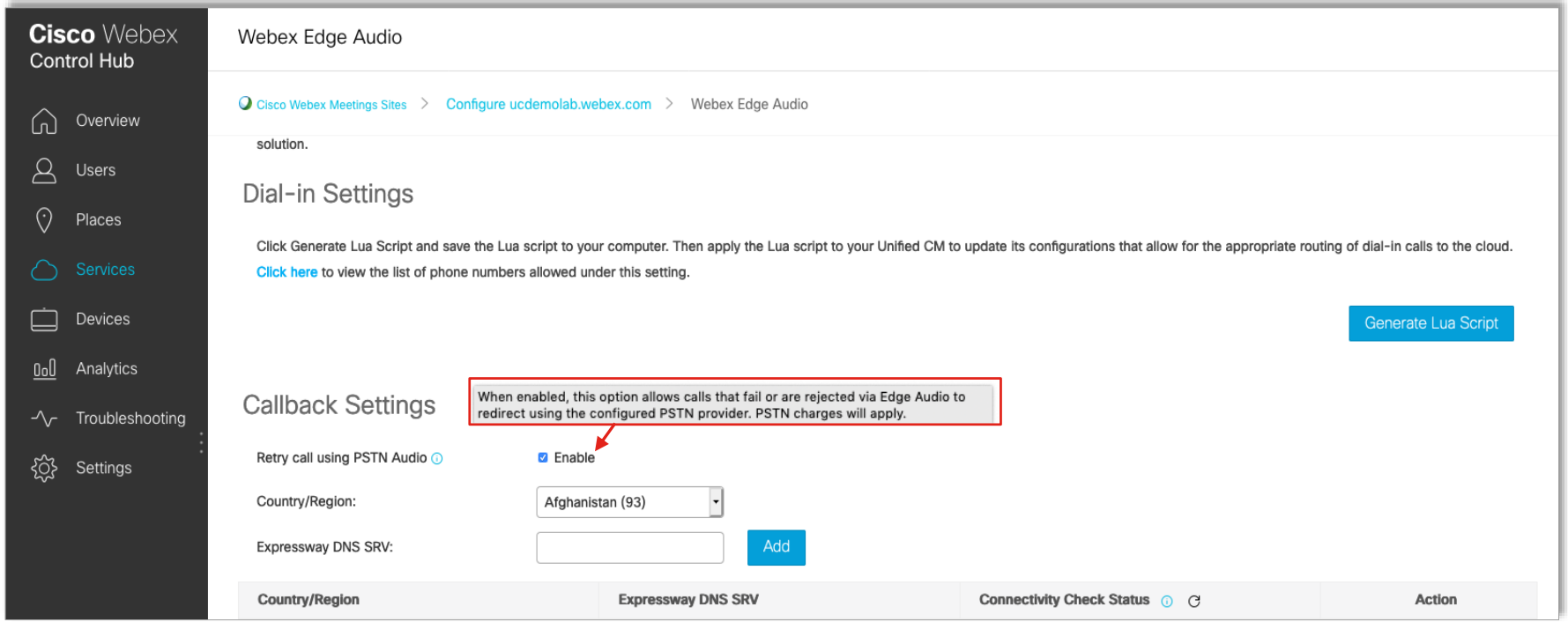
When an Edge Audio call is failed due to

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:

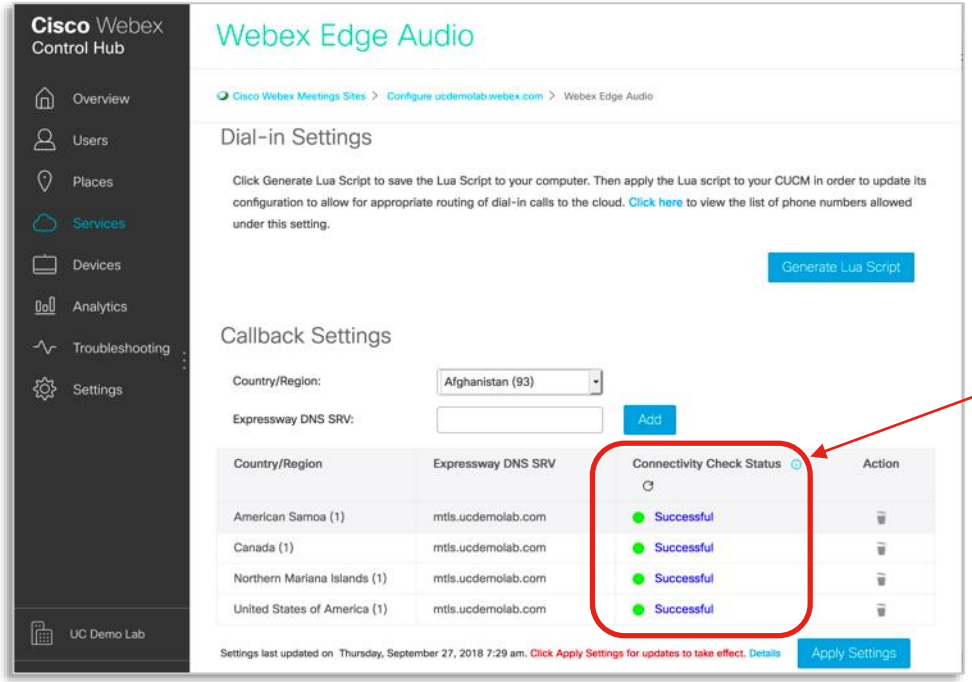
- A SIP response code is sent to the Webex cloud and the call is rerouted out Webex's PSTN.
- Media is sent from Webex PSTN to the cell phone.

PSTN Fall Back



Cisco Webex Edge Audio

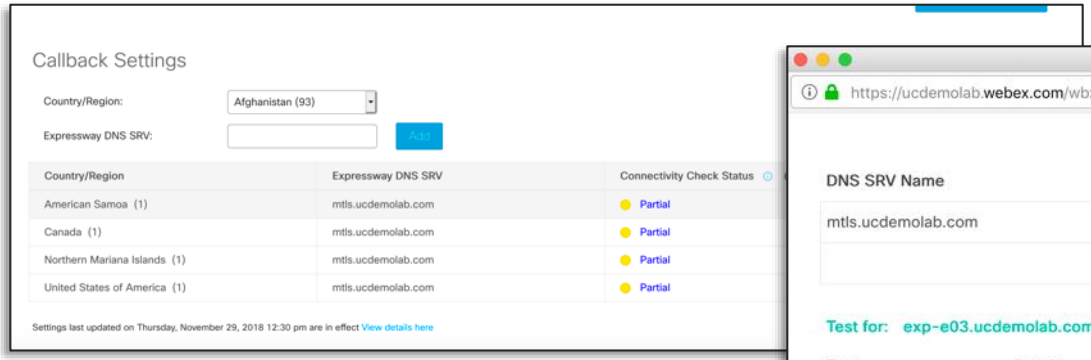
Architecture configuration – Call Back

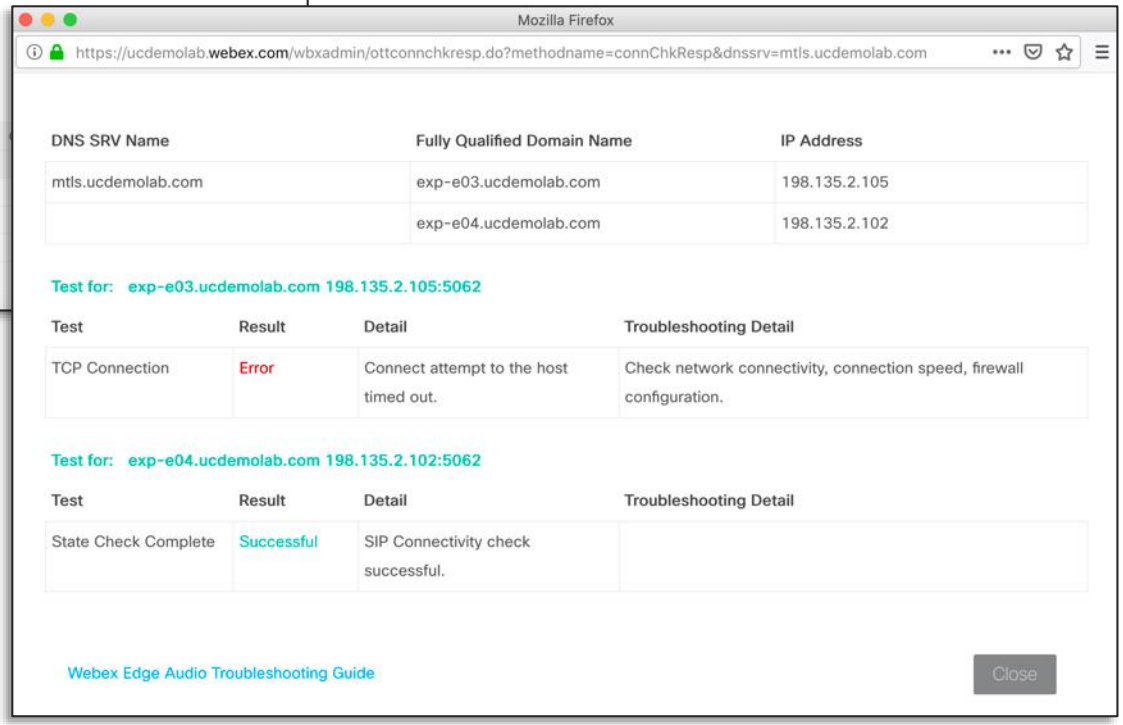


Overview of the Webex Edge Audio Callback Set Up Steps:

1. Apply Webex Edge Audio Callback Settings
   - ✓ Define country callback parameters in Control Hub
   - Ensure 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



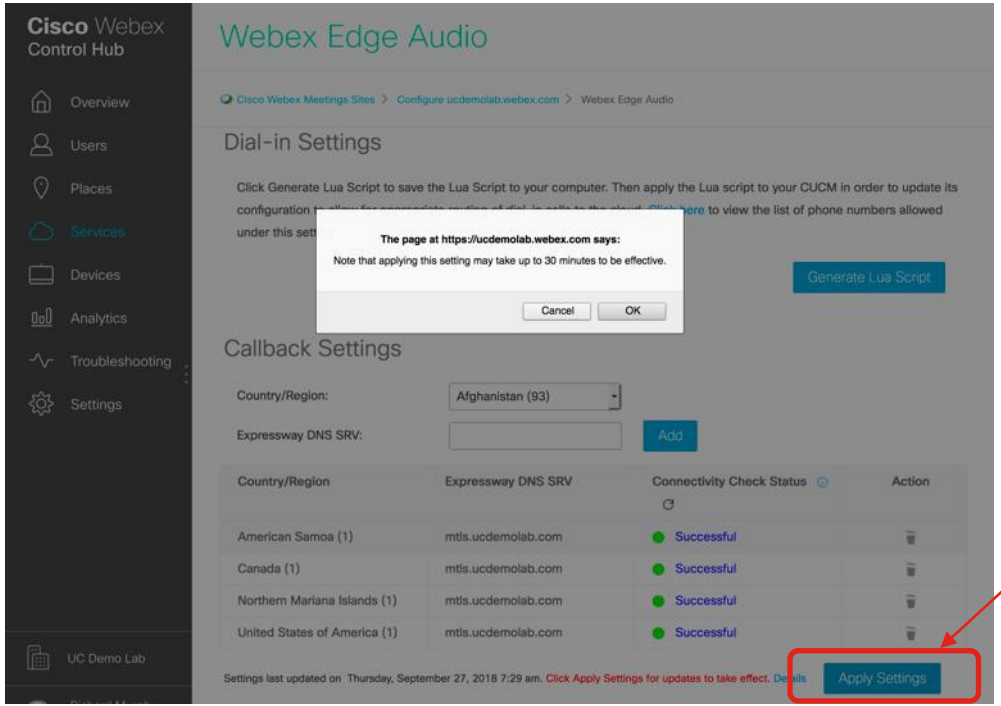


Ensure connectivity checks are successful.

- 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

Architecture configuration – Call Back

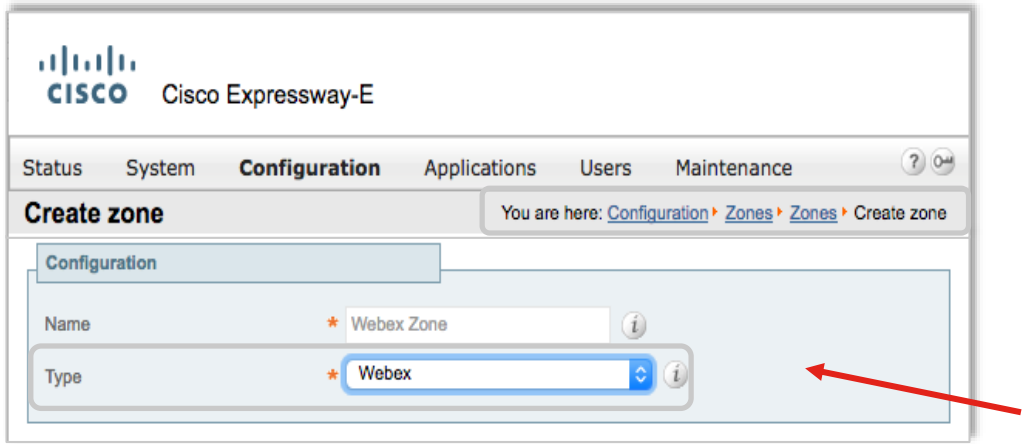


Overview of the Webex Edge Audio Callback Set Up Steps:

1. Apply Webex Edge Audio Callback Settings
   - ✓ Define country callback parameters in Control Hub
   - ✓ Ensure 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



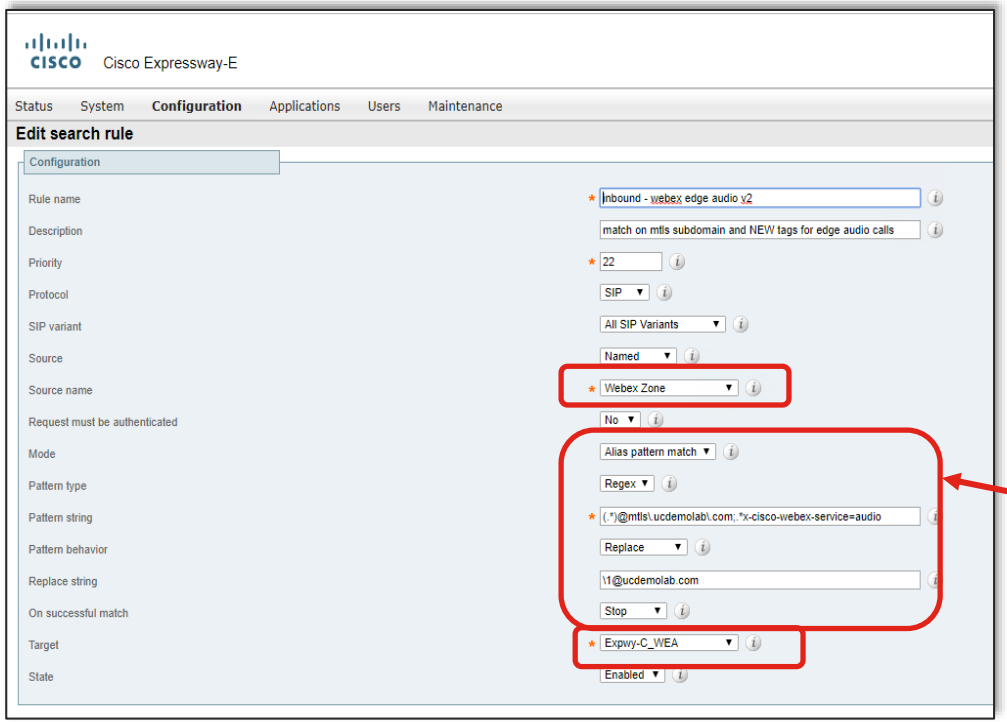
Overview of the Webex Edge Audio Callback Set Up Steps:

- ✓ 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

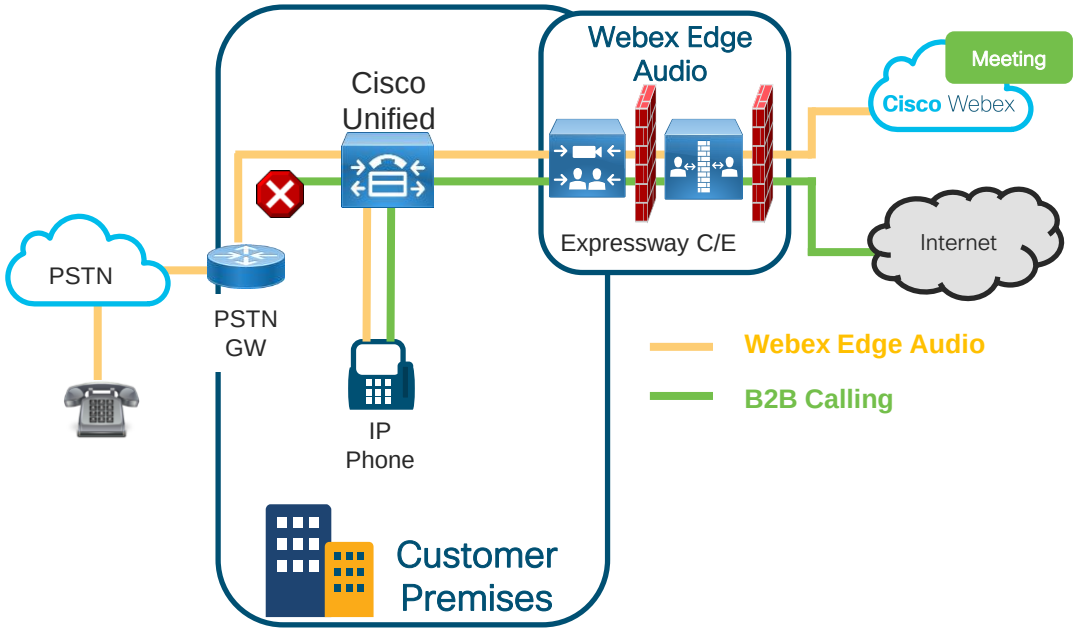


Overview of the Webex Edge Audio Callback Set Up Steps:

- ✓ 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

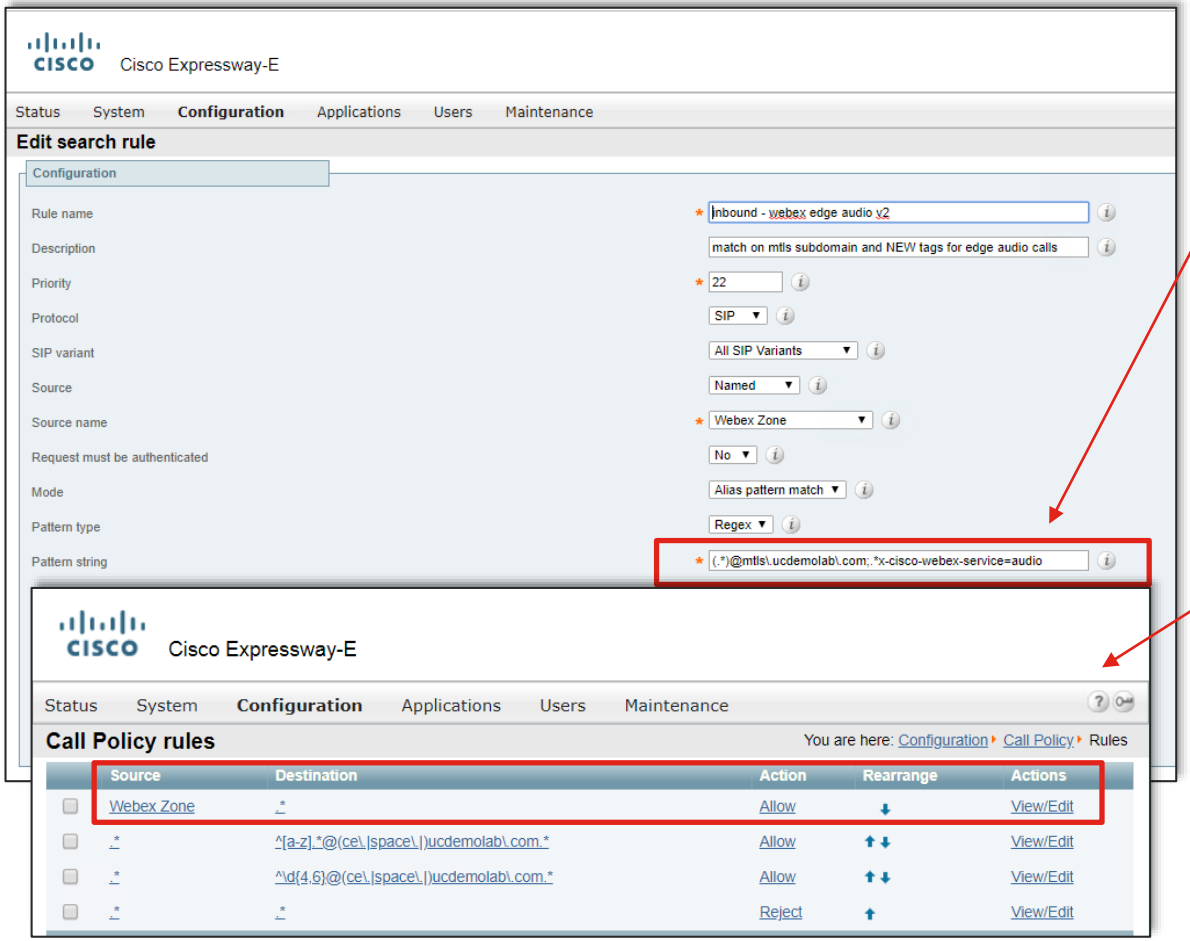
Best practices/Toll Fraud



- 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



- Apply tag to search rule:

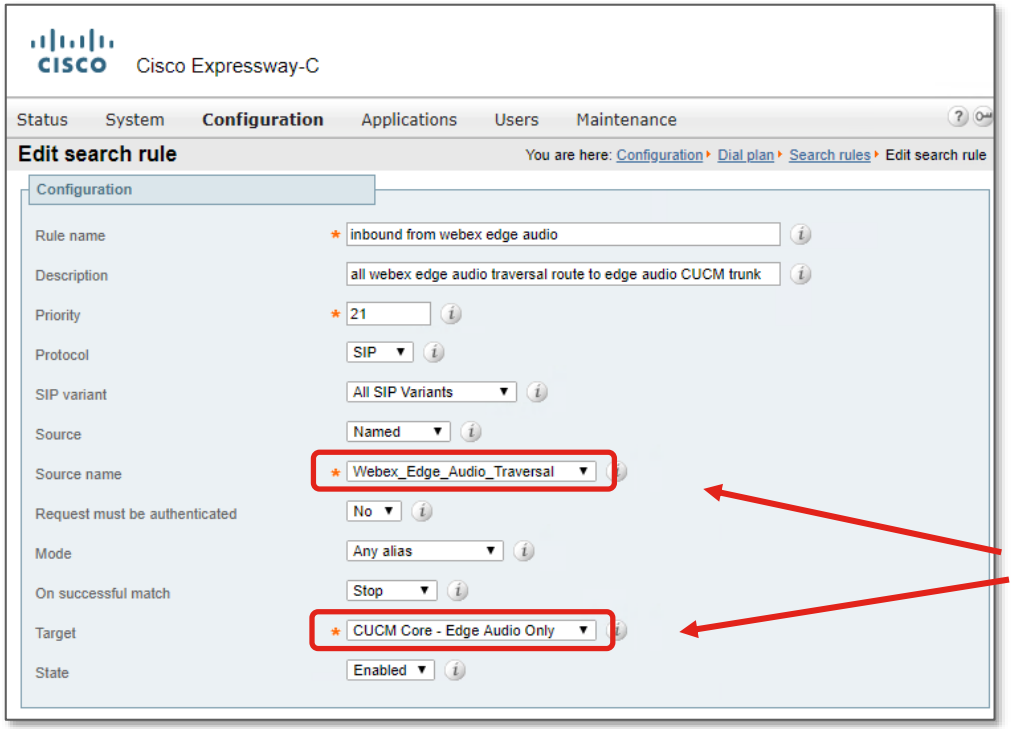
(.)@mtls.ucdemolab.com;.*x-cisco-webex-service=audio*

- 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

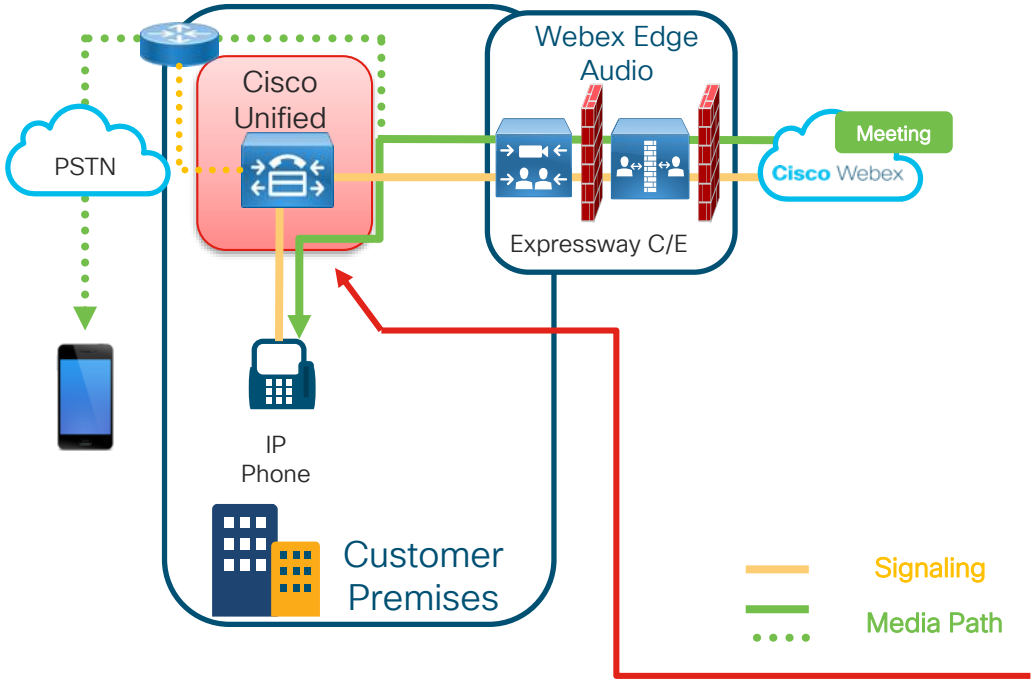
Overview of the Webex Edge Audio Callback Set Up Steps:

- ✓ 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:

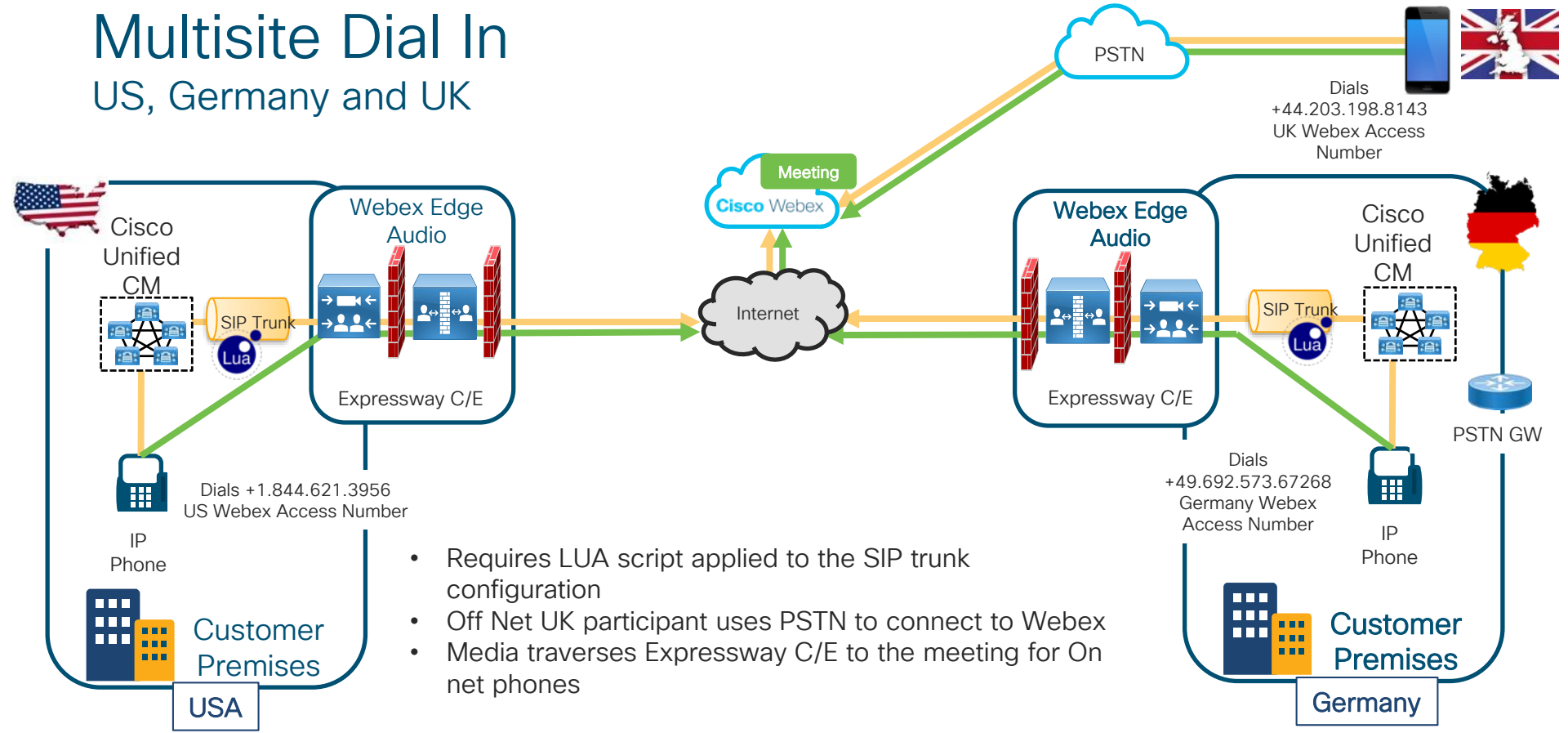
- ✓ Apply Webex Edge Audio Callback Settings
  - ✓ Define country callback parameters in Control Hub
  - ✓ Ensure proper SRV record configuration for Expressway
  - ✓ Ensure connectivity checks are successful.
- ✓ Configure Expressway-E to accept calls and route to Expressway – C
- ✓ Configure Expressway-C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

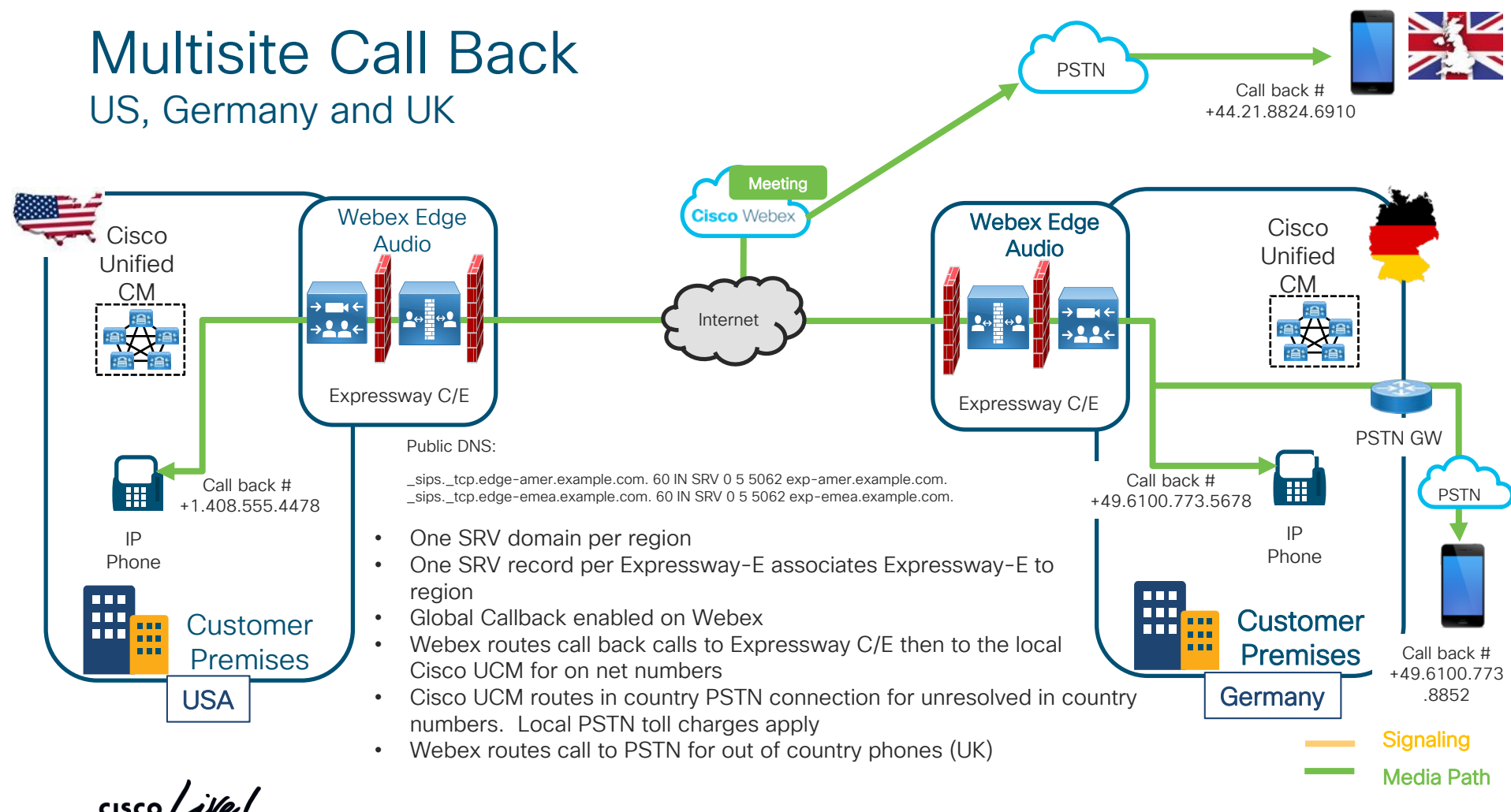
US, Germany and UK



- 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

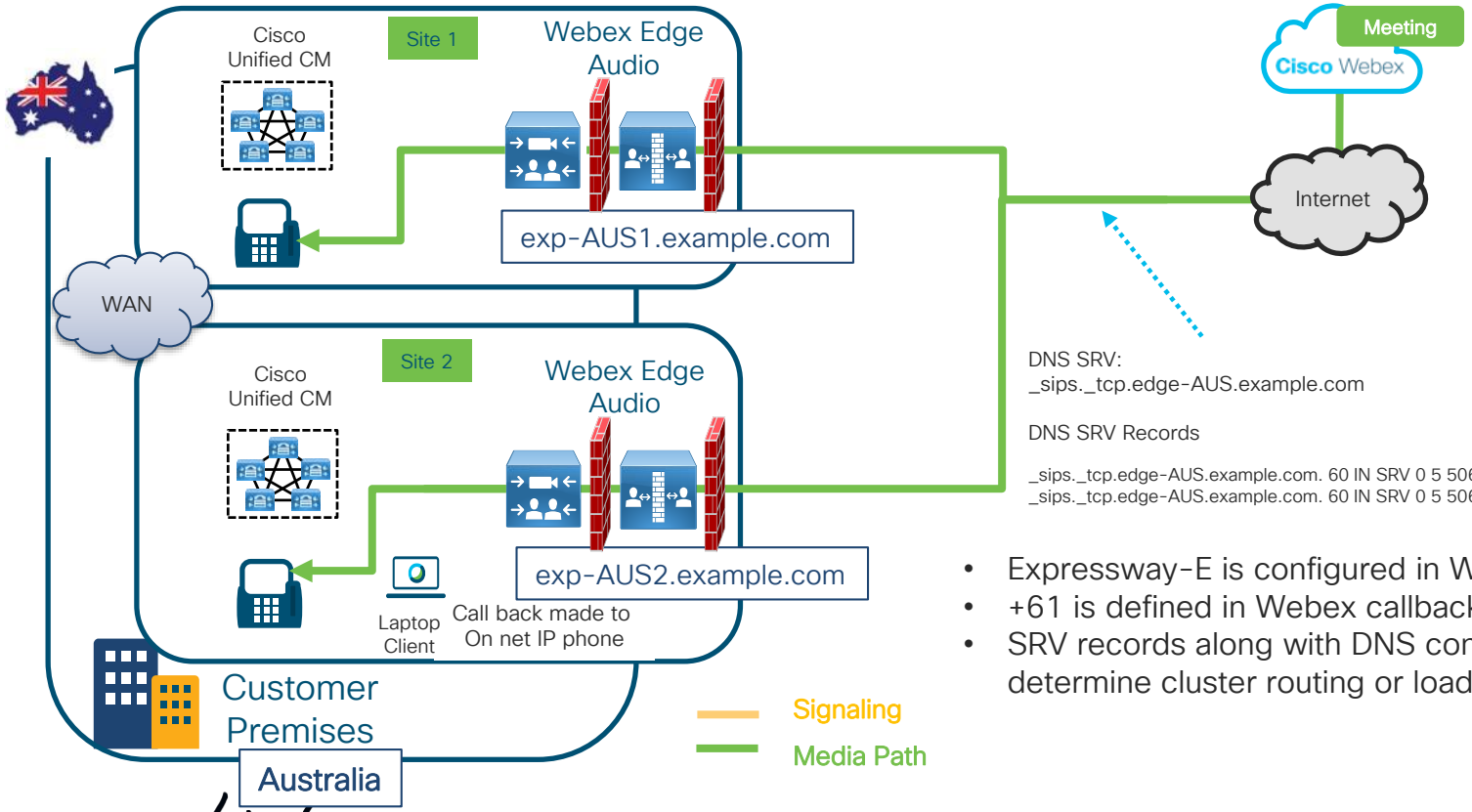
Multisite Call Back

US, Germany and UK



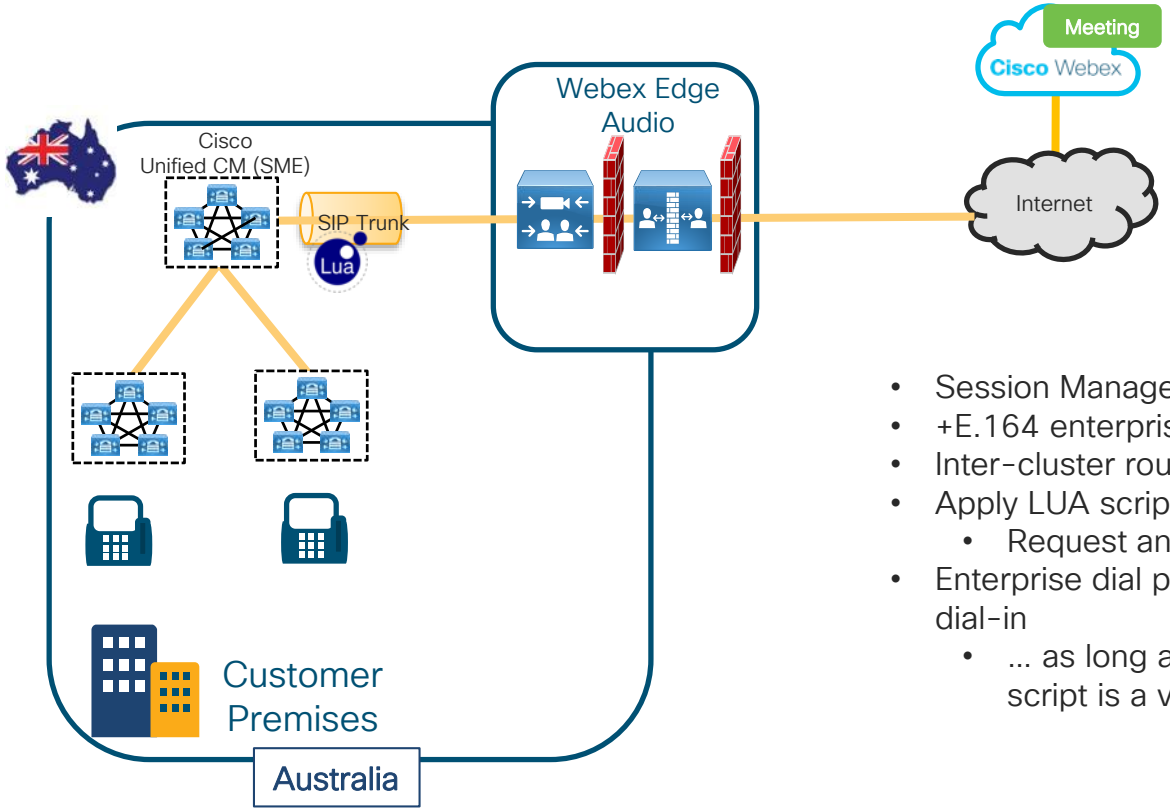
- One SRV domain per region
- One SRV record per Expressway-E associates Expressway-E to region
- Global Callback enabled on Webex
- Webex routes call back calls to Expressway C/E then to the local Cisco UCM for on net numbers
- Cisco UCM routes in country PSTN connection for unresolved in country numbers. Local PSTN toll charges apply
- Webex routes call to PSTN for out of country phones (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

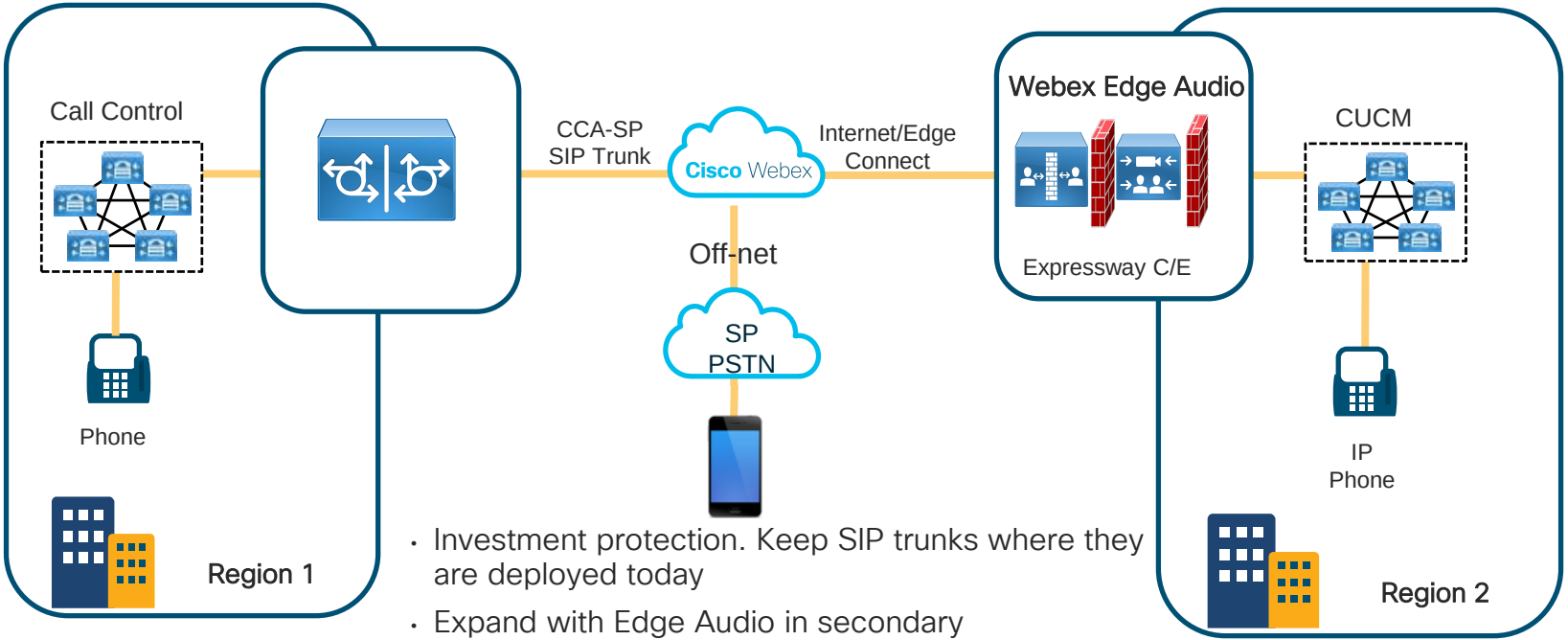


- Session Manager Edition is supported
- +E.164 enterprise dial plan to route dial-in and call-back
- Inter-cluster routing using ILS/GDPR
- Apply LUA script on SME trunk for dial-in
  - Request and To: URI manipulation
- Enterprise dial plan can support arbitrary dialing habits for dial-in
  - … as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

Signaling
Media Path

Cisco Webex Edge Audio w/ CCA-SP

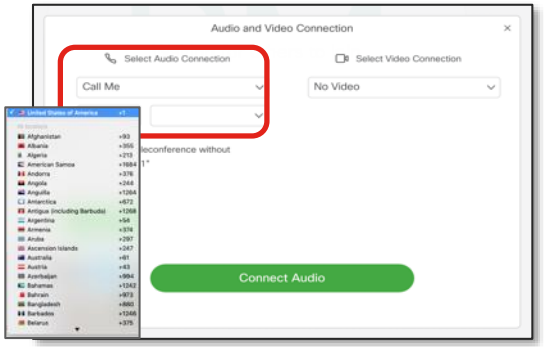
Mixed SIP Trunk & Expressway as Edge in Region 1 and Region 2



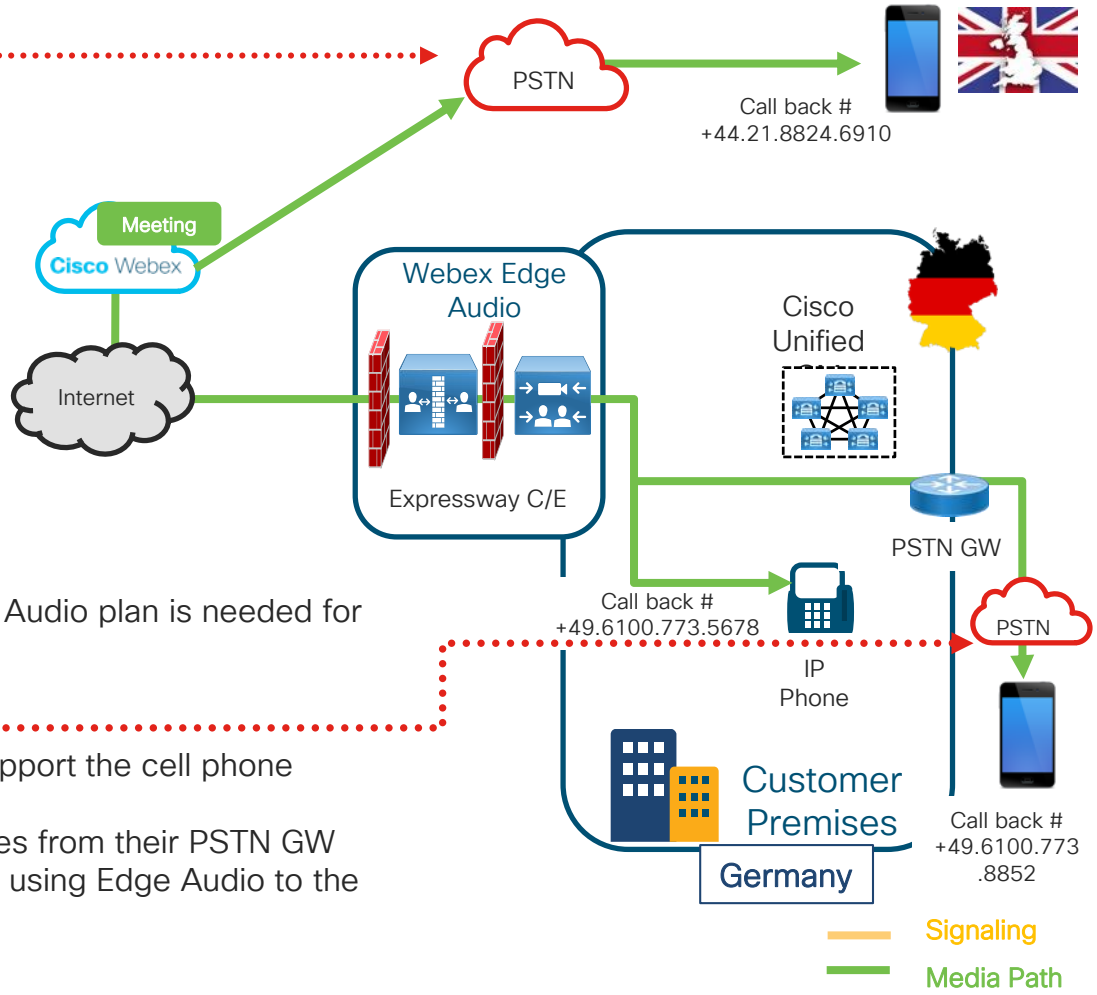
- Investment protection. Keep SIP trunks where they are deployed today
- Expand with Edge Audio in secondary locations/regions
- Both architectures work to support the audio calls

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

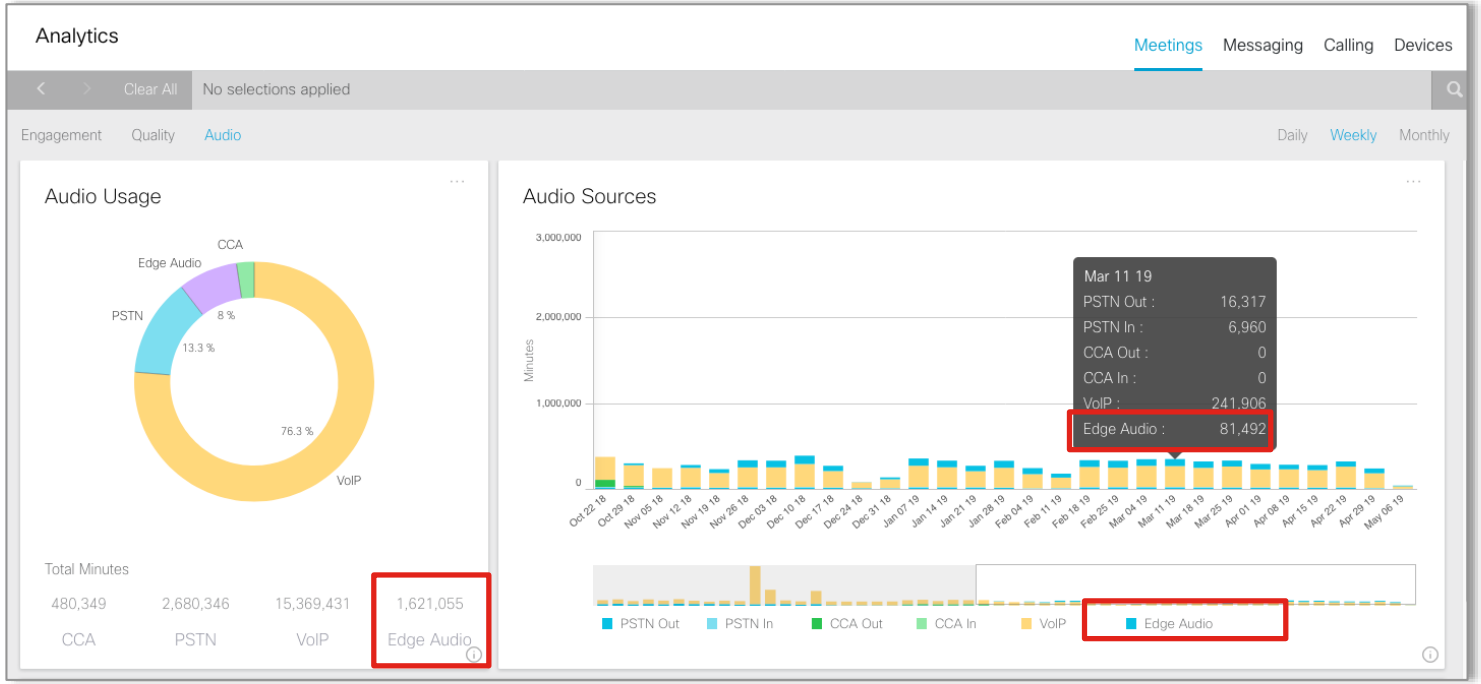


Edge Audio Reporting

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.

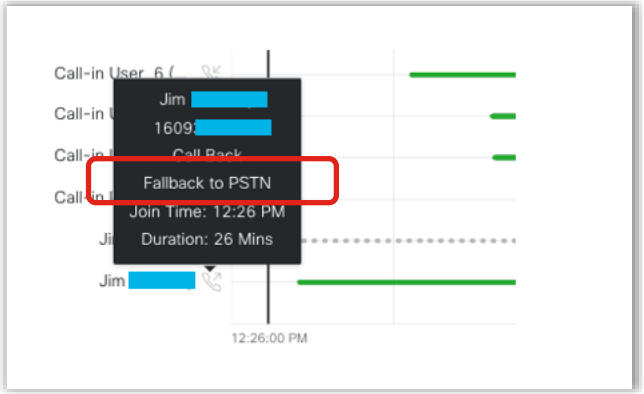
- Number of Edge Audio calls
- Dial in and callback numbers are combined.



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

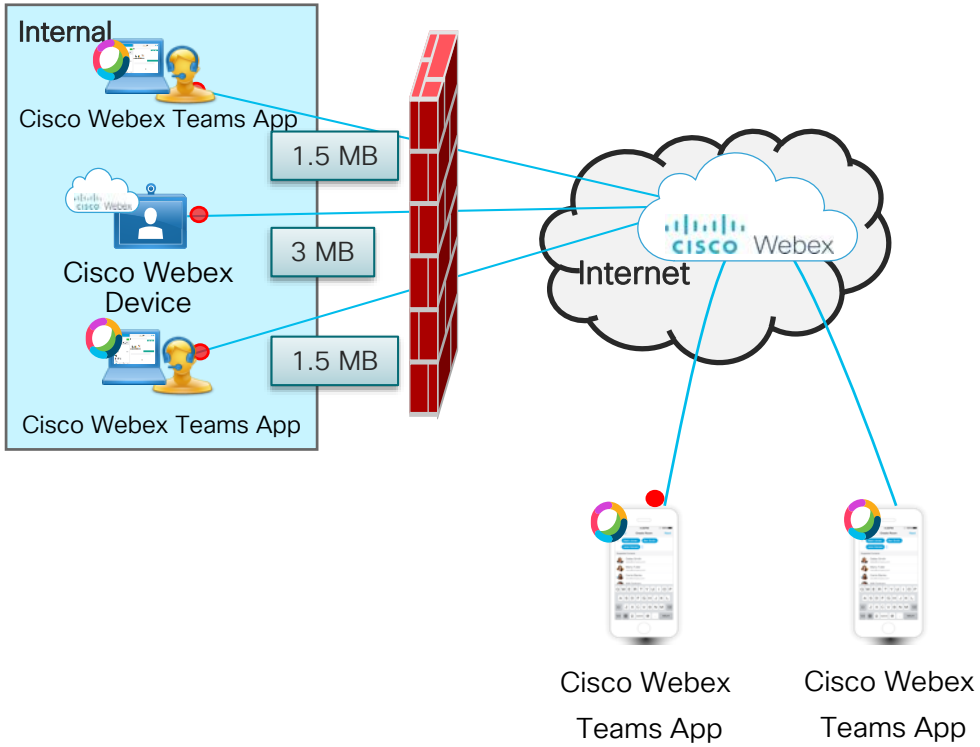
Webex Video Mesh

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

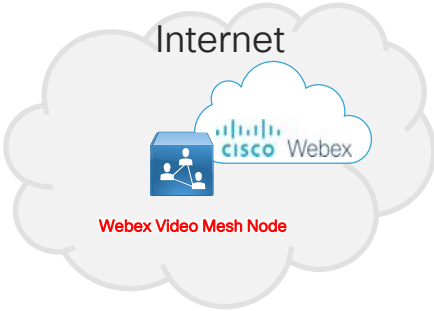
Cisco Webex Video Mesh

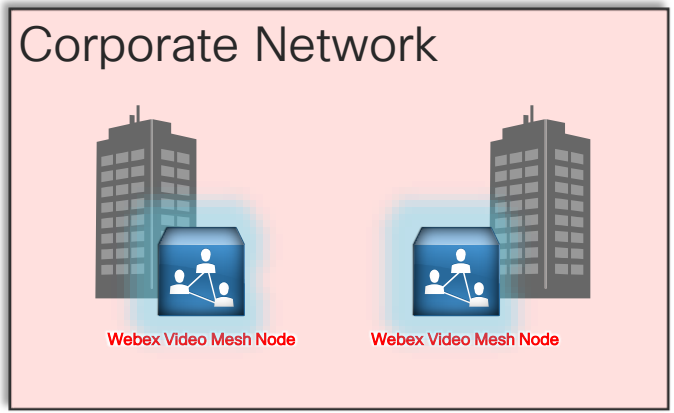


Webex Video Mesh

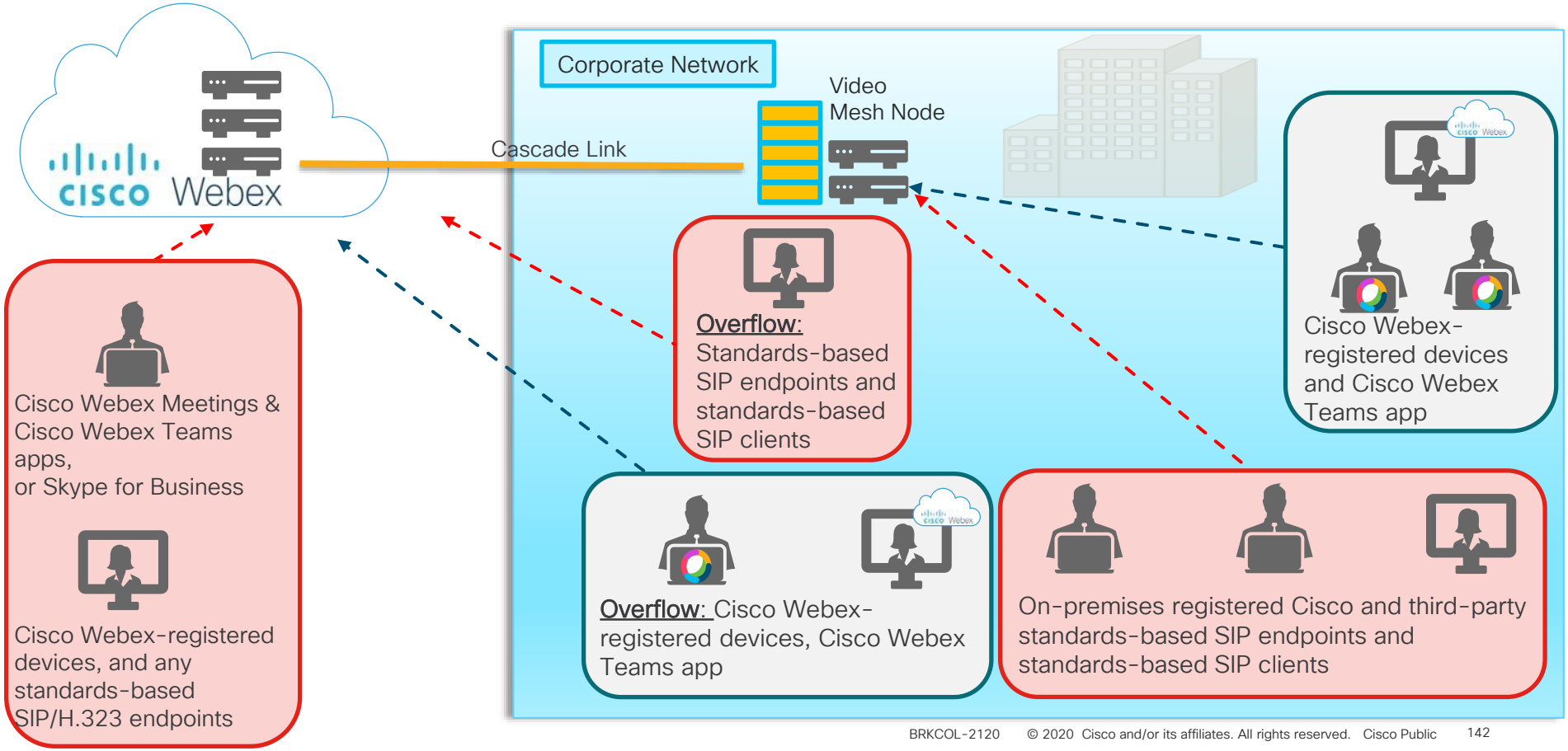
What is it?

- 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

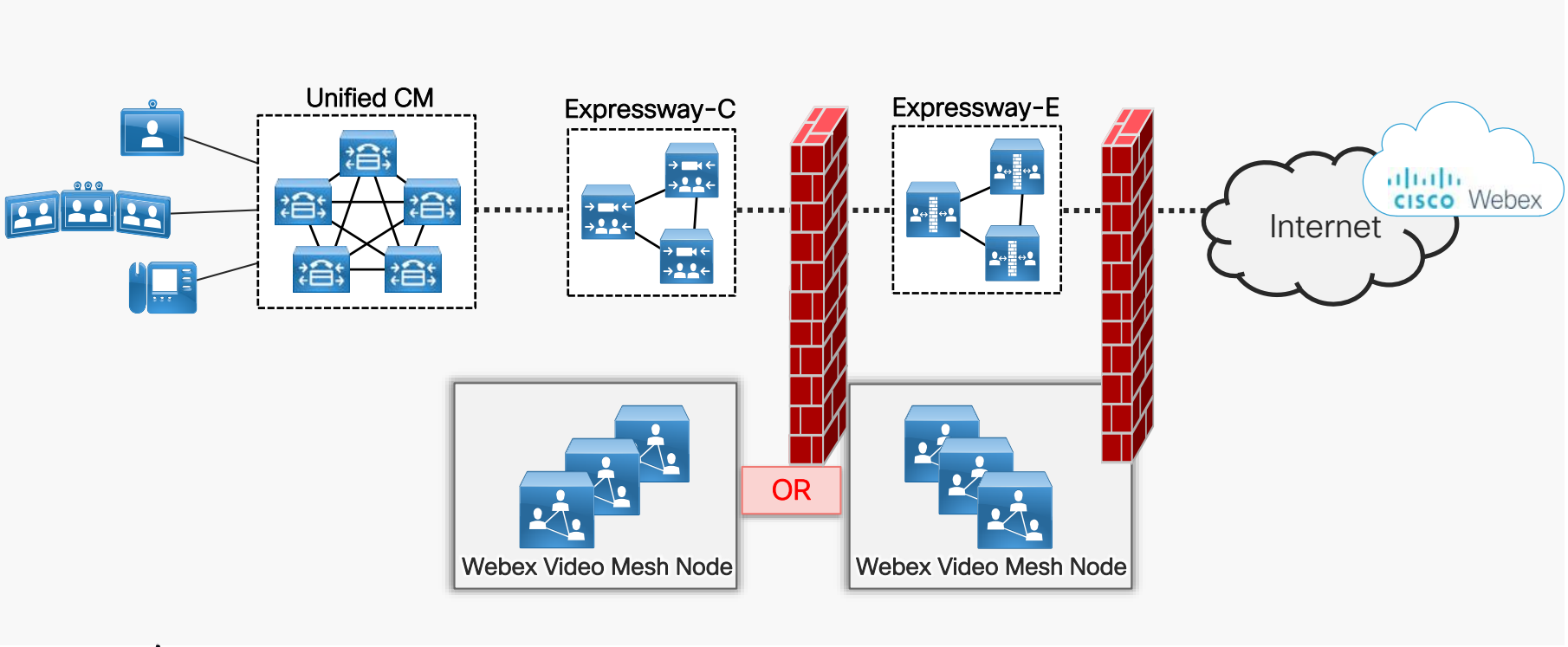




Cisco Webex Video Mesh

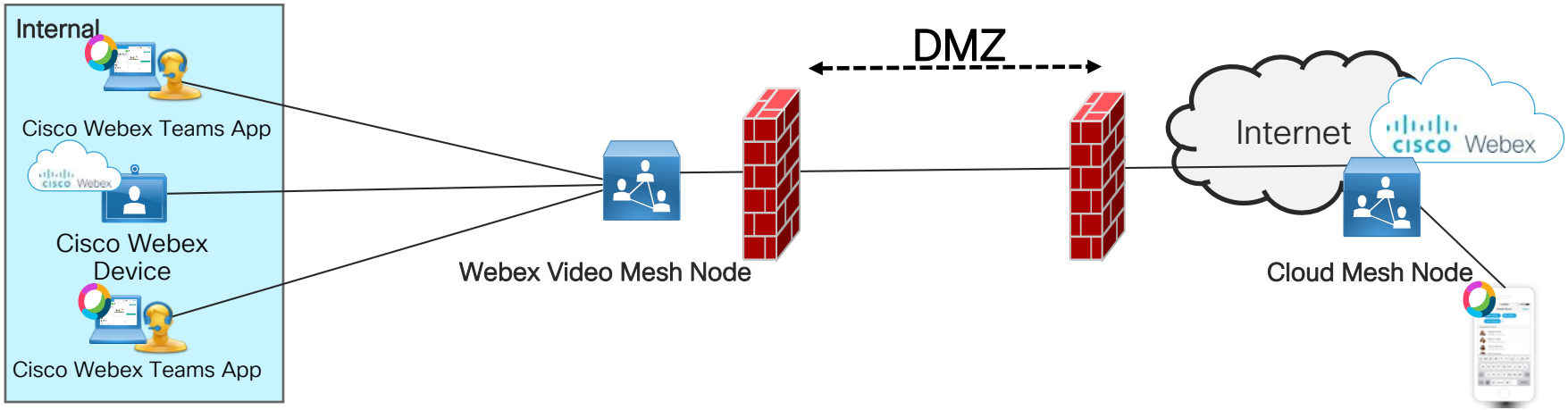


Architecture
Webex Video Mesh



Architecture

Webex Video Mesh – Option 1

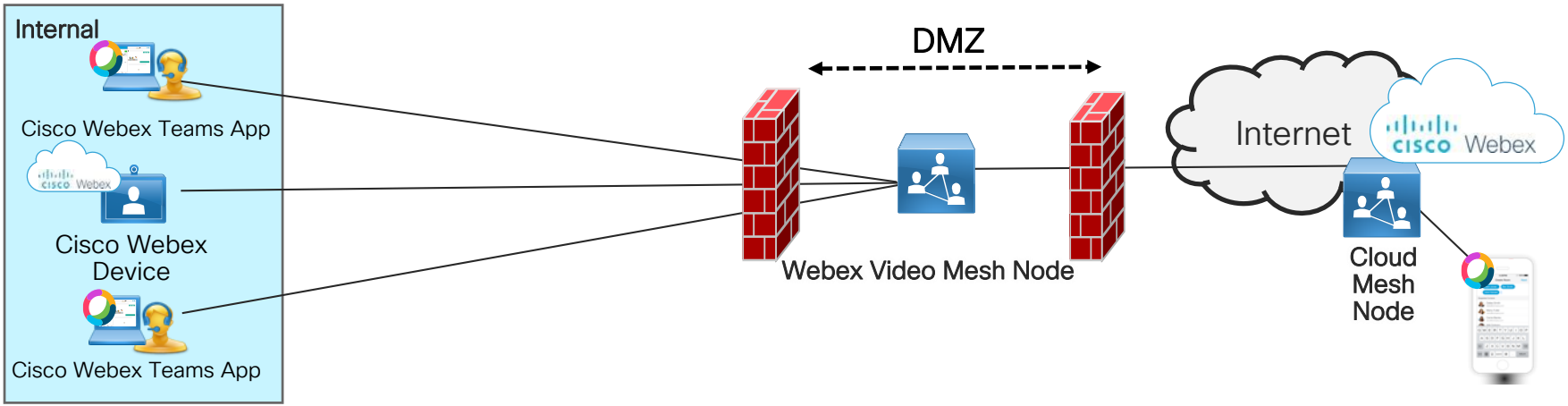


Internal installation considerations:

- 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

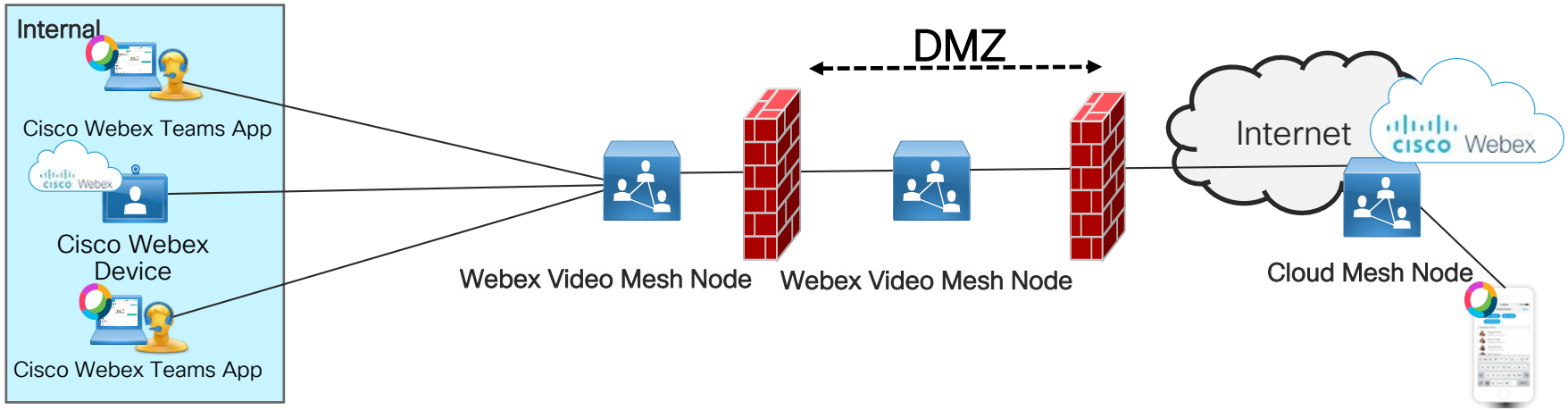


DMZ installation considerations:

- 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

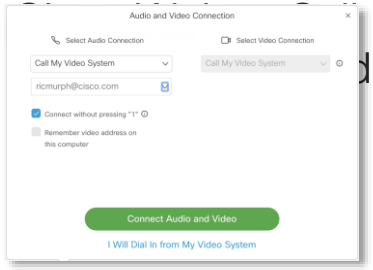
What devices and scenario can the Video Mesh node be used?

Uses the Node

- Any Cisco Webex-registered devi
  - 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 Vide Syste endpoints



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

*Can **NOT** use the Node*

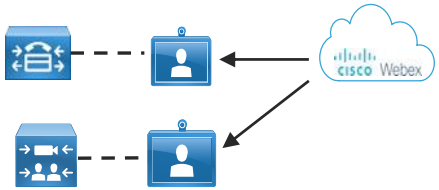
- Webex Teams browser client
  - teams.webex.com

- Webex Calling-registered phones

*Can **NOT** use the Node*

- Webex Meetings app

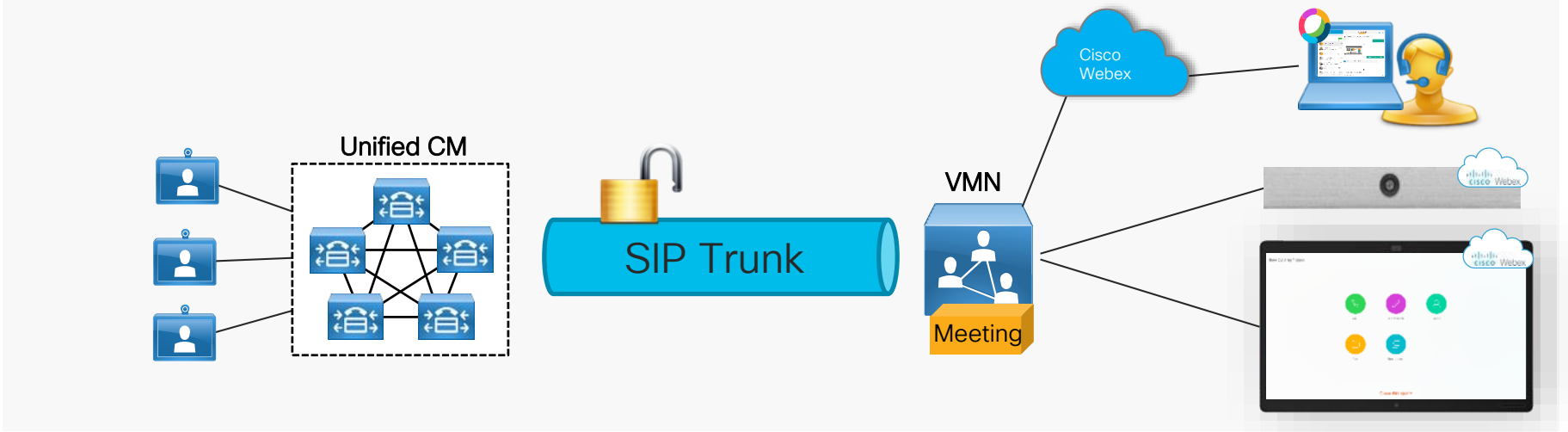
- Cisco Webex Call My Video System to premises-registered endpoints



VMN = Webex Video Mesh Node

Call Control Connectivity

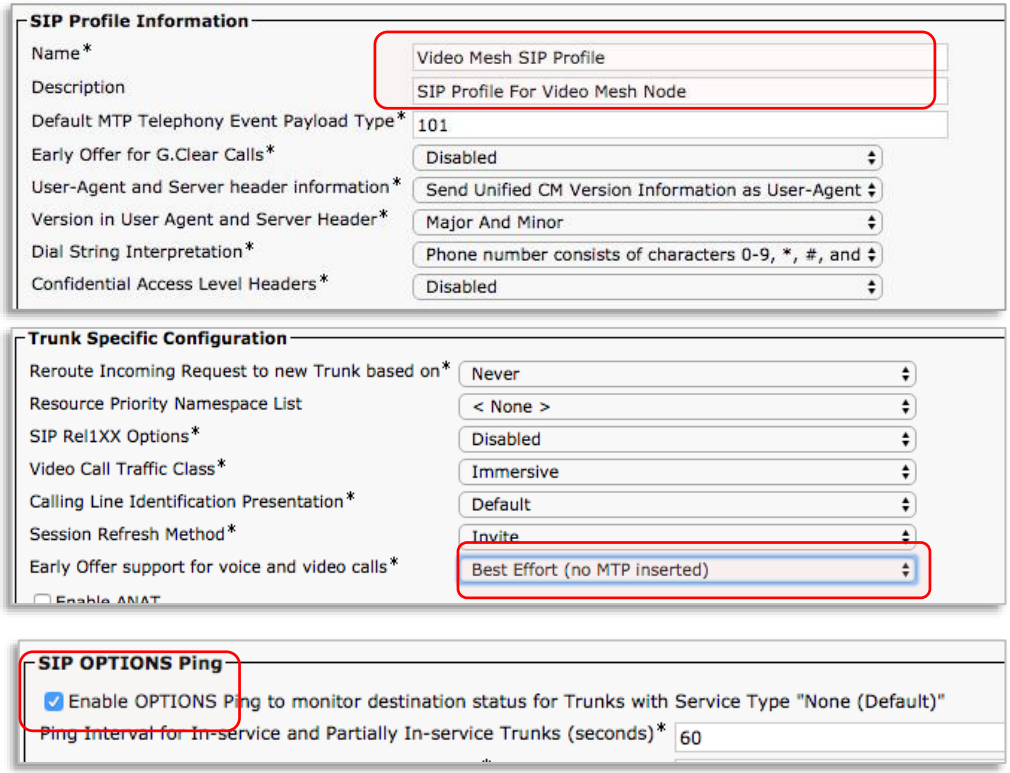
Cisco Unified Communications Manager



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

Unified CM Configuration
SIP Profile

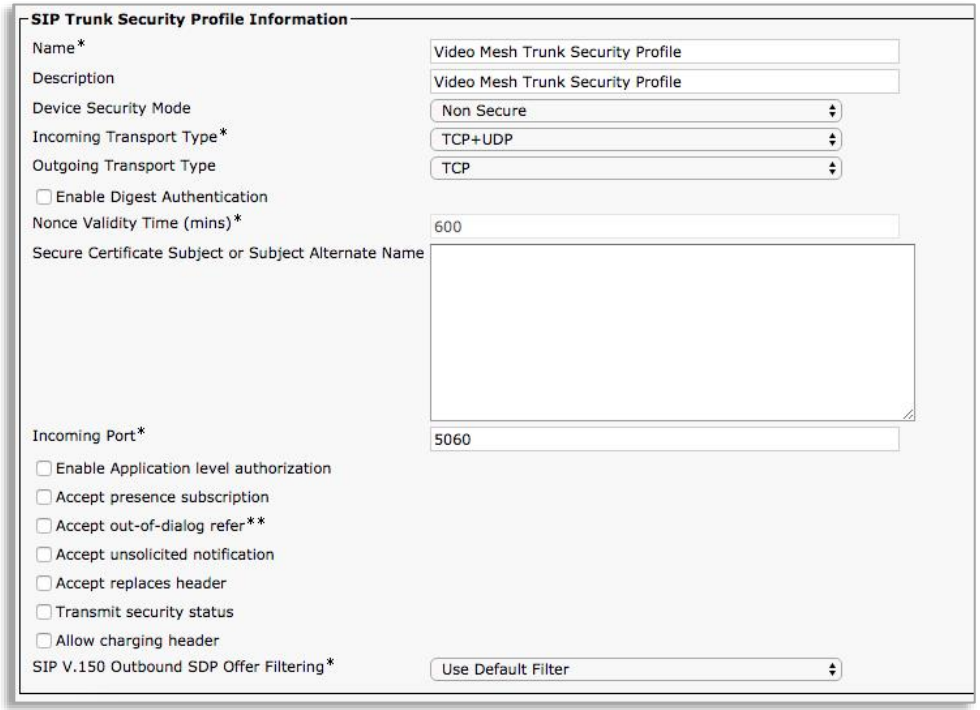
- Create a SIP Profile for VMN
  - Modify Early Offer Support to
    - "Best Effort (no MTP inserted)"
  - Make sure SIP Options Ping is Enabled (default setting)



Unified CM Configuration

SIP Trunk Security Profile

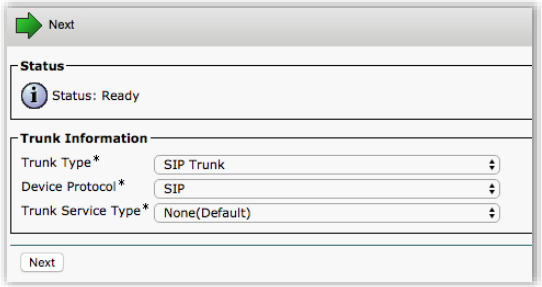
- Create a new SIP Trunk Security Profile
- Add appropriate name and description
- Use default settings

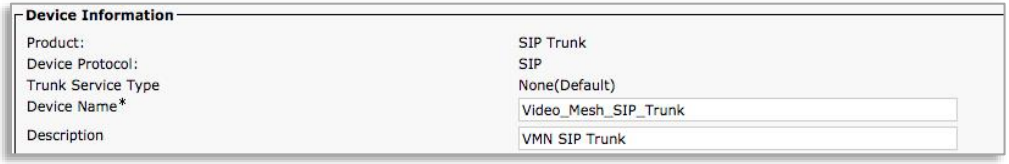


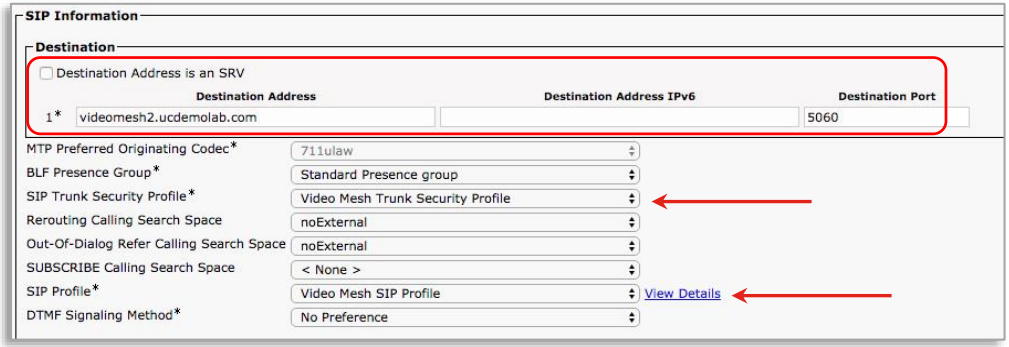
Unified CM Configuration

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.



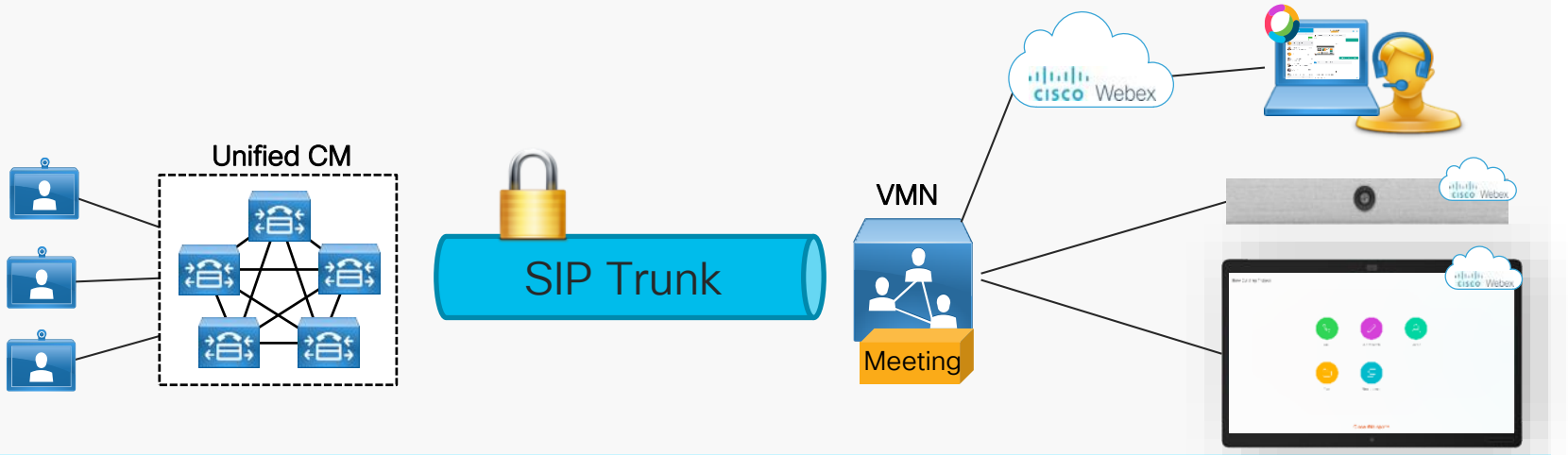




VMN = Webex Video Mesh Node

Call Control Connectivity

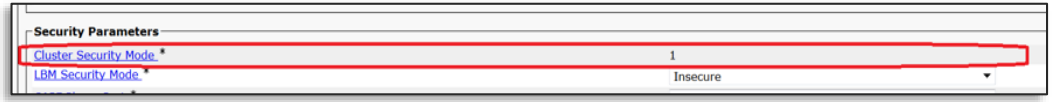
Unified Communications Manager



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

Secured Media & Signaling to CUCM

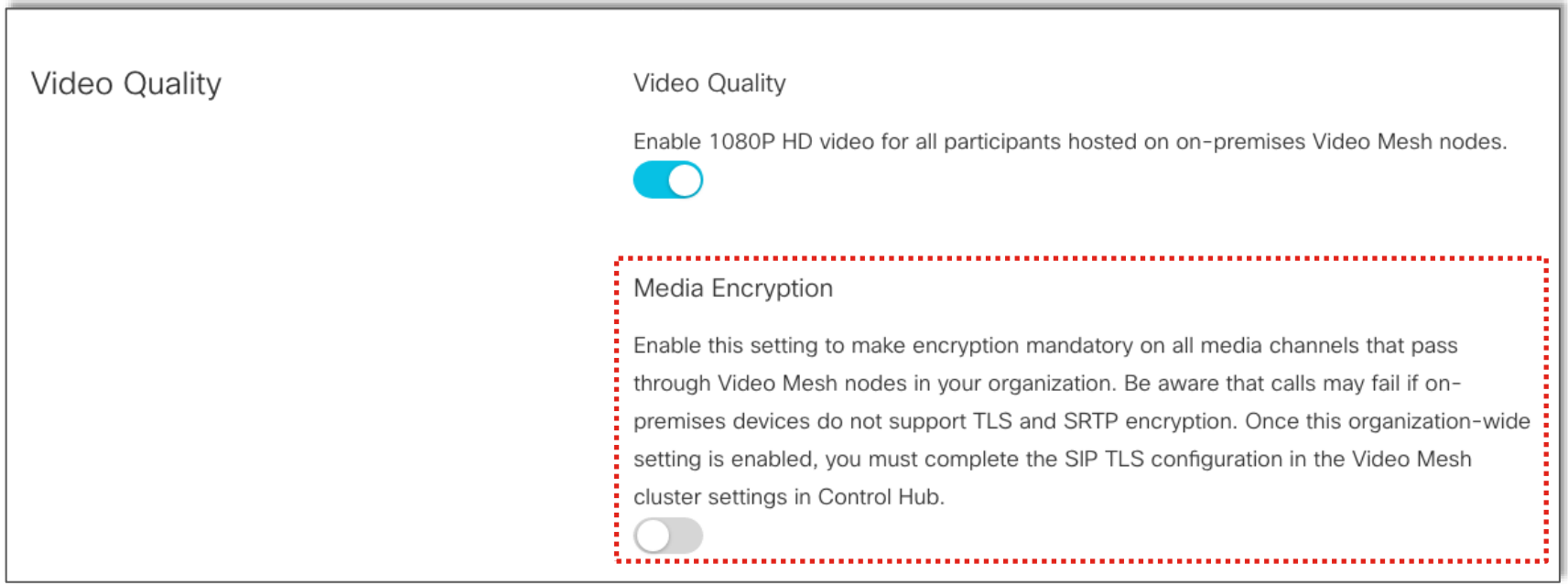
- Secured trunk between CUCM & VMN
  - CUCM in Mixed Mode.



- 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.

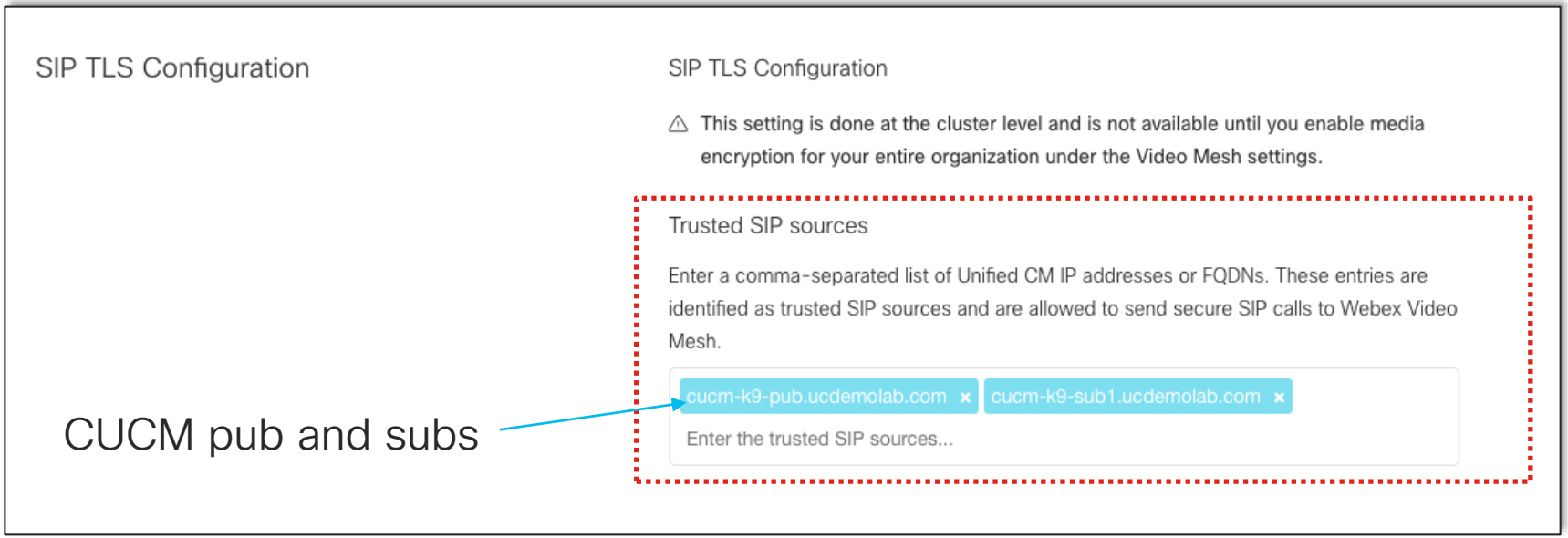
SIP over TLS Trunk

Video Mesh -> Settings



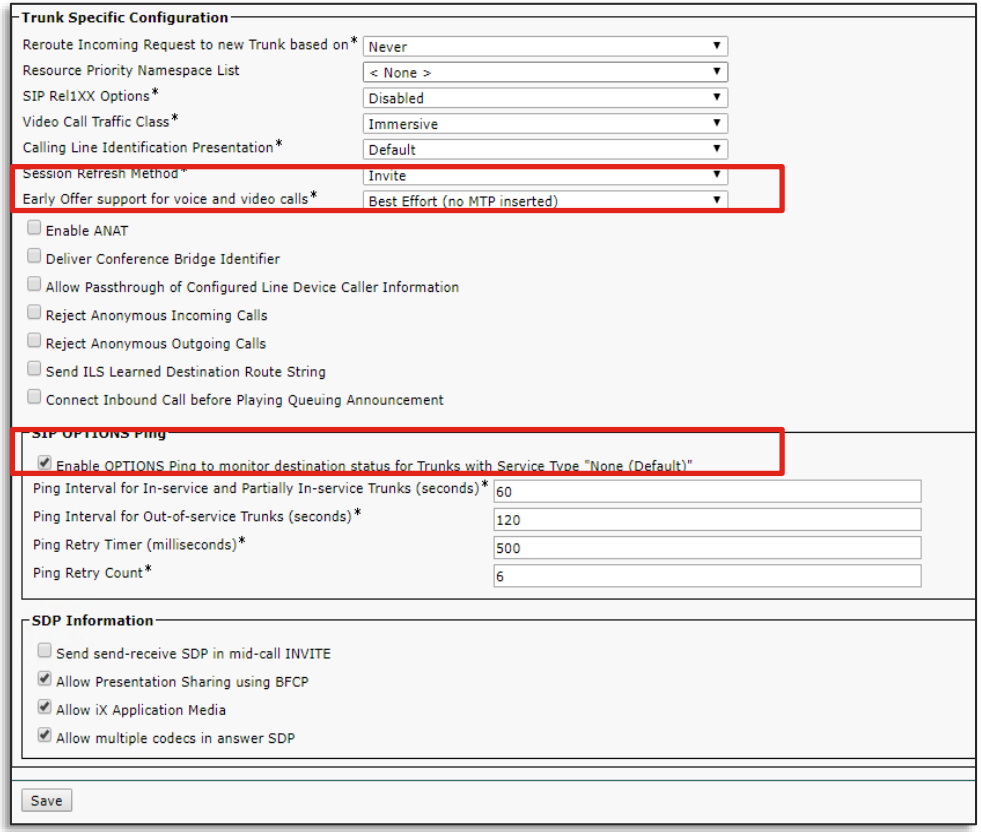
SIP over TLS Trunk

Video Mesh -> Cluster Settings

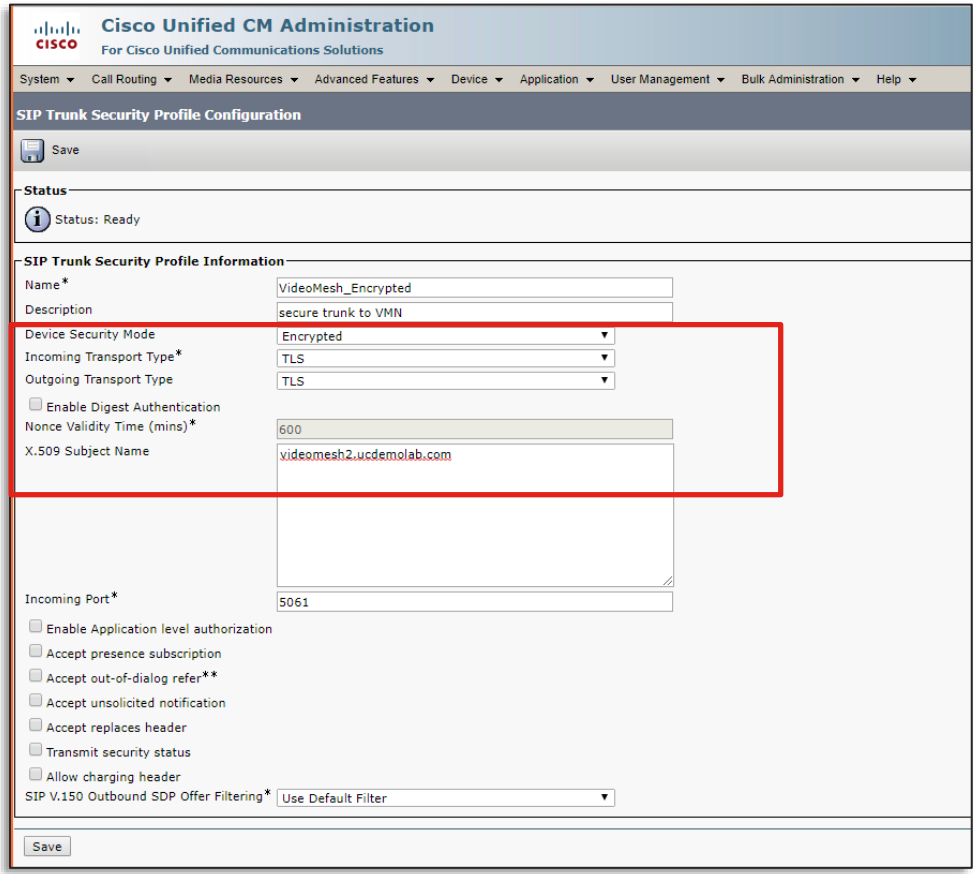


SIP over TLS – SIP Profile

- 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.

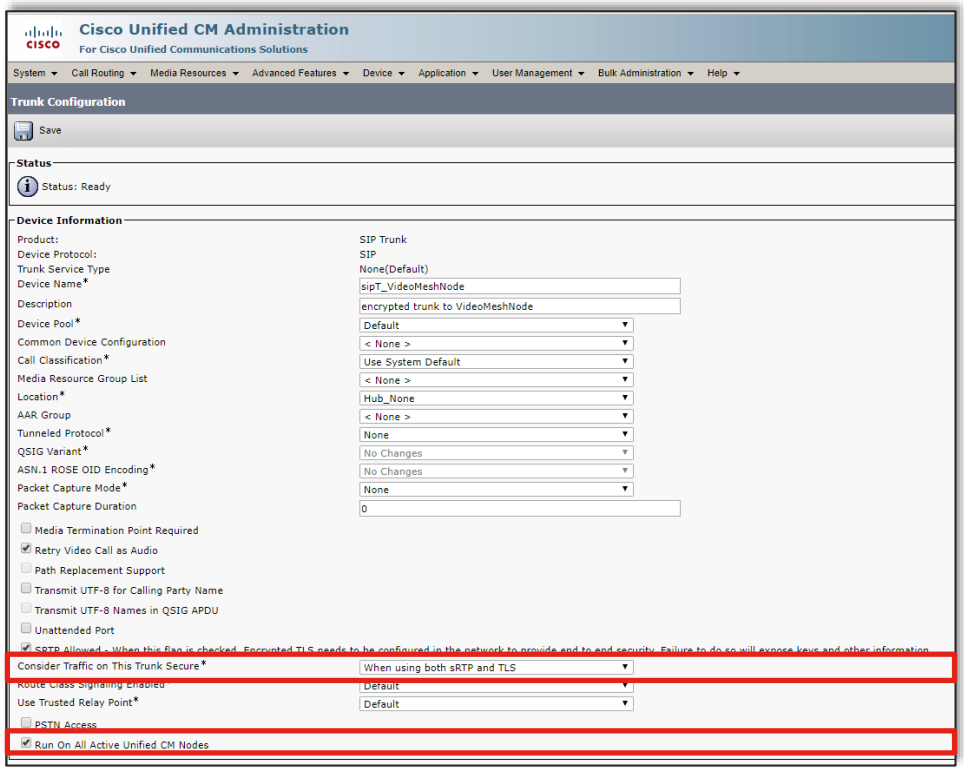


SIP over TLS – Trunk Security Profile



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

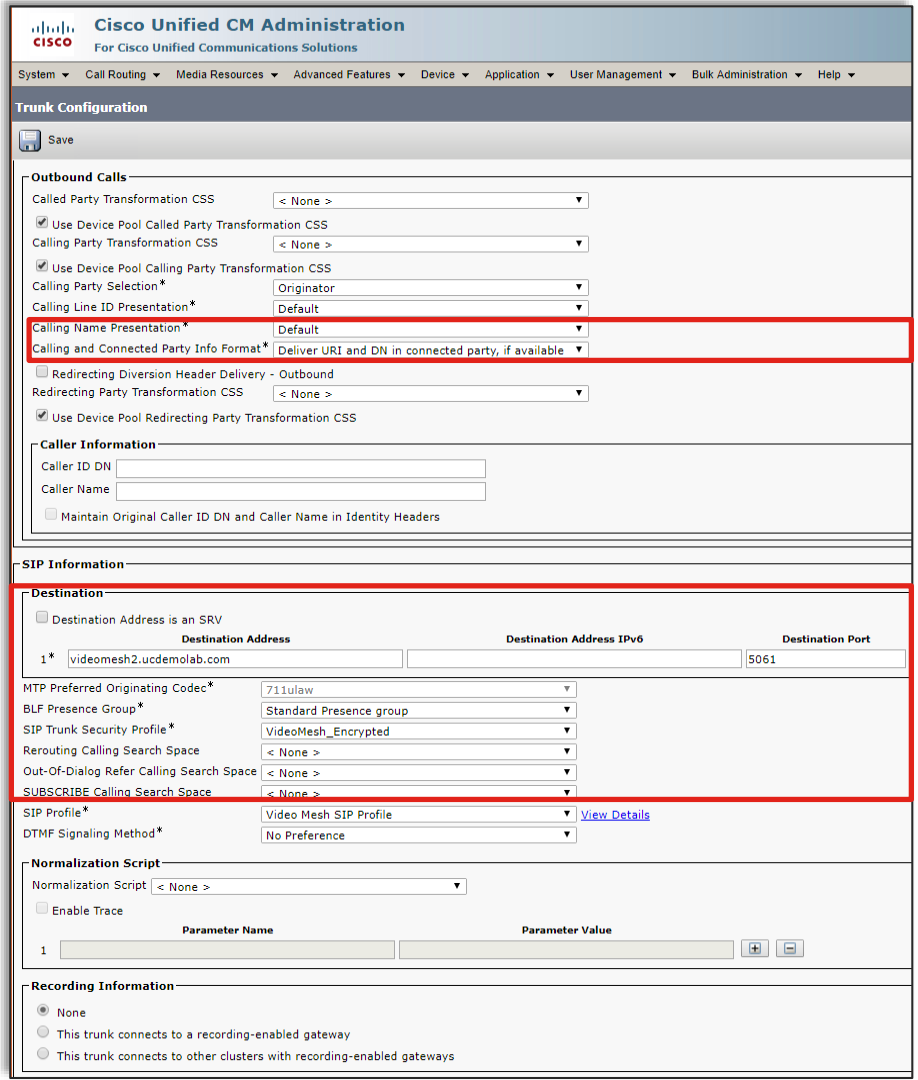
SIP over TLS – Trunk Config



- 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

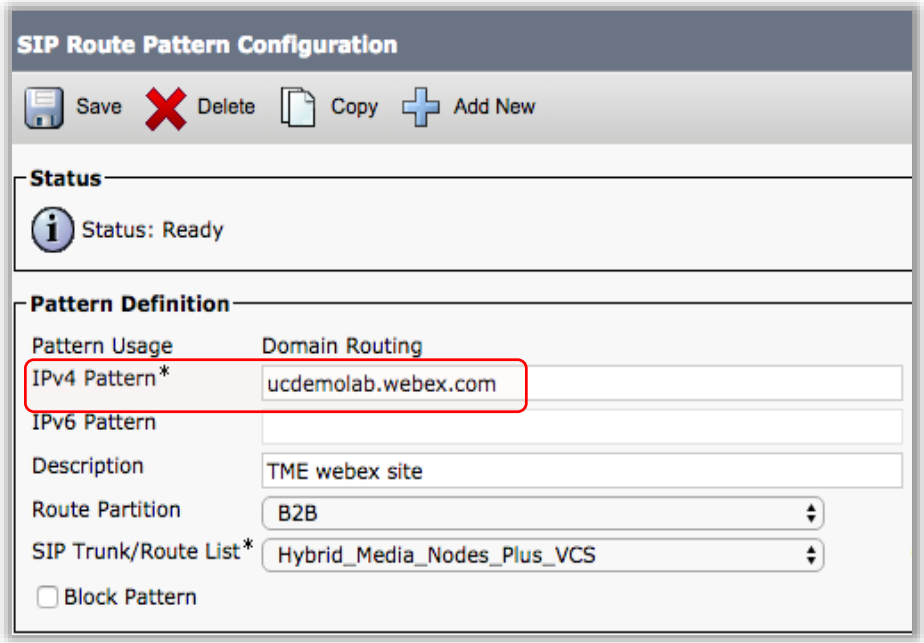


cisco Live!

Unified CM Configuration

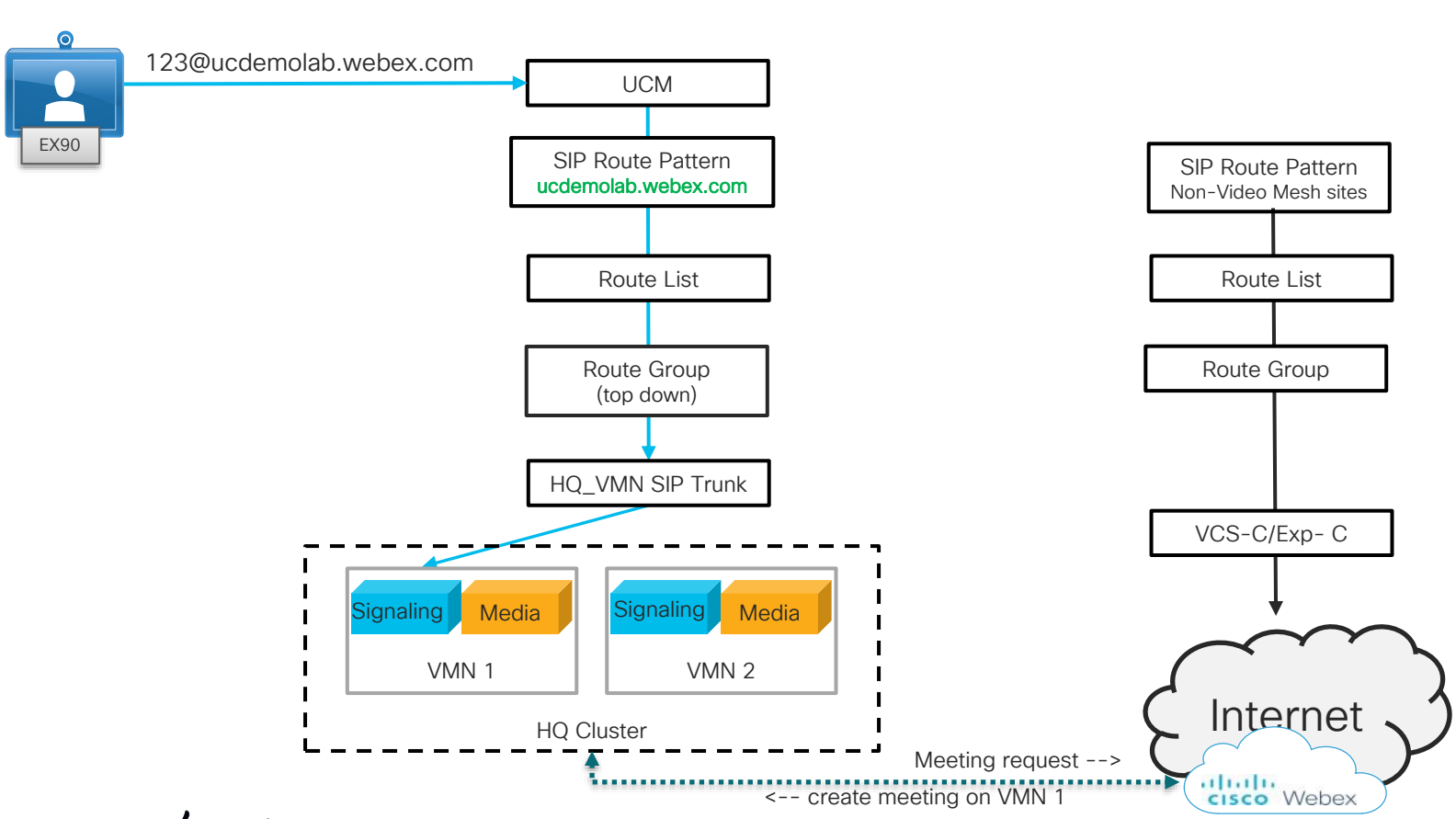
SIP Route Pattern

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



SIP Dial-in Flow to VMN

Ucdemolab = Webex sitename

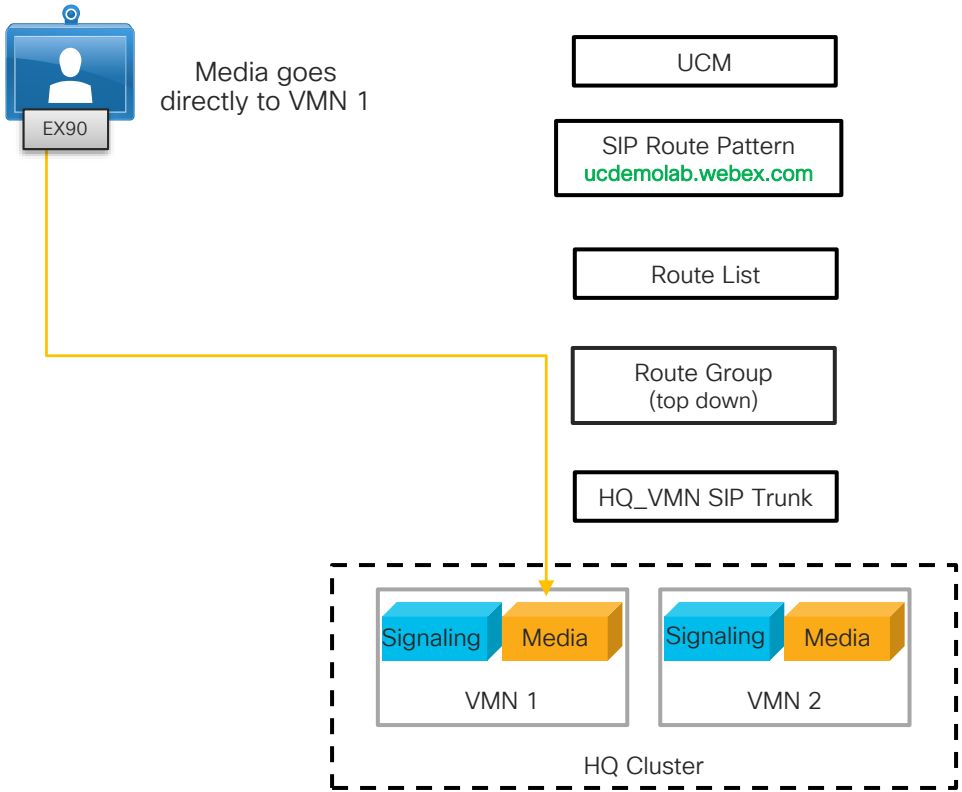


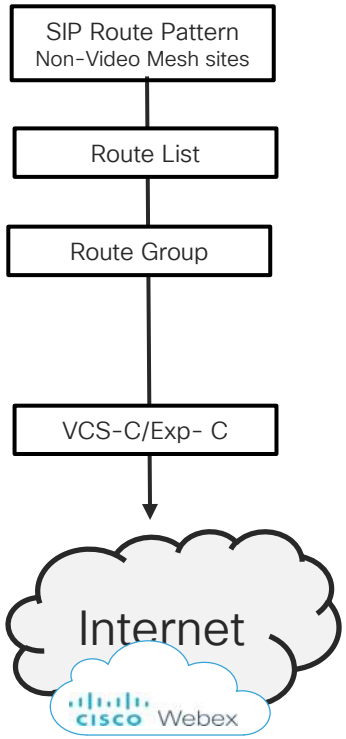
SIP Dial-in Flow to VMN

Ucdemolab = Webex sitename

Signaling

Media



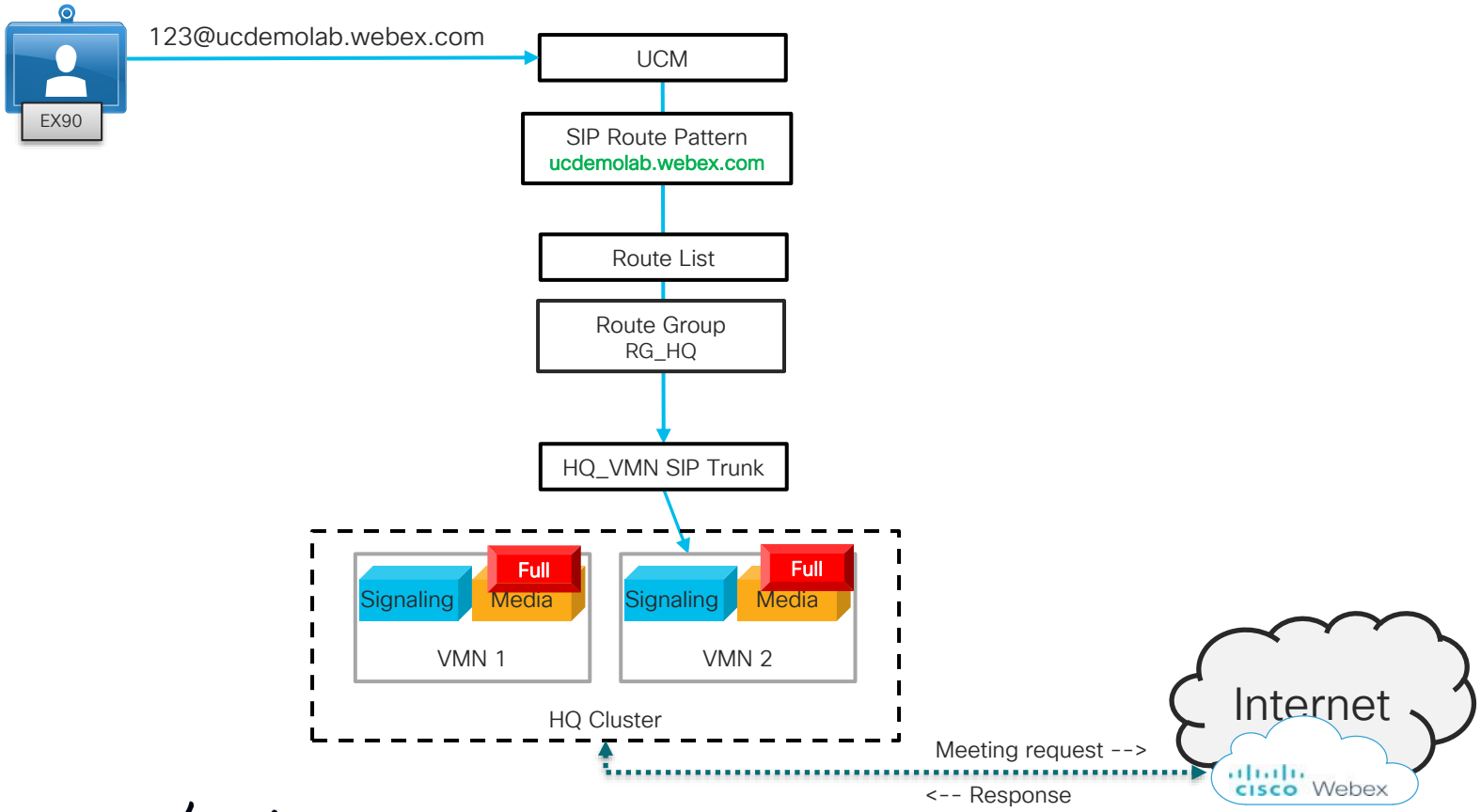


SIP Dial-in Flow to VMN

Ucdemolab = Webex sitename

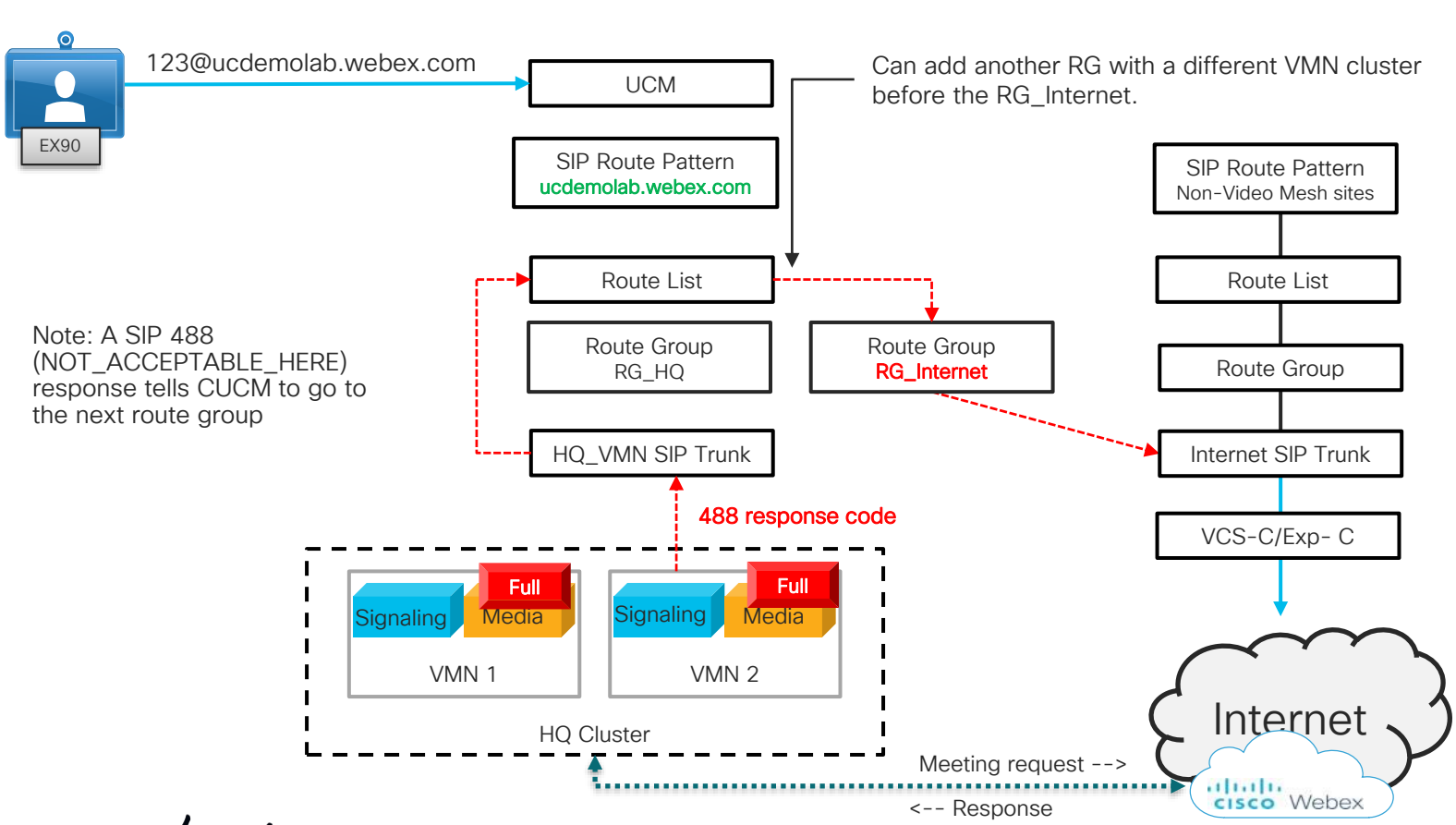
Signaling

Media



SIP Dial-in Flow to VMN

ucdemolab = Webex sitename



Note: A SIP 488 (NOT_ACCEPTABLE_HERE) response tells CUCM to go to the next route group

SIP Dial-in Flow to VMN

Ucdemolab = Webex sitename

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

UCM

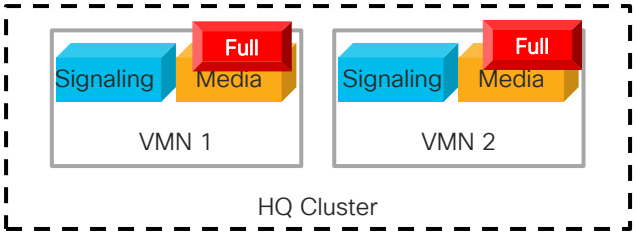
SIP Route Pattern
ucdemolab.webex.com

Route List

Route Group
RG_HQ

Route Group
RG_Internet

HQ_VMN SIP Trunk



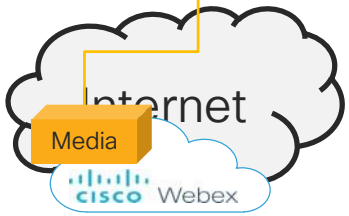
SIP Route Pattern
Non-Video Mesh sites

Route List

Route Group

Internet SIP Trunk

VCS-C/Exp- C



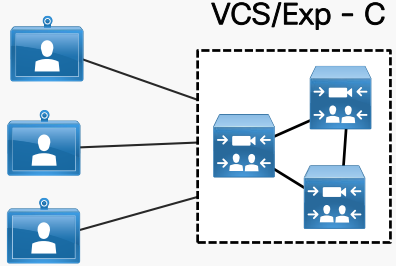
Signaling

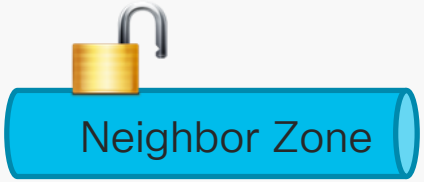
Media

VMN = Webex Video Mesh Node

Call Control Connectivity

VCS/EXP - C

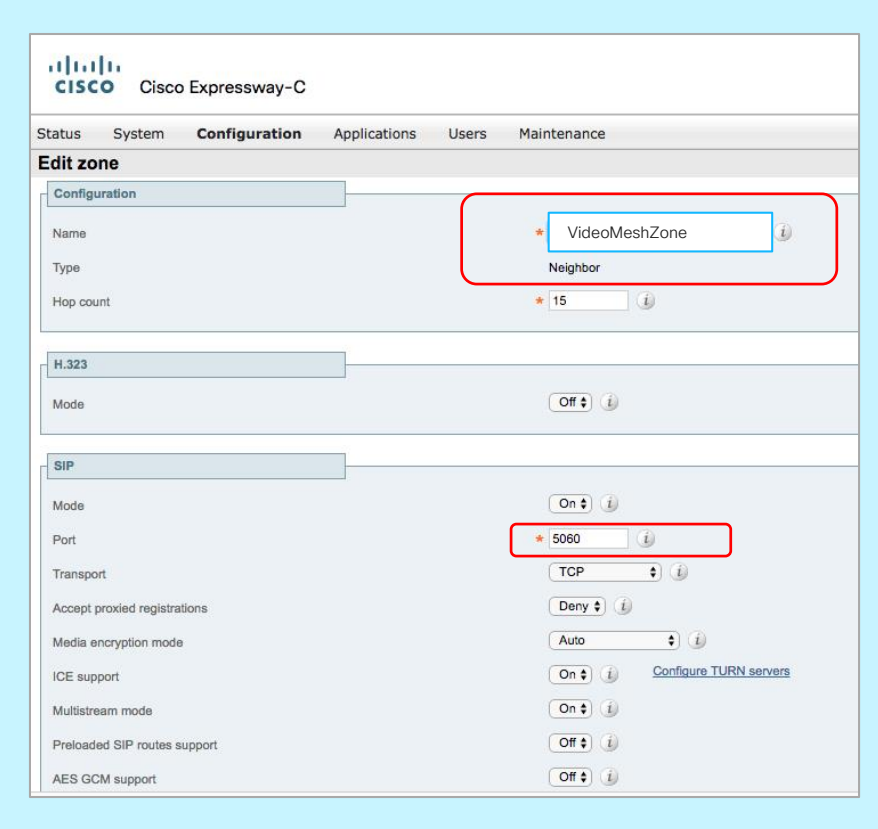




- Supported with VCS or Expressway X8.11.4 or higher

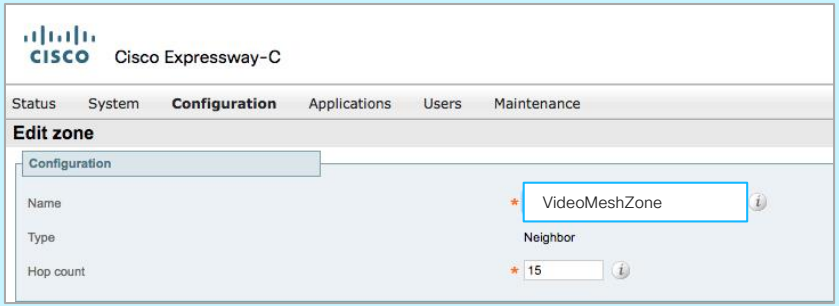
Expressway – C
Neighbor Zone Creation

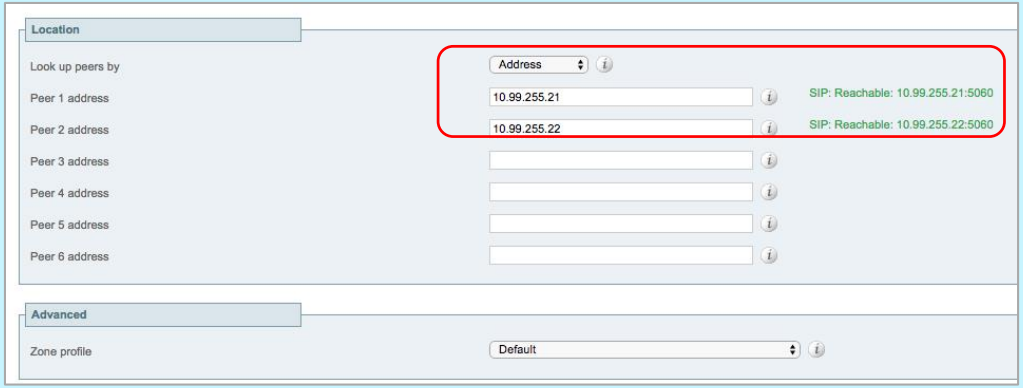
- Create a neighbor zone for Webex Video Mesh Node
  - Configuration > Zones > Zones, and then click New
  - 5060 support only



Expressway – C
Neighbor Zone Creation

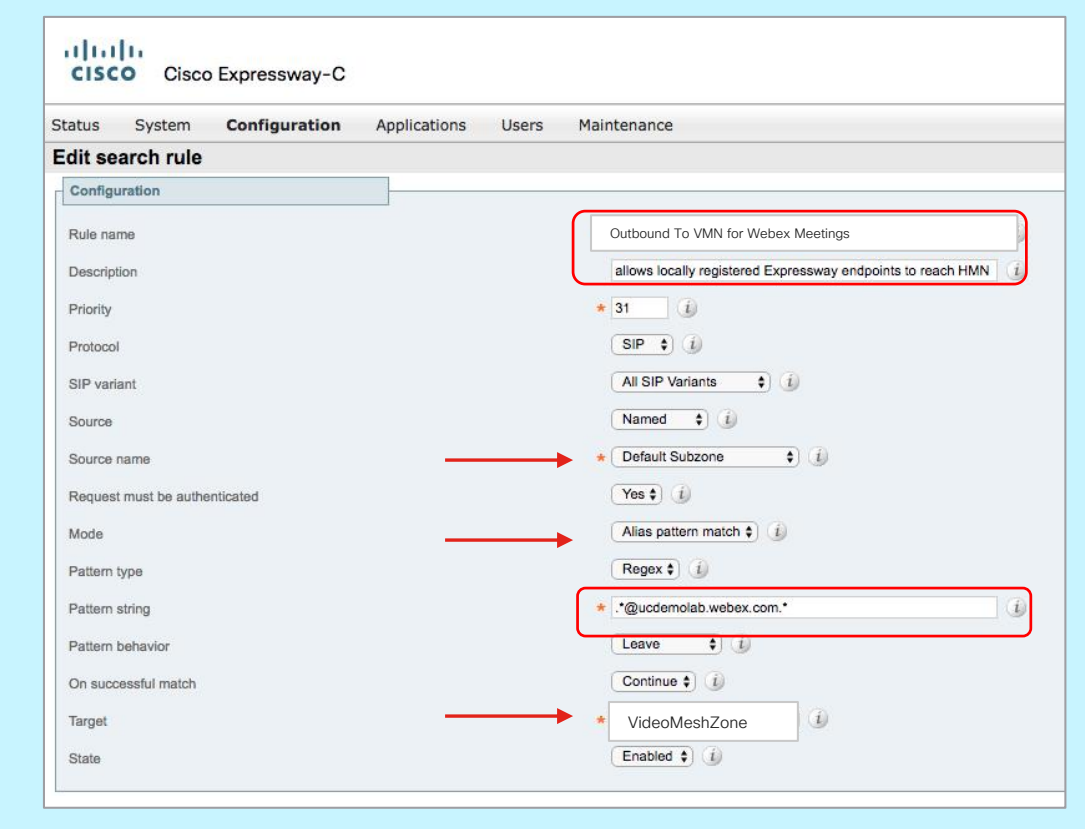
- Create a neighbor zone for Webex Video Mesh Node
  - Configuration > Zones > Zones, and then click New
- Add Webex Video Mesh Nodes



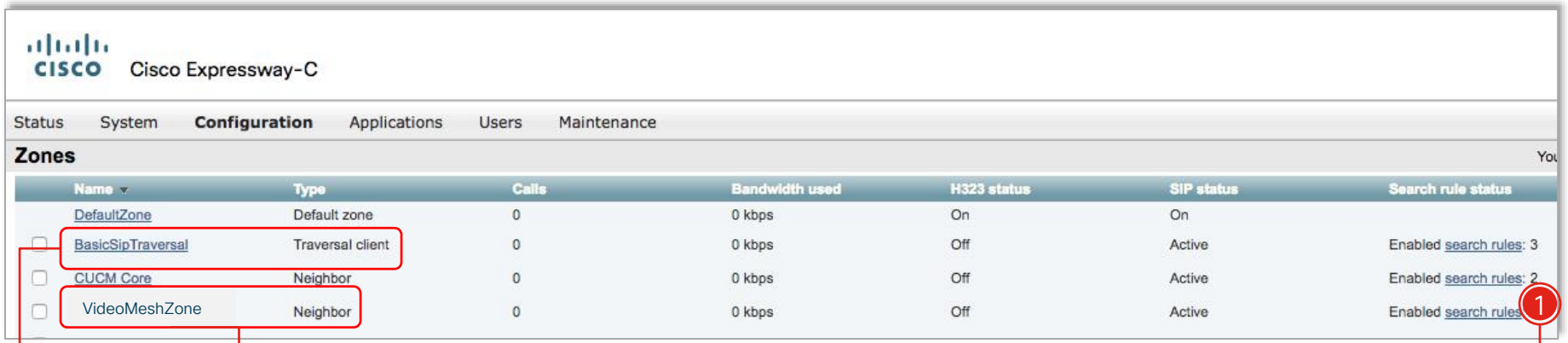


Expressway – C
Search Rule

- 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.*



Expressway – C
Zones



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

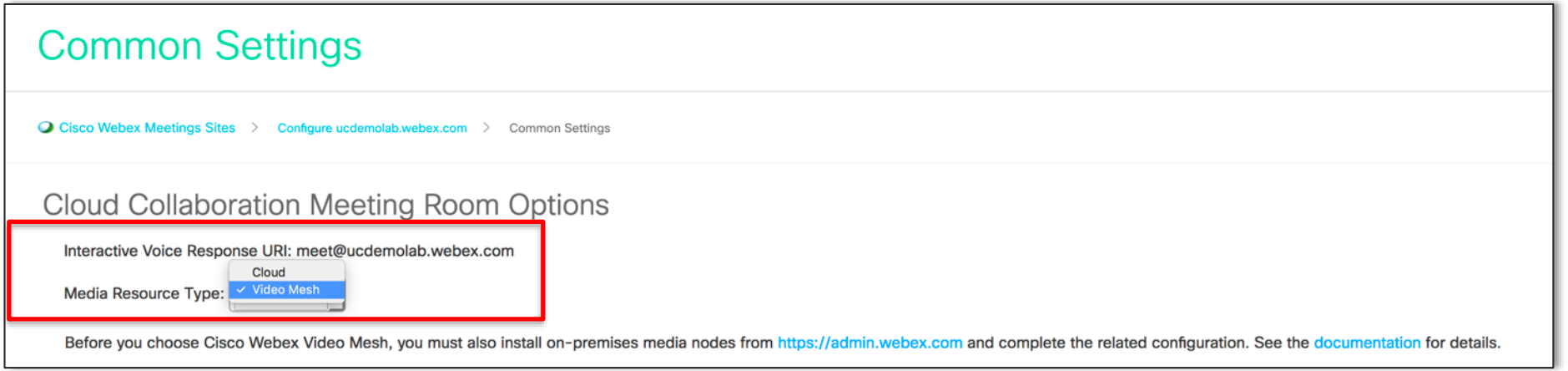
Enable Video Mesh support on Cisco Webex site

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.

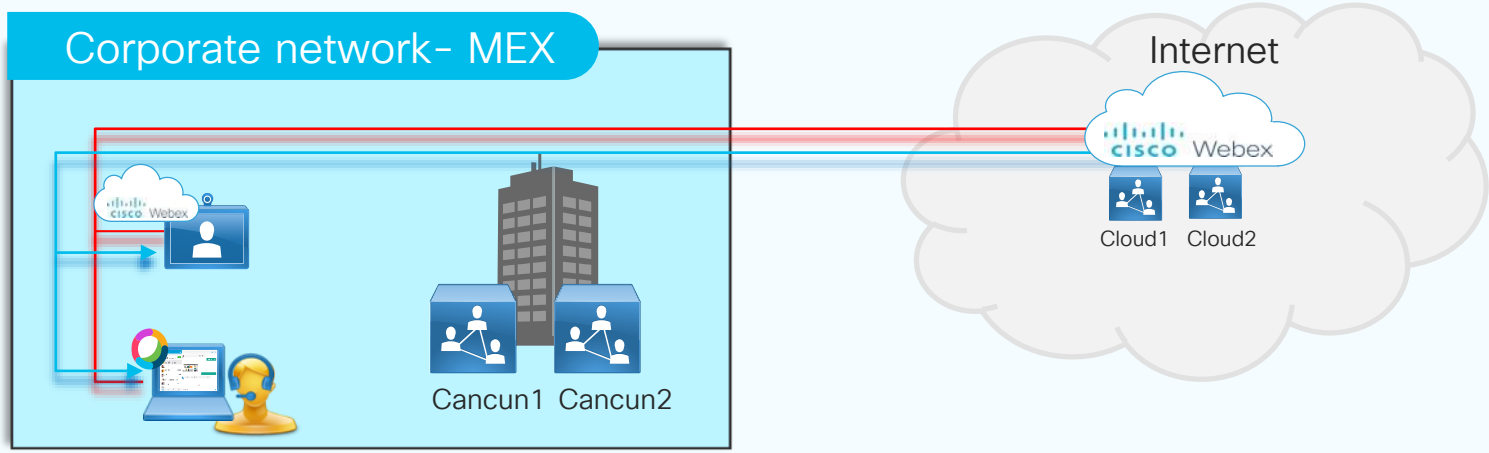
Media Resource Type

- Cloud (default)
- Video Mesh



Webex Video Mesh Node Discovery – Scenario 1

Scenario 1
Registration



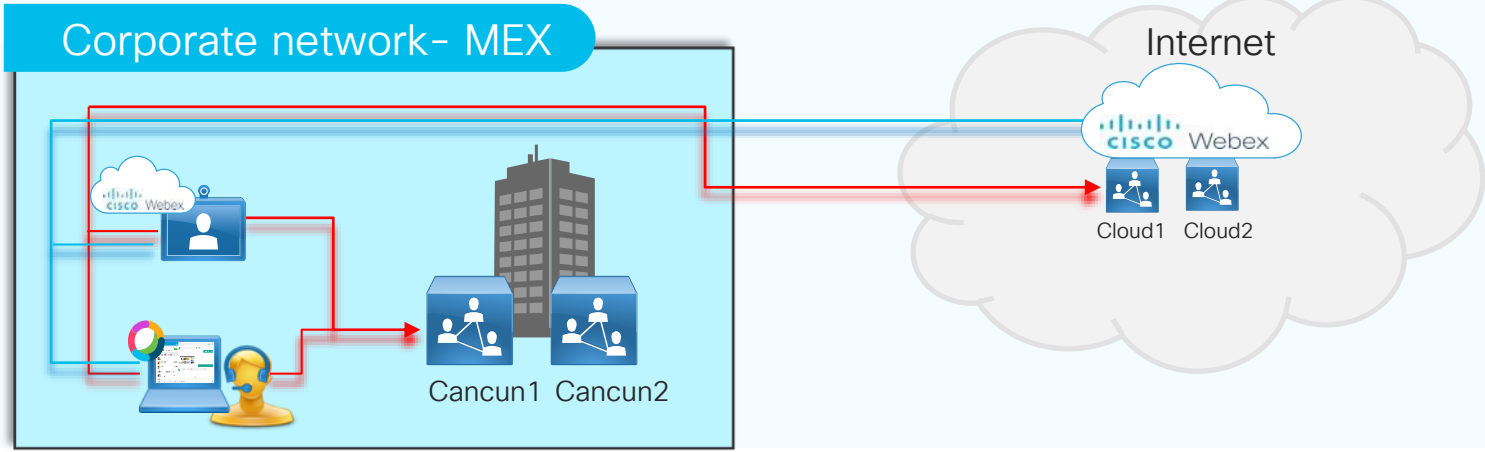
Cisco Webex Teams app and Webex device register to their organization

Cisco Webex responds with the clusters available for the users

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

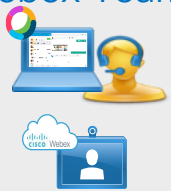
Scenario 1
Reachability Test

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



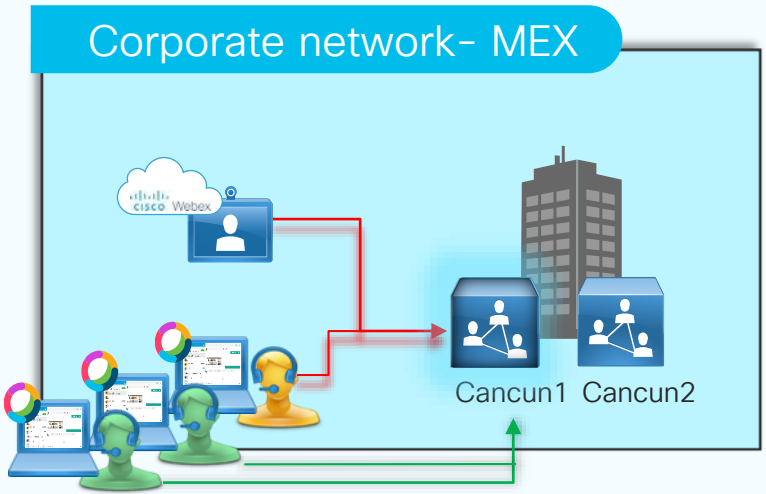
Cisco Webex Teams app and Webex devices do reachability tests to the mesh nodes.

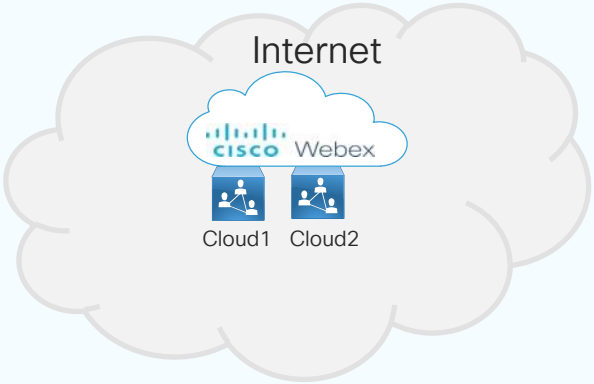
Cisco Webex Teams app and Webex devices sends results to the cloud at call start.



Cluster - Cancun	Cluster - Cloud
1. Node – Cancun1 (RTD = 10) 2. Node – Cancun2 (RTD = 11)	1. Node – Cloud1 (RTD = 220) 2. Node – Cloud2 (RTD = 200)

Scenario 1
Registration





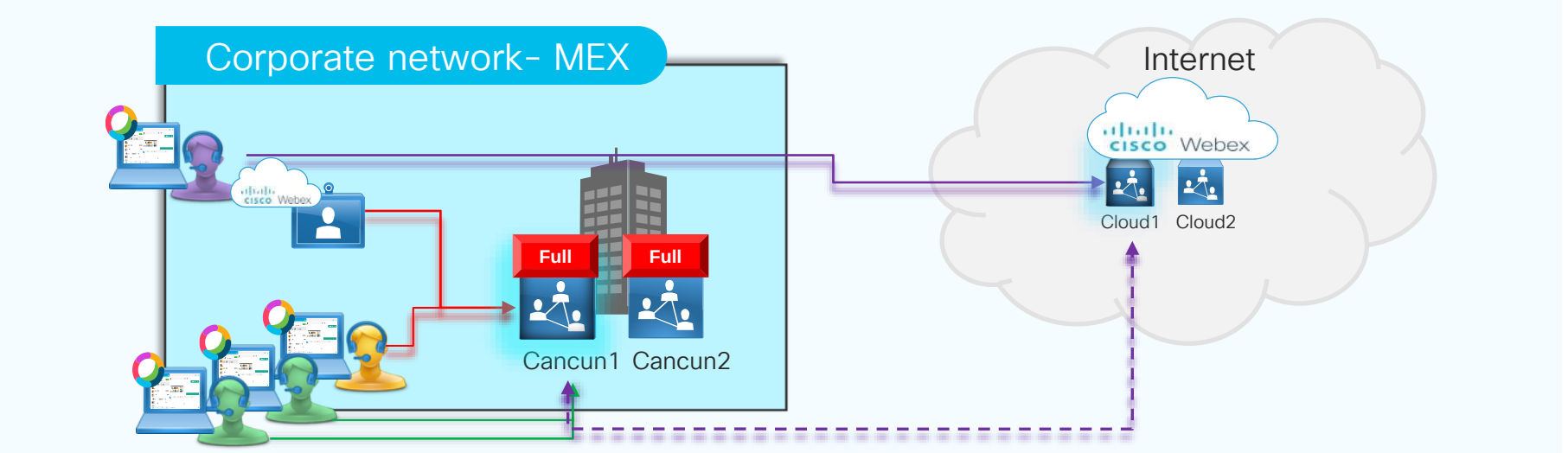
Cisco Webex Teams app and Webex devices connect to a mesh node

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

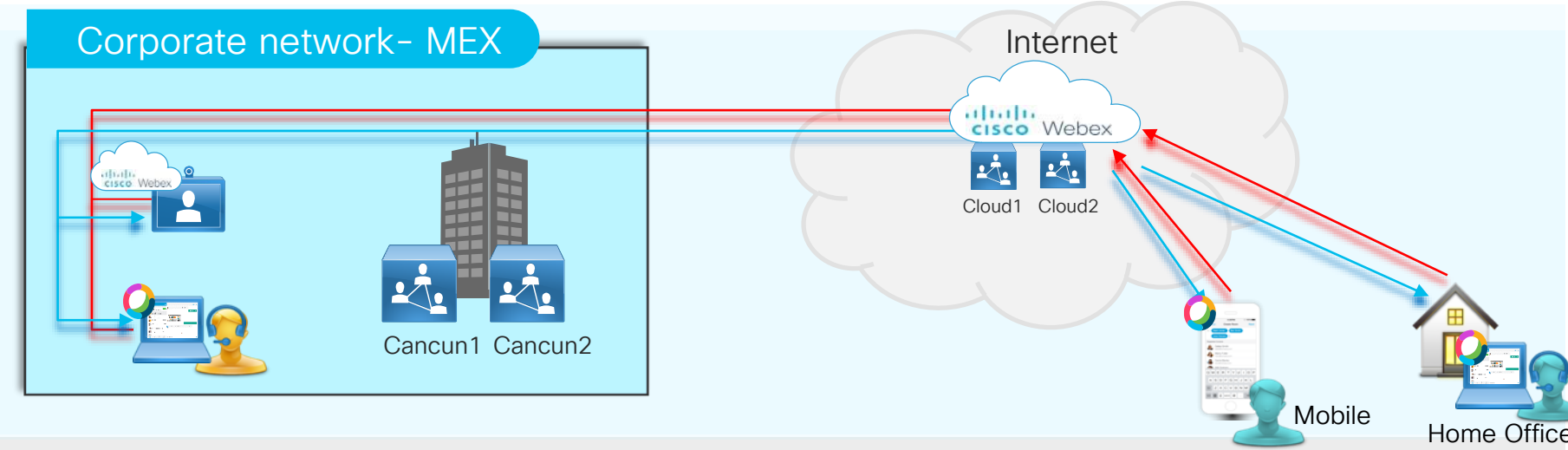
If additional participants join later, they follow the same process

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

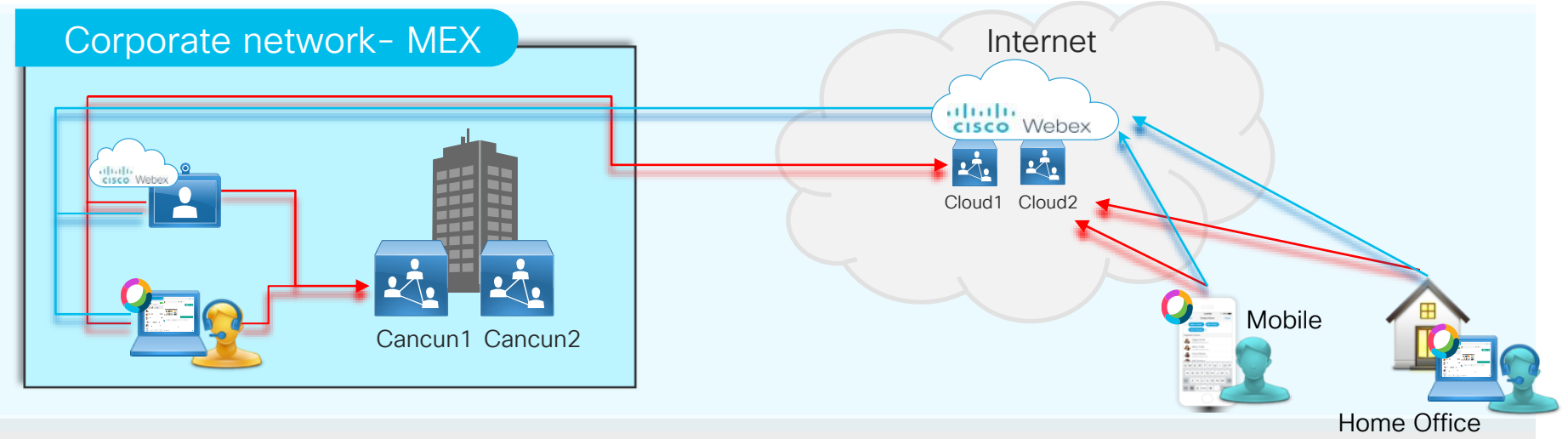


Cisco Webex Teams app and Webex device register to their organization

Cisco Webex responds with the clusters available for the users

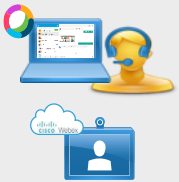
Cluster - Cancun	Cluster - Cloud
1. Node – Cancun1 2. Node – Cancun2	1. Node – Cloud1 2. Node – Cloud2

Scenario 2
Reachability Test



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

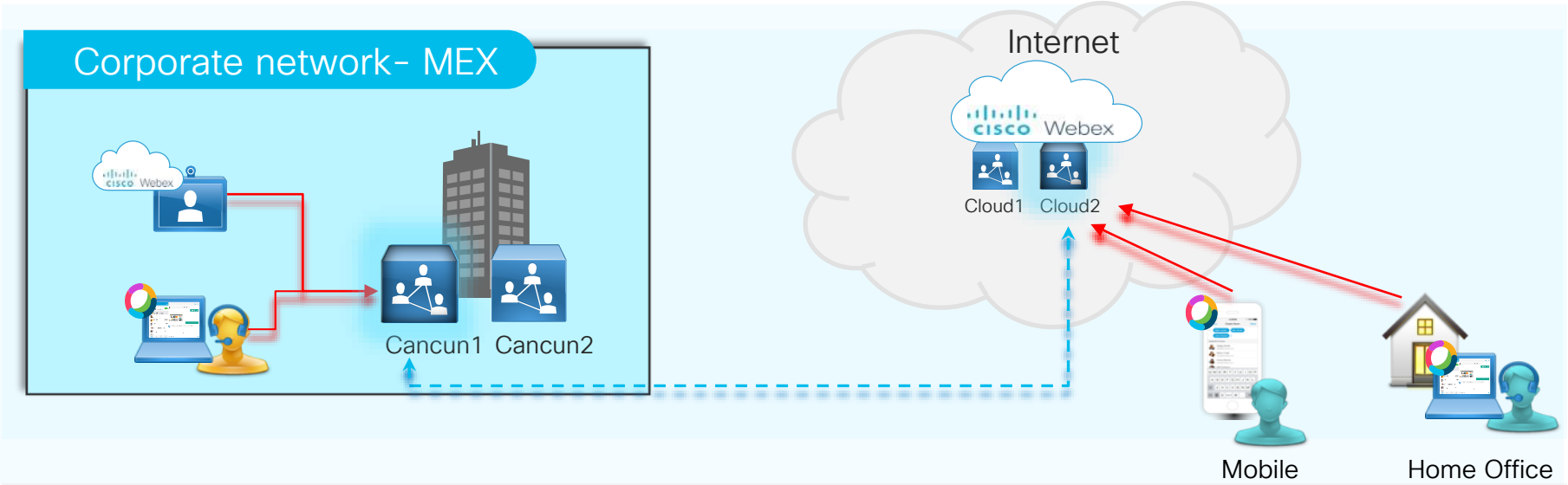
Cisco Webex Teams app and Webex devices sends results to the cloud at call start.



Cluster - Cancun	Cluster - Cloud
1. Node – Cancun1 (RTD = 10) 2. Node – Cancun2 (RTD = 11)	1. Node – Cloud1 (RTD = 220) 2. Node – Cloud2 (RTD = 200)

Scenario 2

Meeting



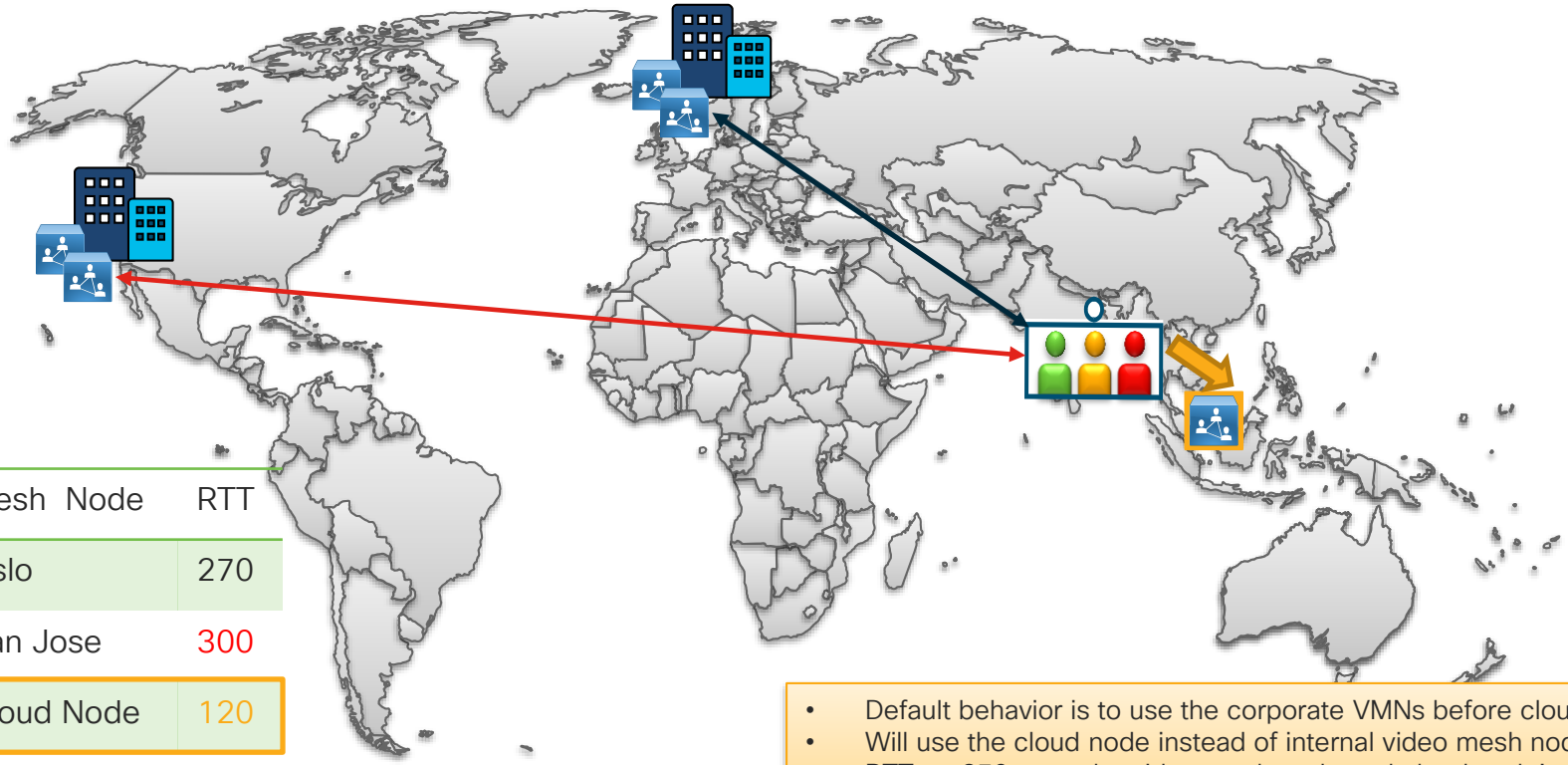
Cisco Webex Teams app and Webex devices connect to a mesh node

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



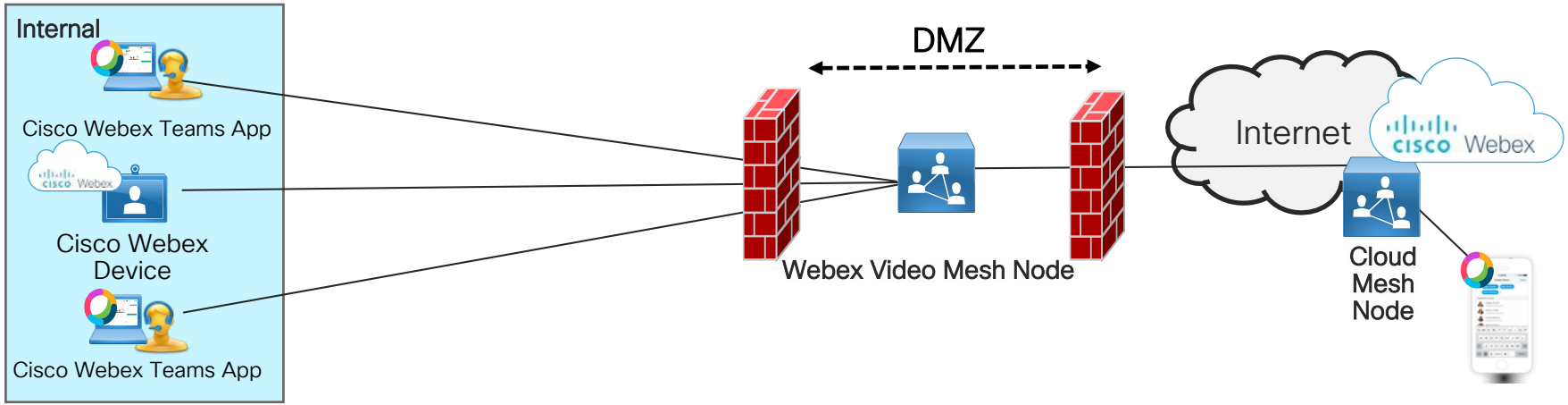
Mesh Node	RTT
Oslo	270
San Jose	300
Cloud Node	120

- 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 >= 250ms 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



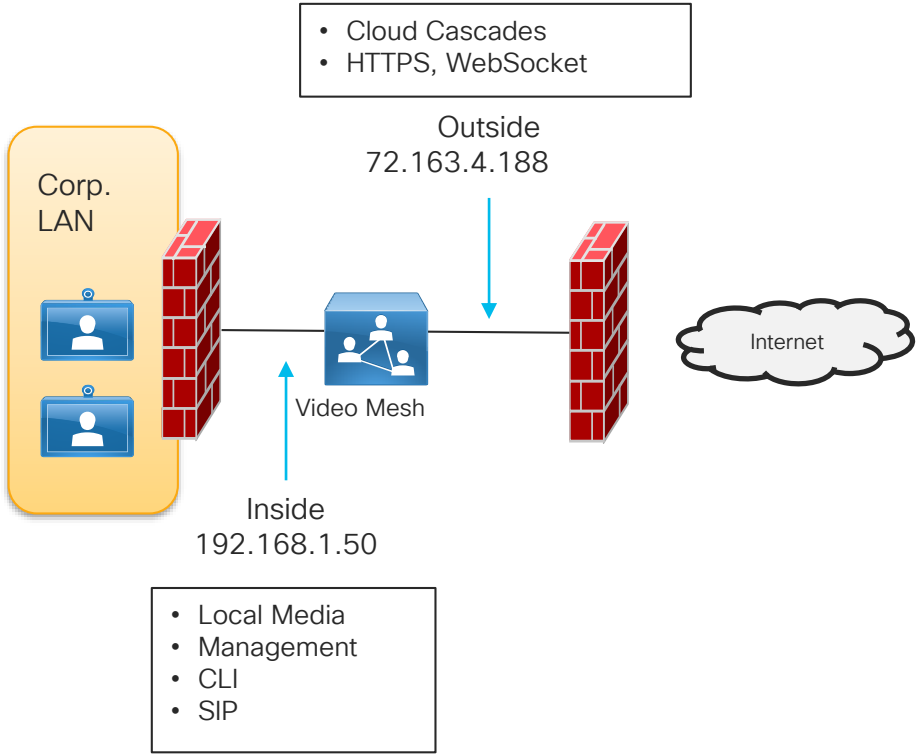
DMZ installation considerations:

- 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

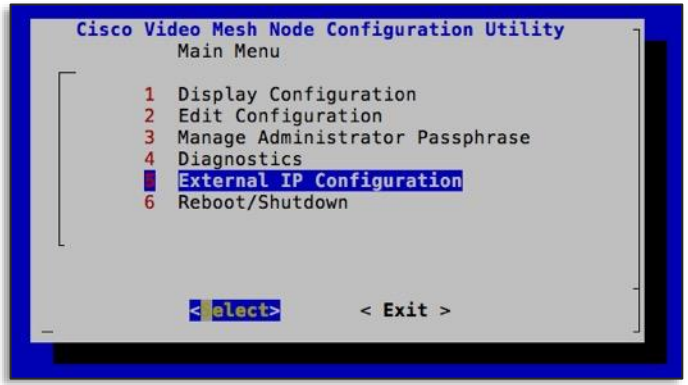
Deployment:

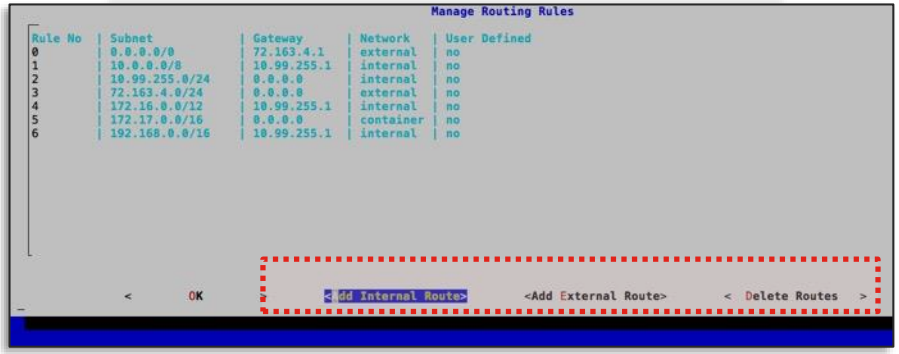
- Require all nodes be the same configuration in the cluster
  - For example dual-NIC only
- Recommend changes be done in maintenance mode
- RFC 1918 address is acceptable on the internal interface only. The external interface needs to be a publicly routable address.
- Use internal IP address for node 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.



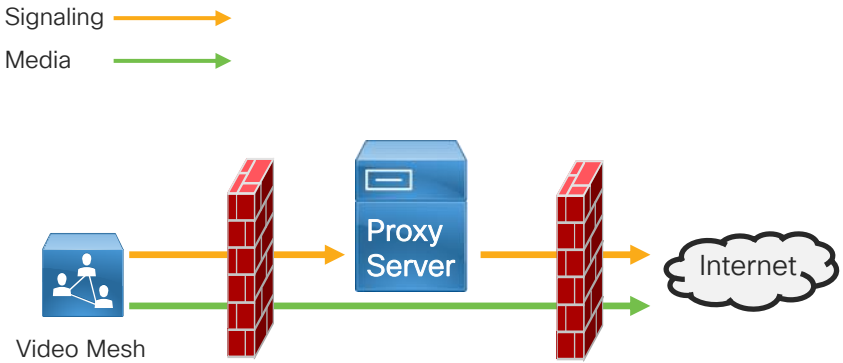
Dual NIC – External IP Configuration

- 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



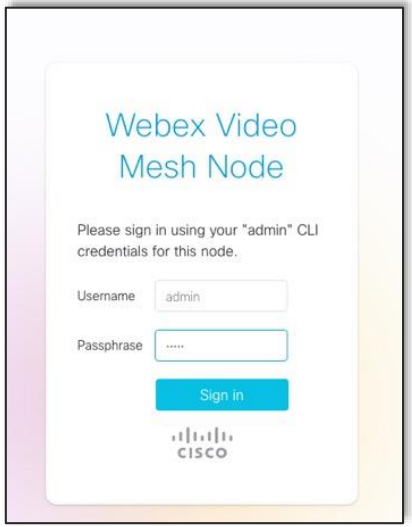
- HTTP(s) signaling support only
  - Ports 443 and 444
- Media goes direct to the cloud
  - UDP port 5004

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

Video Mesh Webpage

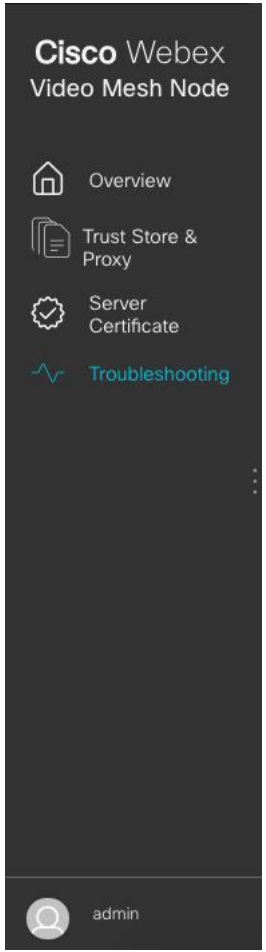
This webpage is available per node

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



What can you view?

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



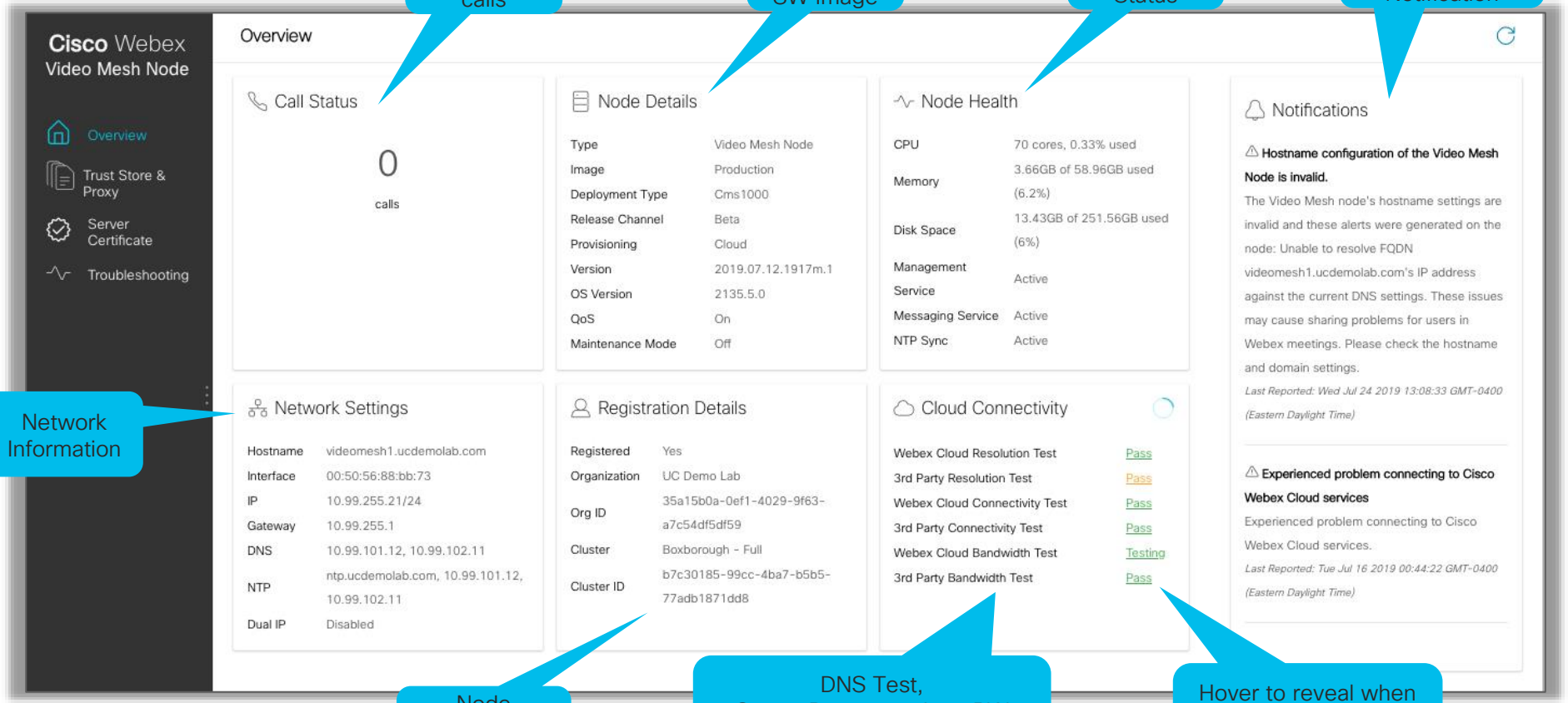
Overview

Number of ongoing calls

Node Type, SW Image

Usage and Service Status

Node specific Alarm Notification



Network Information

Node Registration Status

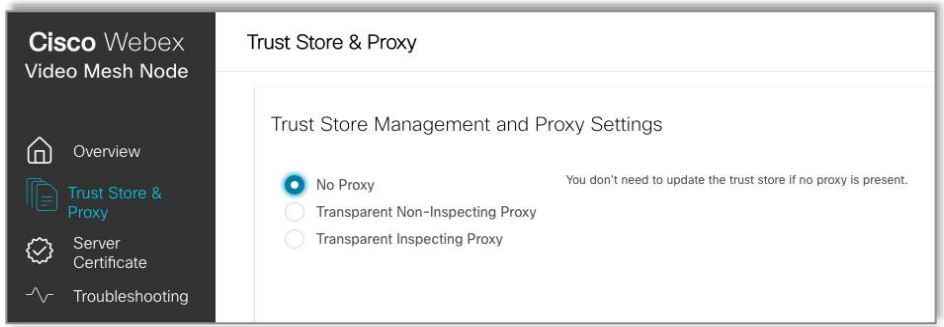
DNS Test, Server Response time, BW test

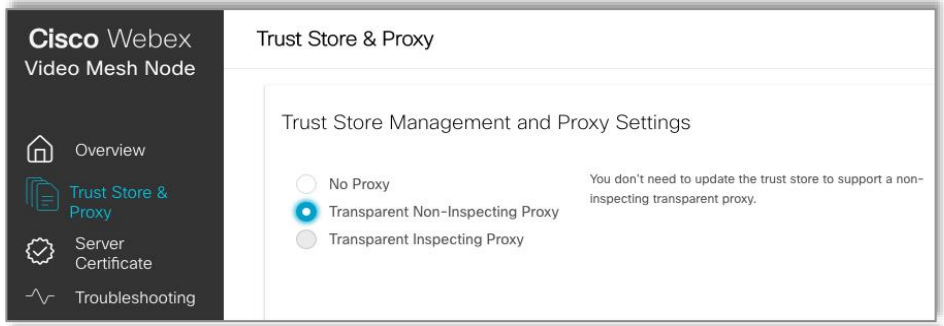
Hover to reveal when the test was run and what was checked

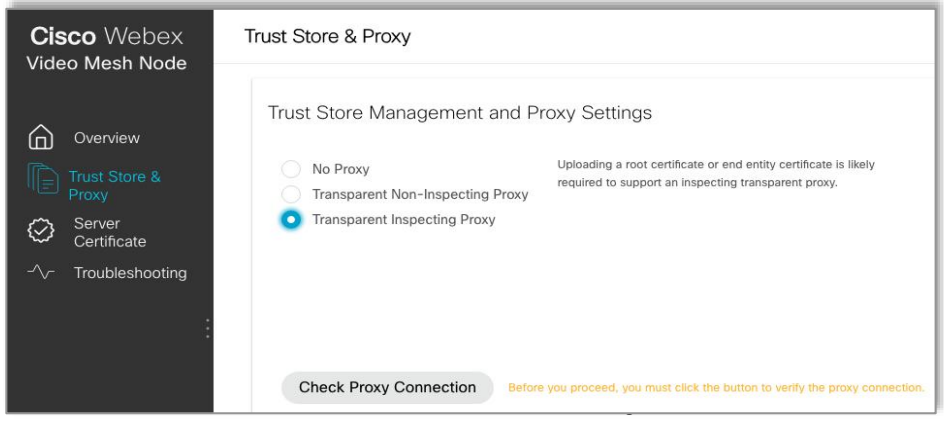
Transparent Proxy

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

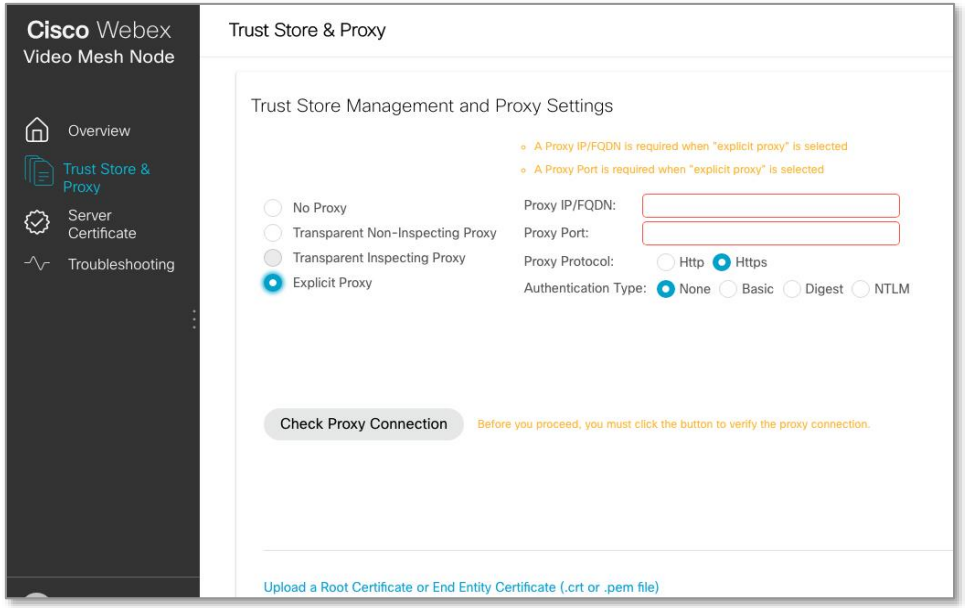






cisco Live!

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

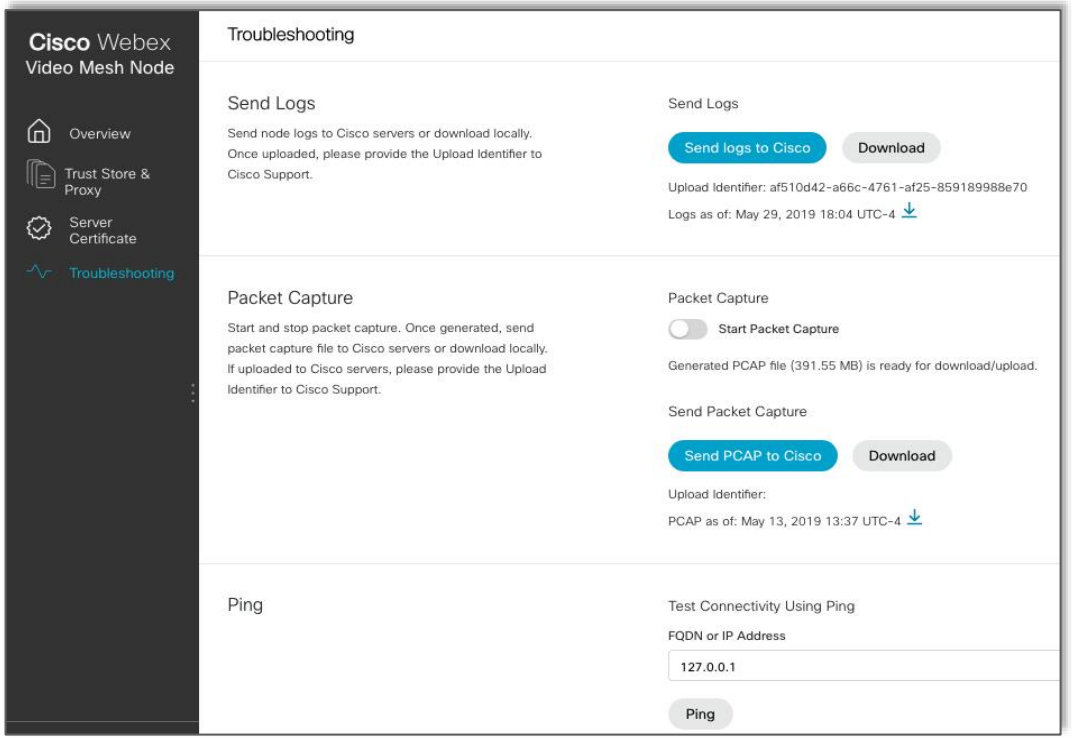
Authentication Type:

- **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

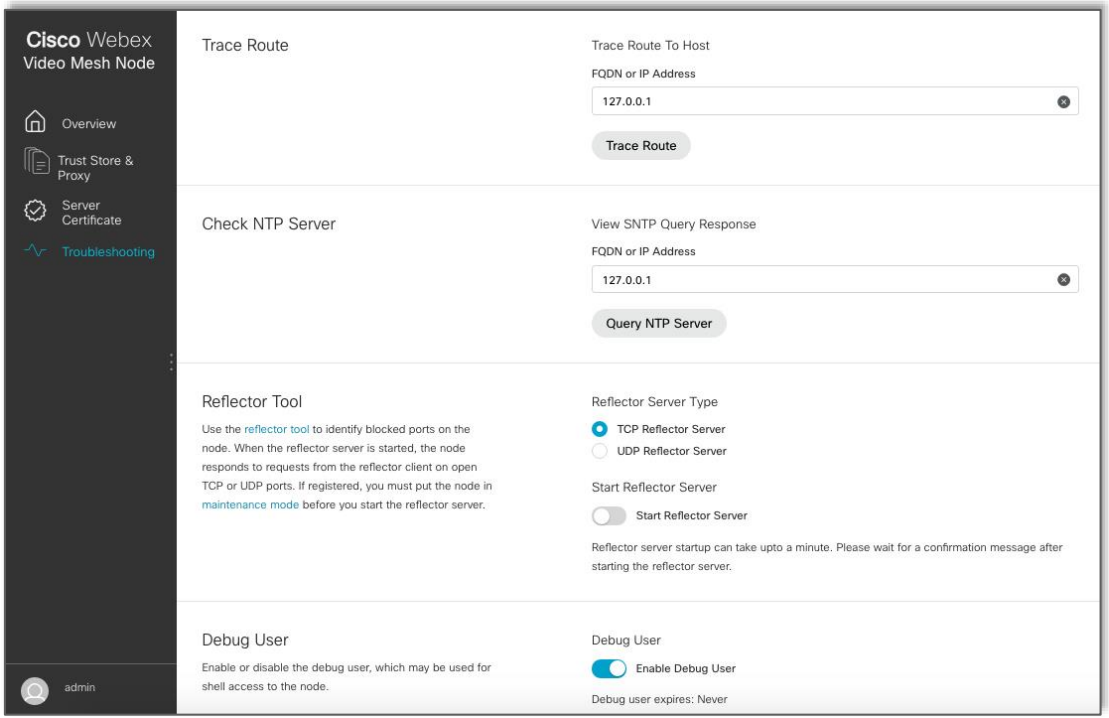
Troubleshooting the Cisco Webex Video Mesh Solution - BRKCOL-3002
Event: 2019 San Diego
Speaker: Paul Stojanovski
https://www.ciscolive.com/global/on-demand-library.html?#/

- 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



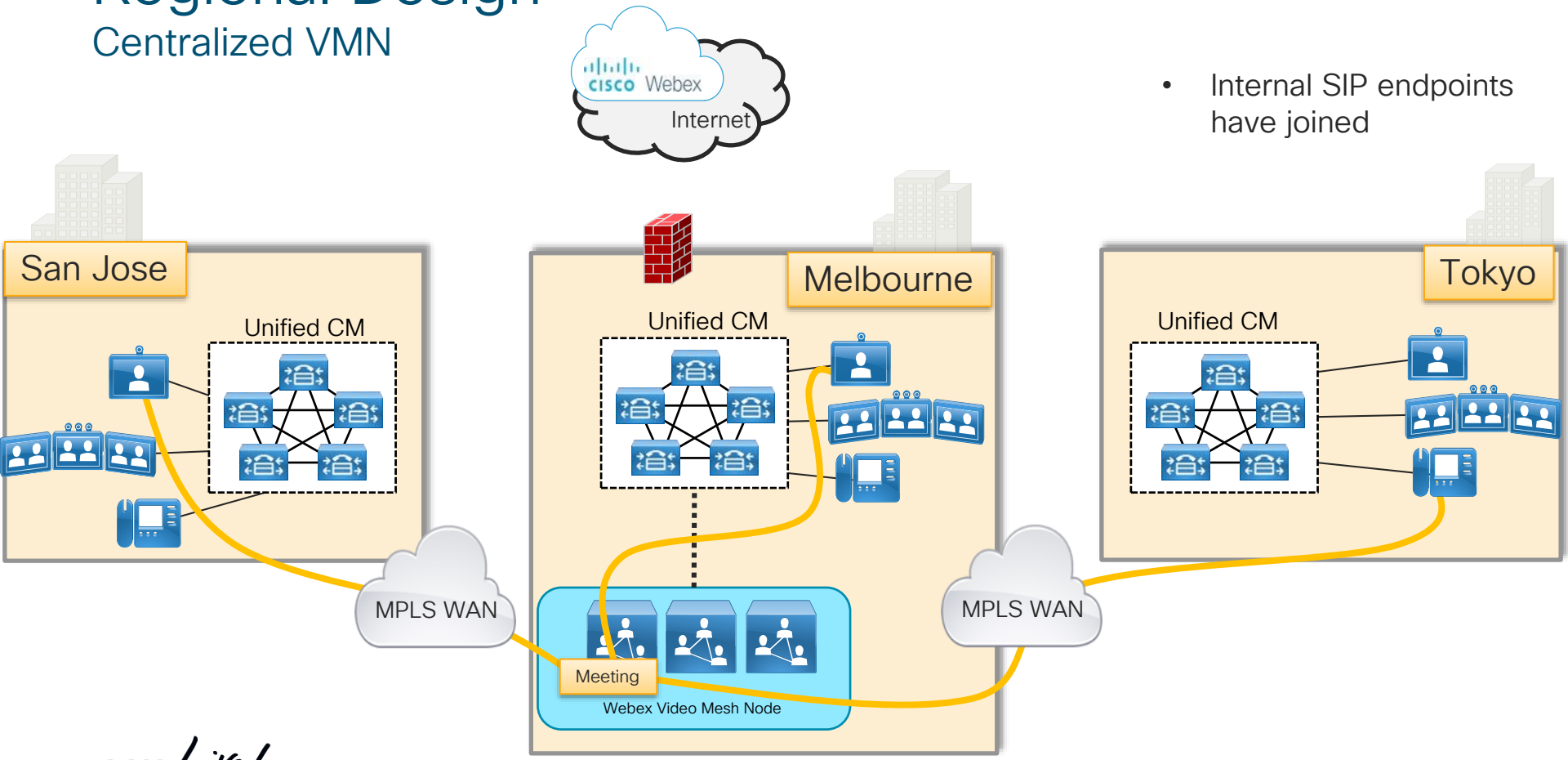
Troubleshooting

- 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



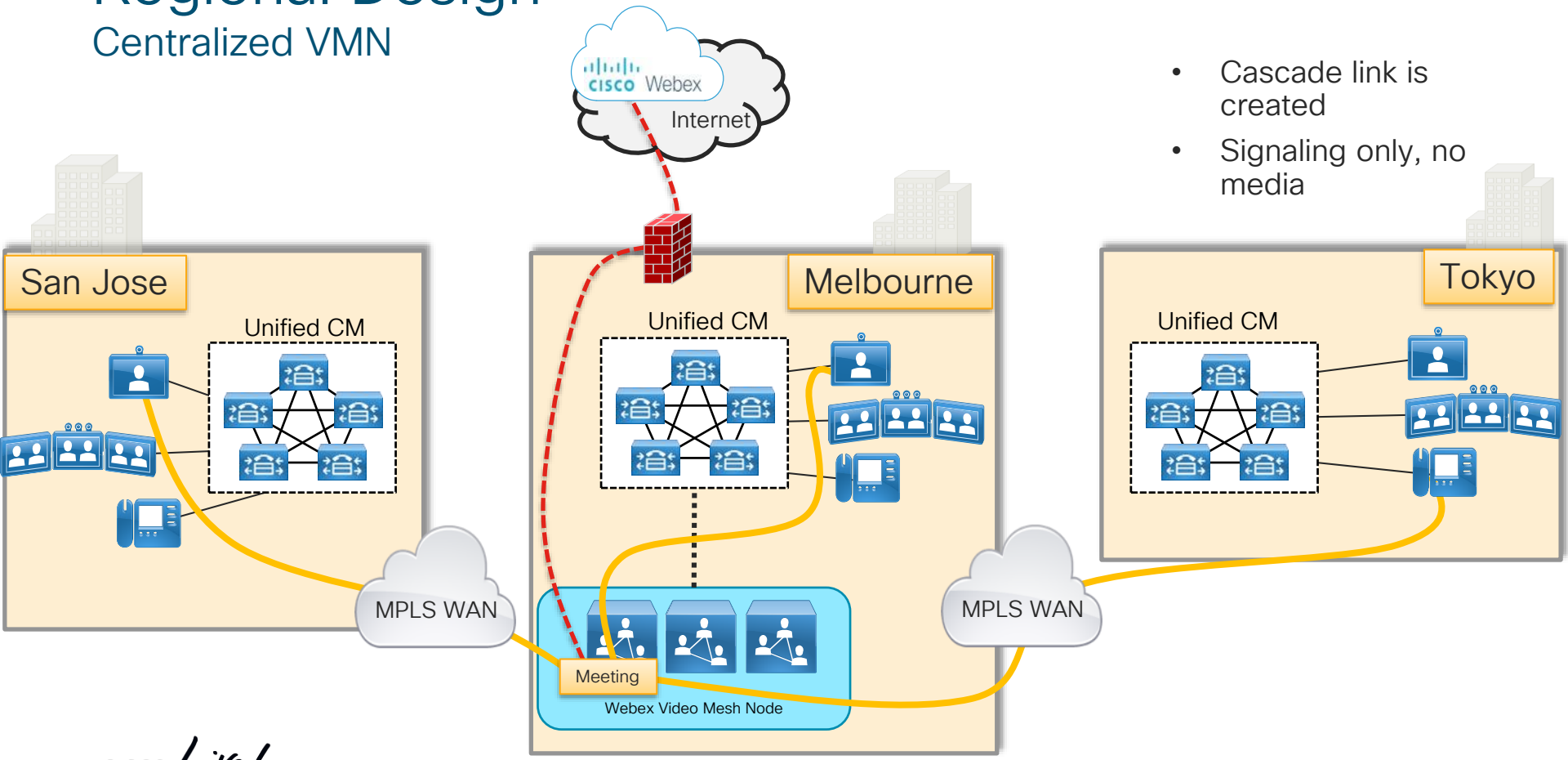
VMN Architecture
Deployments

Regional Design
Centralized VMN



- Internal SIP endpoints have joined

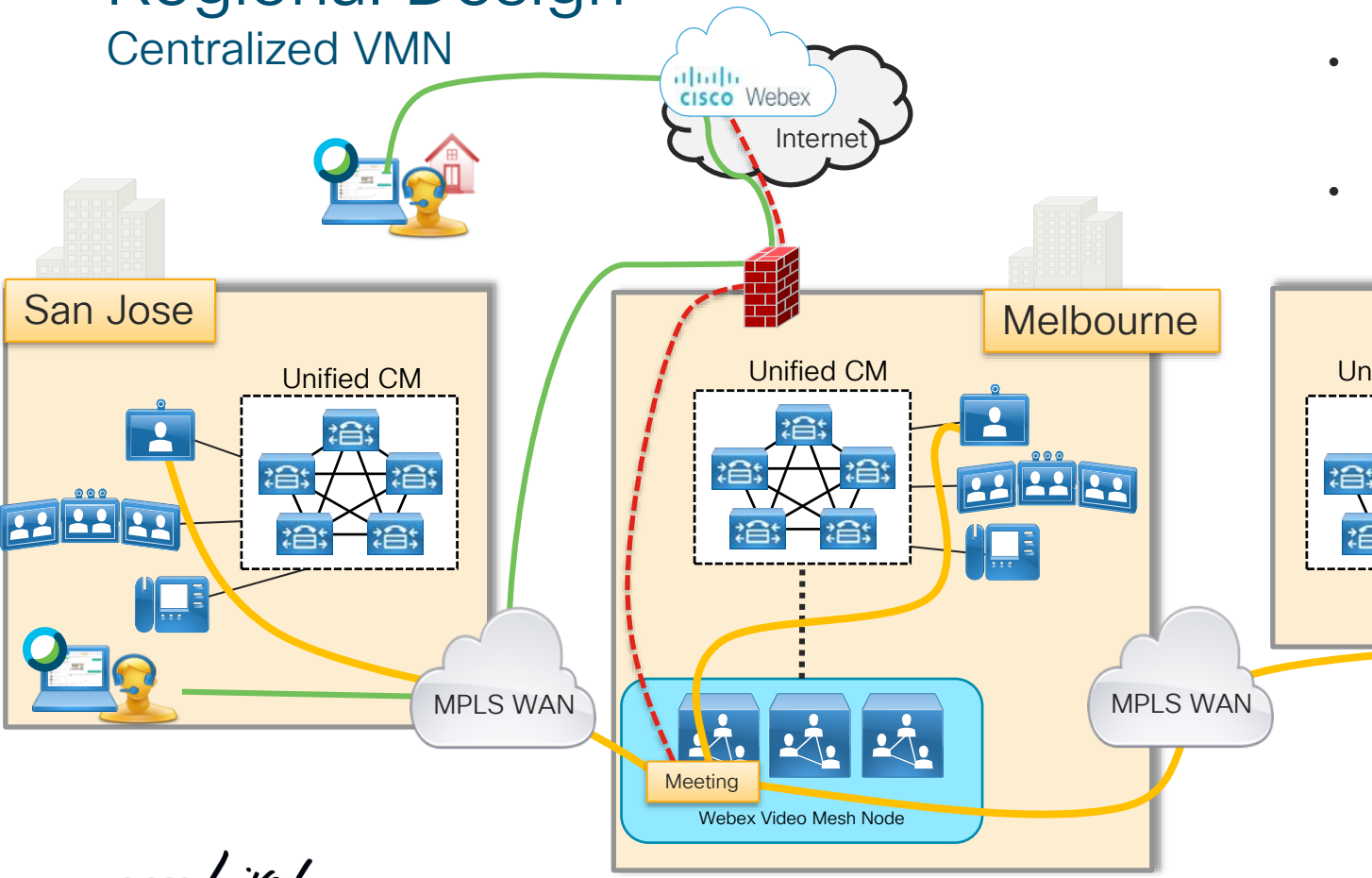
Regional Design
Centralized VMN



- Cascade link is created
- Signaling only, no media

Regional Design

Centralized VMN

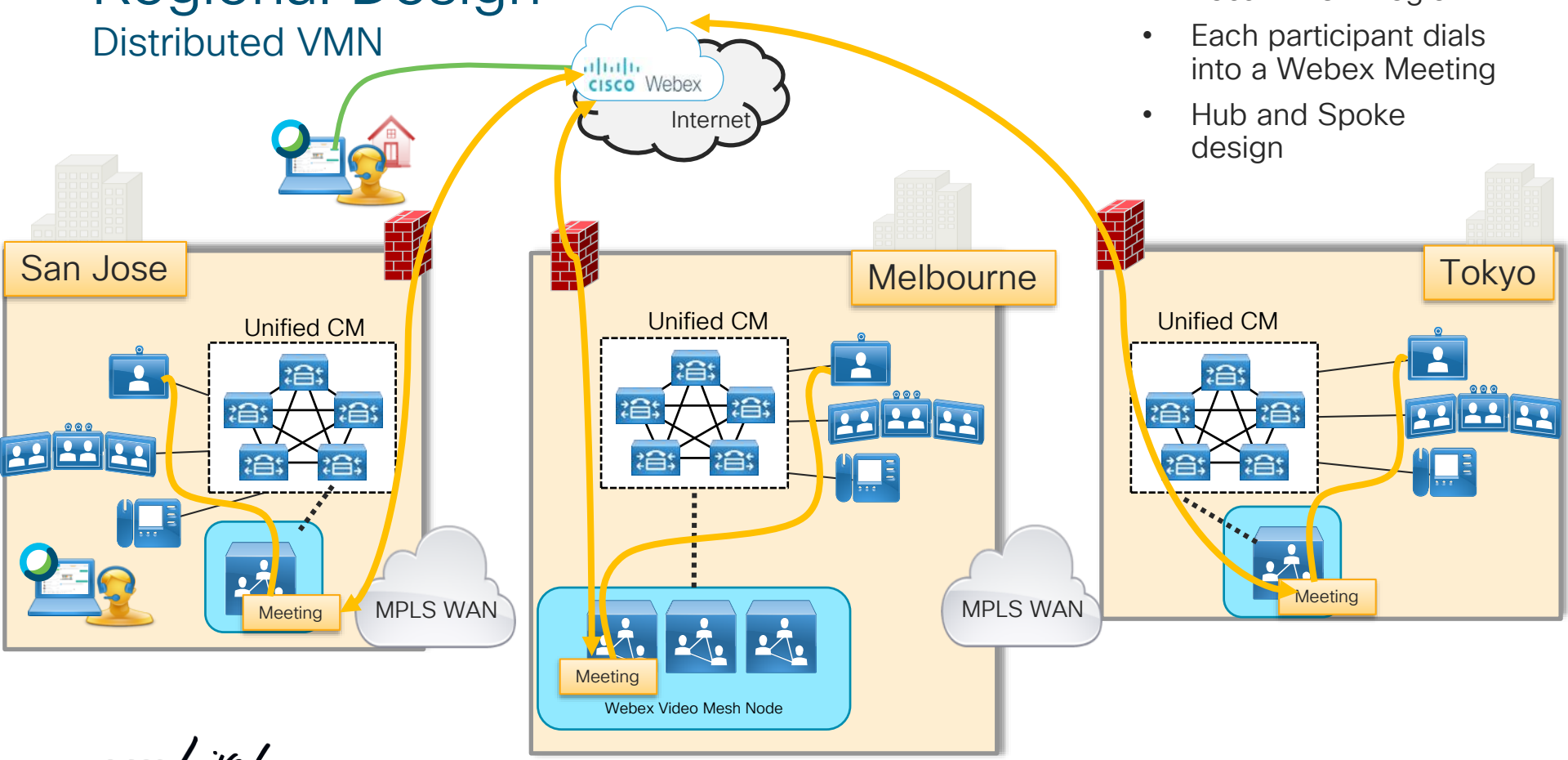


- Webex Meeting App sends media to the cloud.
- They can not use the VMN

Regional Design

Distributed VMN

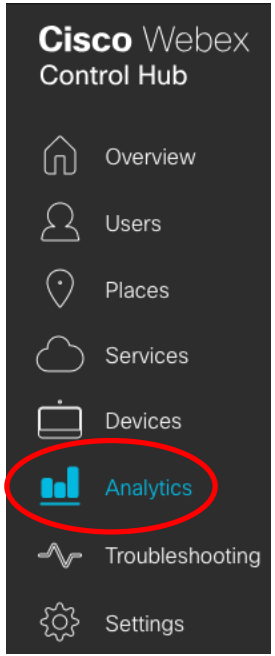
- Local VMs in region
- Each participant dials into a Webex Meeting
- Hub and Spoke design



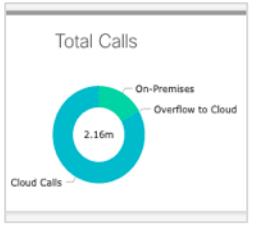
Control Hub Reporting

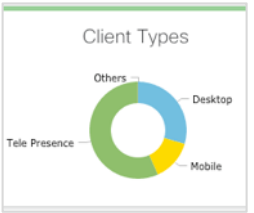
Cisco Webex Control Hub

https://admin.webex.com



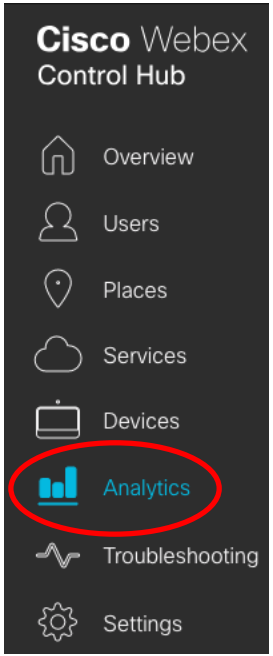
- Webex Video Mesh Reports enables administrator to understand the trend of their on premises resource capacity and utilization, as well as availability that impacts capacity.
- Webex Video Mesh Activity graph gives an overall perspective of the number of calls hosted on the cloud vs the number of calls 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.



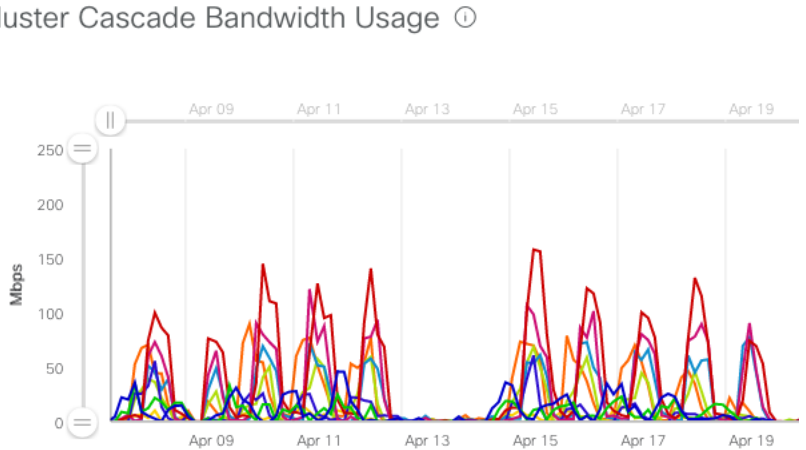


Cisco Webex Control Hub

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



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

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

cisco Live!

You make **possible**