The bridge to possible

CUBE v14 Updates

Hussain Ali, Technical Marketing Engineer
https://www.linkedin.com/in/hussaincube

BRKCOL-2314

Cisco Webex App

Questions?

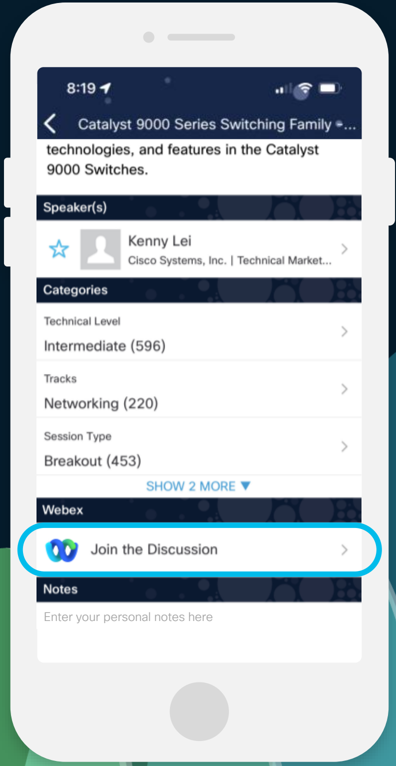
Use Cisco Webex App to chat
with the speaker after the session

How

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

Webex spaces will be moderated
by the speaker until June 7, 2024.

https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKCOL-2314

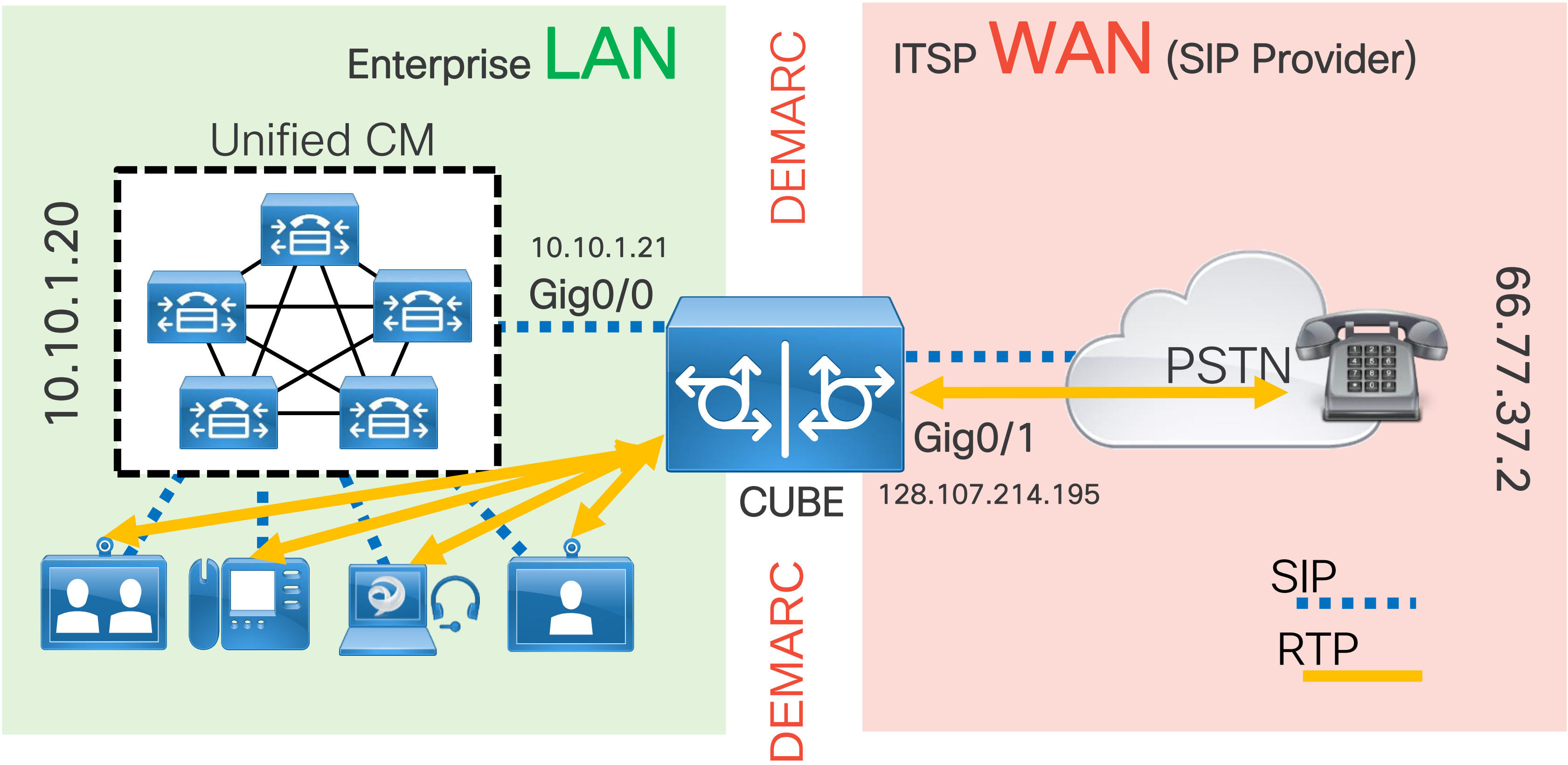


Agenda

- CUBE Recap
- Version 14 Updates
  - vCUBE on AWS / Azure
  - Multiple SIP Listen ports and TLS Profiles
  - NAT traversal using RTP keepalives
  - CUBE High Availability Updates
  - DNS SRV Load Balancing
  - Enabling 3rd party Cloud Calling with CUBE
  - Managing Gateways from the Cloud
- Local Gateway (LGW) for Webex Calling
- Survivability Gateway (SGW) for Webex Calling

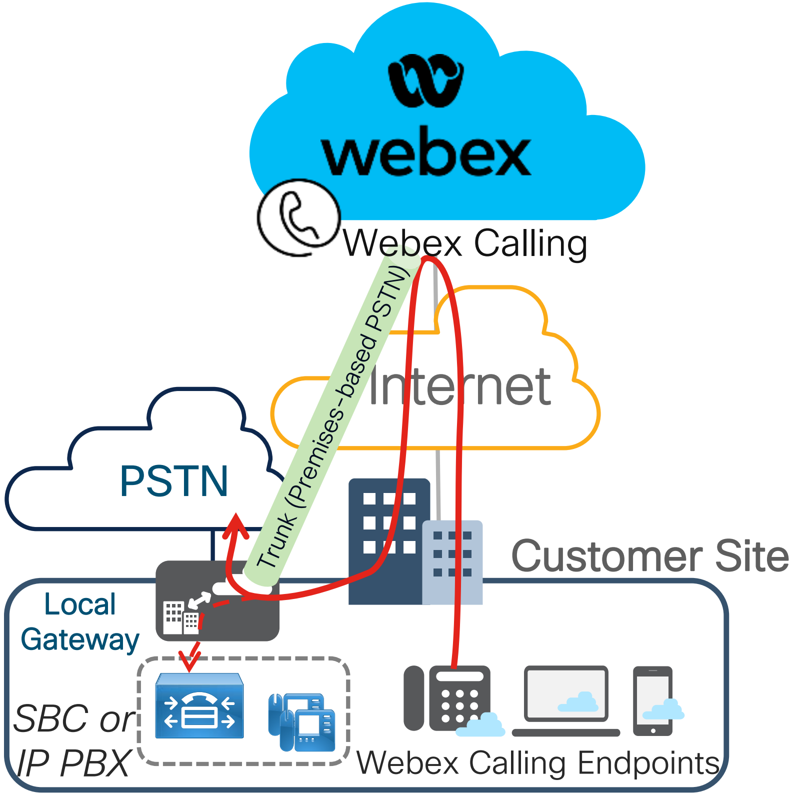
CUBE Recap

CUBE as an SBC for an on-premises Collaboration Deployment



Webex Calling Trunk - Local Gateway

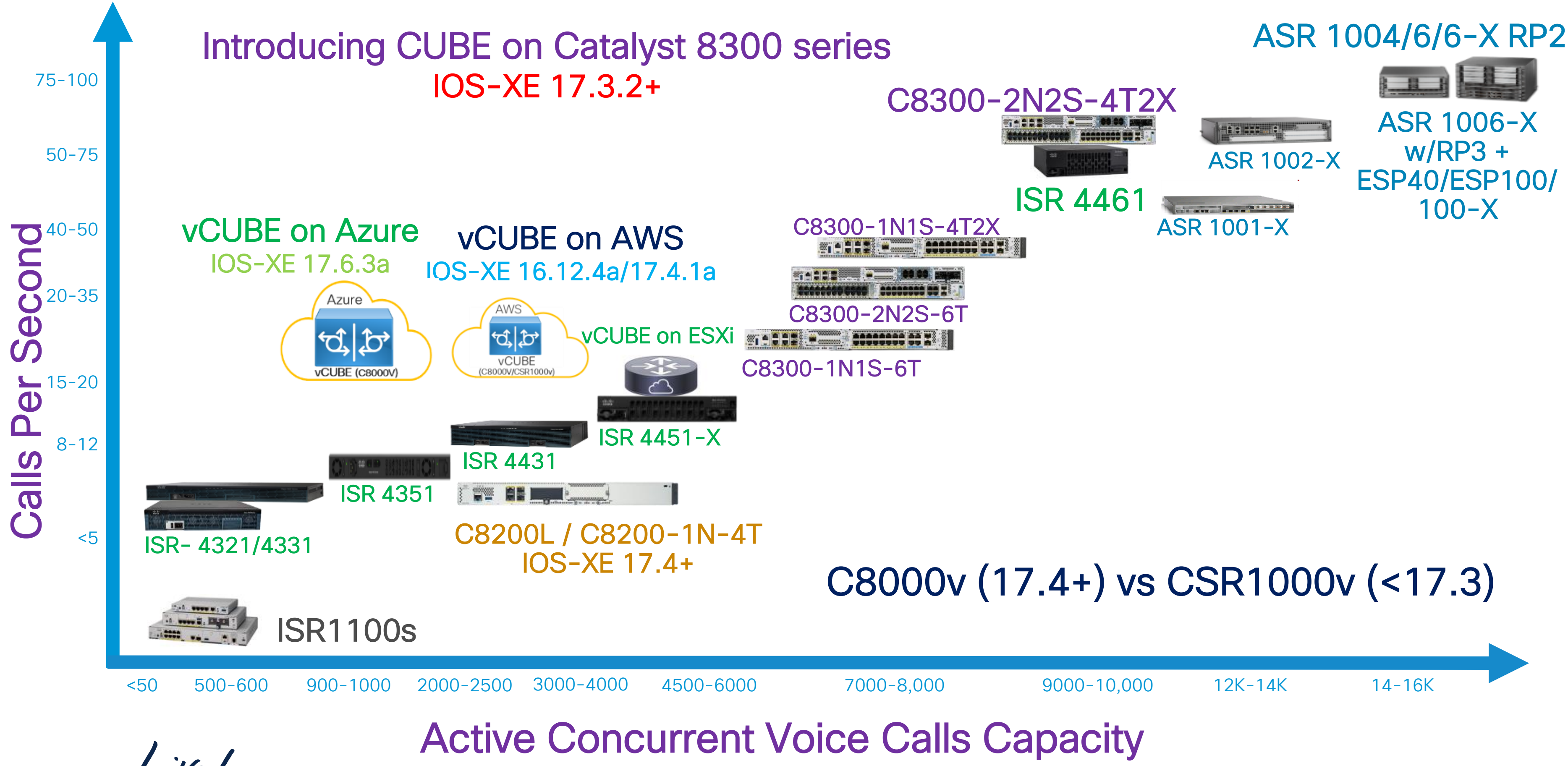
(Premises-based PSTN) Deployment



- Provides connectivity to a customer-owned premises-based PSTN service
- May also provide connectivity to an on-premises IP PBX or dedicated SBC/PSTN GW
- Enables on-prem to Webex Calling transition
- **Endpoint registration is NOT proxied through Local Gateway.** Endpoints directly register to Webex Calling over the Internet.

Platforms for CUBE/vCUBE

CUBE (Enterprise) Product Portfolio [Not to Scale]



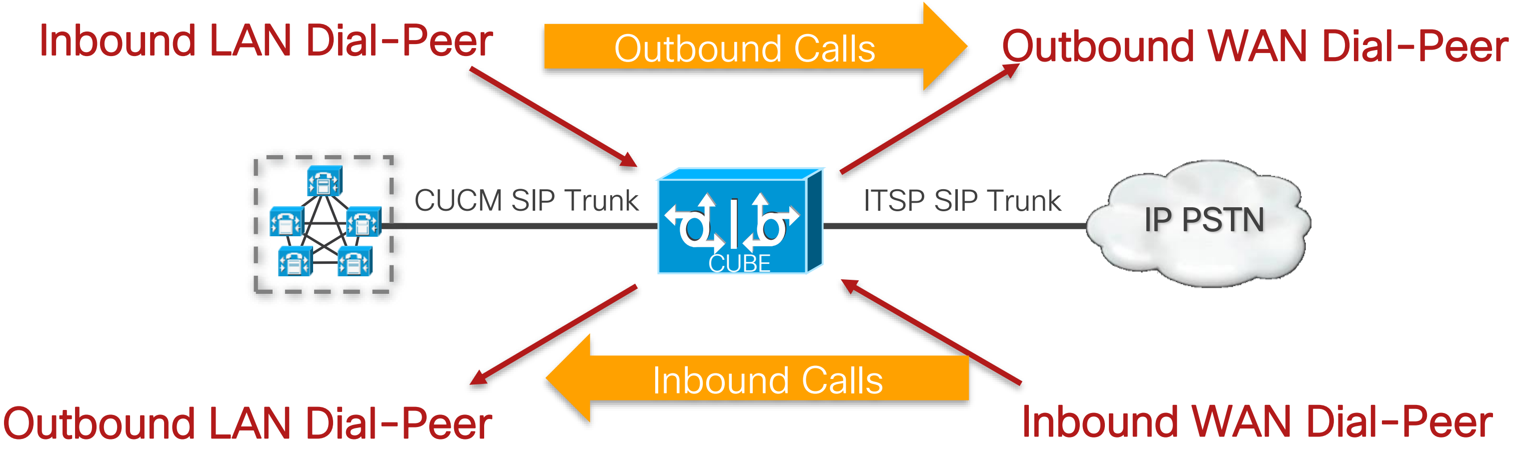
CUBE/IOS-XE Software Release Mapping

CUBE Version	Initial IOS-XE Release for this CUBE version and Release date		Subsequent IOS-XE Release for this CUBE version
14.2	17.4.1a	Nov 2020	17.4.2
14.3	17.5.1	March 2021	17.5.1a
14.4	17.6.1a	July 2021	17.6.6a
14.4	17.7.1a	Nov 2021	17.7.2
14.5	17.8.1a	March 2022	
14.6	17.9.1a	July 2022	17.9.4a
14.6	17.10.1a	Nov 2022	
14.6	17.11.1a	March 2023	
14.7	17.12.1a	July 2023	17.12.2
14.8	17.13.1a	Nov 2023	
14.9	17.14.1a	March 2024	
TBD	17.15.1a	July 2024	

Last release for ISR4K except ISR4461

Understanding Dial-Peer Matching Techniques:
LAN & WAN Dial-Peers

- LAN Dial-Peers – Dial-peers that are facing towards the IP PBX for sending and receiving calls to & from the PBX. Should be bound to the LAN interface(s) of CUBE to ensure SIP/RTP is sourced from the LAN IP(s) of the CUBE.
- WAN Dial-Peers – Dial-peers that are facing towards the SIP Trunk provider for sending & receiving calls to & from the provider. Should be bound to WAN interface(s) of CUBE.



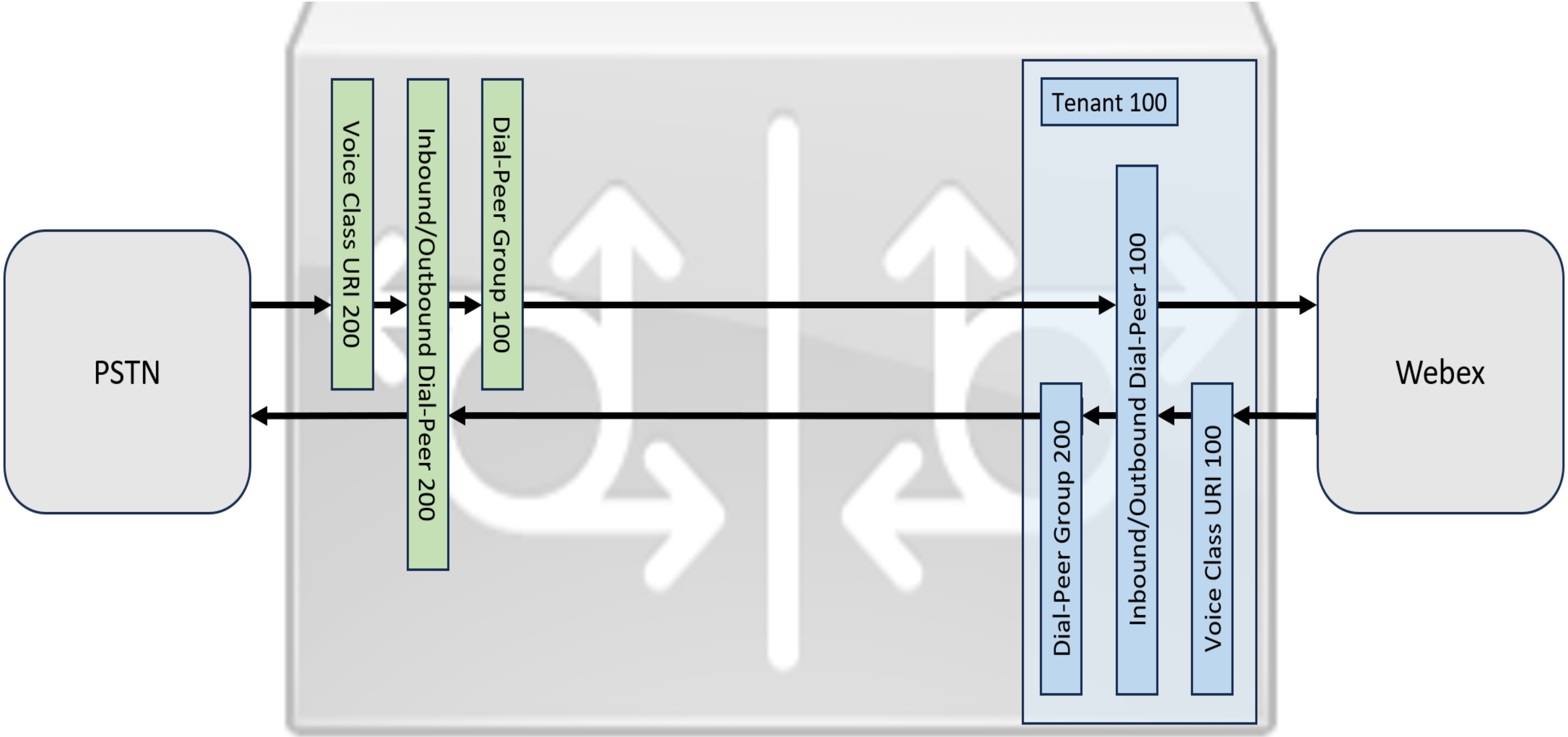
Inbound SIP Dial-Peer Selection Preference

Preference	Match Criteria	Dial-peer Commands
1	URI	incoming uri via <uri-tag>
2		incoming uri request <uri-tag>
3		incoming uri to <uri-tag>
4		incoming uri from <uri-tag>
5	Called Number	incoming called-number <number-string> incoming called e164-pattern-map <pattern-map-number>
6	Calling Number	incoming calling e164-pattern-map <pattern-map-number> answer-address <number-string>
7	Destination-pattern (ANI)	destination-pattern <number-string>
8	Carrier-ID	carrier-id source <string>

Outbound SIP Dial-Peer Matching

Priority	Match Criteria	Dial-peer Commands
1	Dial-Peer Group Dial-Peer	destination dpg <dpg-tag> *(DPG configured on inbound dial-peer)*
2	Dial-Peer Provision Policy URI	destination uri-from <uri-tag> destination uri-to <uri-tag> destination uri-via <uri-tag> destination uri-diversion <uri-tag> destination uri-referred-by <uri-tag> *(DPP configured on inbound dial-peer)*
3	ILS Route String	destination route-string <route-string-tag>
4	URI and Carrier-ID	destination uri <uri-tag> AND carrier-id target <string>
5	Called Number & Carrier-ID	destination-pattern <number-string> AND carrier-id target <string>
6	URI	destination uri <uri-tag>
7	Called Number	destination-pattern <DNIS-number> destination e164-pattern-map <pattern-map-number> dnis-map <dnis-map-number>
8	Calling Number	destination calling e164-pattern-map <pattern-map-number>

Grouping trunks with voice class tenants



Sizing Updates

CUBE IP Telephony (Collab) Session Capacity Summary

Platform [1]CSR1Kv - Based on tests using Cisco UCS ® C240 host with Intel ® Xeon ® 6132 2.60GHz processors running VMware ESXi 6.0.	CUBE SIP-SIP Audio Sessions (Flow-thru) RTP(G711)-RTP(G711)	Sustainable CPS IOS-XE 16.12+
1100 series (Default DRAM)	500	5
4321	500	4
4331	1000	10
4351	2000	13
4431	3000	15
4451	6000	40
4461	10000 (IOS-XE 17.2.1r+)	55
C8200L-1N-4T (4 GB)	1500 (IOS-XE 17.5.1+)	9
C8200-1N-4T (8 GB)	2500 (IOS-XE 17.4.1a+)	14
C8300-1N1S-6T (8 GB)	7000 (17.3.2)	40
C8300-2N2S-6T (8 GB)	7500 (17.3.2)	42
C8300-1N1S-4T2X (8 GB)	8000 (17.3.2)	45
C8300-2N2S-4T2X (16 GB)	10000 (17.3.2)	55
C8000V-S/CSR1Kv – 1 vCPU[1] (4 GB)	1000	5
C8000V-M/CSR1Kv – 2 vCPU[1] (4 GB)*	3000	20
C8000V-L/CSR1Kv – 4 vCPU[1] (8 GB)	6000	30

* vCUBE in AWS/Azure session counts same as CSR1Kv – 2 vCPU

CUBE IP Telephony (Collab) Session Capacity Summary

Platform	Session Count IOS-XE 16.12+ RTP(G711)-RTP(G711)	Sustainable CPS IOS-XE 16.12+
ASR1001-X	12000	50
ASR1002-X	14000	55
ASR1006-X RP3 ESP40/ESP100	16000	65
ASR1004/6/6-X RP2/ESP40	16000	70

CUBE Encrypted IPT Audio Call Capacity

Platform	Audio IP Telephony calls RTP(G711)-RTP(G711)	Encrypted Audio (SHA1_80) calls sRTP(G711)-RTP(G711)	CPS
1100 series (Default DRAM)	500	300	2
4321 (4 GB)	500	300	1
4331 (4 GB)	1000	600	3
4351 (4 GB)	2000	750	4
4431 (8 GB)	3000	750	4
4451 (8 GB)	6000	2100 (16.12.2)	11
4461 (8 GB)	10000 (17.2.1r)	9900 (17.6.4)	30
C8200L-1N-4T (4 GB)	1500 (17.5.1)	400 (17.5.1)	3
C8200-1N-4T (8 GB)	2500 (17.4.1)	650 (17.4.1)	4
C8300-1N1S-6T (8 GB)	7000 (17.3.2)	1600 (17.3.2)	9
C8300-2N2S-6T (8 GB)	7500 (17.3.2)	1800 (17.3.2)	10
C8300-1N1S-4T2X (8 GB)	8000 (17.3.2)	3500 (17.12+)	15
C8300-2N2S-4T2X (16 GB)	10000 (17.3.2)	4300 (17.3.2)	24
C8000V-S/CSR1Kv - 1 vCPU[1] (4 GB)	1000	300	1
C8000V-M/CSR1Kv - 2 vCPU[1] (4 GB)	3000	1000	6
C8000V-L/CSR1Kv - 4 vCPU[1] (8 GB)	6000	1080	6

CUBE Session Capacity for UCCE (IOS-XE 16.12+)

Platform	Session Capacity RTP(G711)-RTP(G711)	UCCE Call Capacity	Impact of UCCE to IPT (Collab)	UCCE CPS
4321 (4 GB)	500	500	0%	3
4331 (4 GB)	1000	1000	0%	7
4351 (4 GB)	2000	1500	25%	8
4431 (8 GB)	3000	1800	40%	10
4451 (8 GB)	6000	3600	40%	20
4461 (8 GB)	10000 (17.2.1r)	4680 (17.2.1r)	53%	26
C8200L-1N-4T (4 GB)*	1500 (IOS-XE 17.5.1+)	1000	33%	6
C8200-1N-4T (8 GB)*	2500 (IOS-XE 17.4.1a+)	1400	44%	8
C8300-1N1S-6T (8 GB)*	7000 (17.3.2)	3200 (17.3.2)	54%	18
C8300-2N2S-6T (8 GB)*	7500 (17.3.2)	3700 (17.3.2)	51%	21
C8300-1N1S-4T2X (8 GB)*	8000 (17.3.2)	3800 (17.3.2)	52.5%	21
C8300-2N2S-4T2X (16 GB)*	10000 (17.3.2)	4100 (17.3.2)	59%	23

CUBE Encrypted IPT Audio Call Capacity

Platform [1]CSR1Kv - Based on tests using Cisco UCS ® C240 host with Intel ® Xeon ® 6132 2.60GHz processors running VMware ESXi 6.0.	Audio IP Telephony calls RTP(G711)-RTP(G711)	Encrypted Audio (SHA1_80) calls sRTP(G711)-RTP(G711)	CPS
1100 series (Default DRAM)	500	300	2
4321 (4 GB)	500	300	1
4331 (4 GB)	1000	600	3
4351 (4 GB)	2000	750	4
4431 (8 GB)	3000	750	4
4451 (8 GB)	6000	2100 (16.12.2)	11
4461 (8 GB)	10000 (17.2.1r)	9900 (17.6.4)	30
C8200L-1N-4T (4 GB)	1500 (17.5.1)	400 (17.5.1)	3
C8200-1N-4T (8 GB)	2500 (17.4.1)	650 (17.4.1)	4
C8300-1N1S-6T (8 GB)	7000 (17.3.2)	1600 (17.3.2)	9
C8300-2N2S-6T (8 GB)	7500 (17.3.2)	1800 (17.3.2)	10
C8300-1N1S-4T2X (8 GB)	8000 (17.3.2)	3500 (17.12+)	15
C8300-2N2S-4T2X (16 GB)	10000 (17.3.2)	4300 (17.3.2)	24
C8000V-S/CSR1Kv – 1 vCPU[1] (4 GB)	1000	300	1
C8000V-M/CSR1Kv – 2 vCPU[1] (4 GB)	3000	1000	6
C8000V-L/CSR1Kv – 4 vCPU[1] (8 GB)	6000	1080	6

Version 14 Updates

vCUBE on AWS / Azure

vCUBE on Amazon Web Services (AWS) / Microsoft Azure

- [AWS] Platform validated and currently supported – c5.large [2vCPU, 4GB RAM, 8GB SSD] and c5n.large [2vCPU, 5.3 GB]
  - IOS-XE versions validated – CSR1000v (16.12.4a, 17.3.2), C8000V (17.4.1a) [Subsequent releases also supported]
- [Azure] Platform validated and currently tested –D2_v2 [2 vCPUs, 7 GB memory]
  - IOS-XE versions validated – 17.3.4a [Subsequent releases also supported]
- BYOL – Instance billed only for hosting by AWS/Azure and licensing managed through Cisco Smart Licensing [DNA Network Essentials or above for C8000V]
- vCUBE in AWS/Azure session counts same as vCUBE - 2 vCPU

AWS and Azure deployment considerations

- vCUBE specific image **MUST** be used. Do not use the generic CSR1000V/Cat8kV images
- [AWS] Currently only c5.large and c5n.large instances supported
- All existing vCUBE limitations are applicable
  - No DSP based features (transcoding/inband-RFC2833 DTMF/ASP/NR)
- VOIP Signaling and Media IP and Ports advertised by the peer entities must be reachable from vCUBE in Azure
- Although CLI commands for unsupported features may be visible on the Cisco CSR 1000v, testing by Cisco has determined that these unsupported features do not work in Azure deployments.
- All Cat8Kv/CSR1000v restrictions apply to vCUBE-Azure/vCUBE-AWS as well

https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/aws/b_csraws/overview_of_cisco_csr_1000v_deployment_on_amazon_web_services.html

Introducing multiple SIP listen ports

SIP Listening Port on CUBE before IOS-XE 17.8.1a

- Default SIP Listen ports are 5060 (UDP/TCP) and 5061 (TLS)

```
voice service voip
   sip
      listen-port non-secure 2000 secure 2050
```

Introducing voice class TLS-profile

IOS-XE 17.3.1

Prior to IOS-XE 17.3.1

```
CUBE(config-sip-ua)#crypto signalling remote-addr 10.65.105.24
255.255.255.255 trustpoint trustpoint-name
```

Starting IOS-XE 17.3.1

```
CUBE(config-sip-ua)#crypto signalling remote-addr
10.65.105.24 255.255.255.255 ?
  tls-profile  Associate a tls-profile
  trustpoint   Associate a trustpoint
```

```
voice class tls-profile 2
 trustpoint CUCM
 cn-san validate server
 cipher ecdsa-cipher
 sni send
```

Multi Tenant – SIP listen ports

- From IOS-XE 17.8.1a, inbound listen ports can be configured under each tenant. Previously it was only a global configuration
- Multiple inbound TLS (secured) and TCP/UDP (non-secured) connection can be established on different listen ports.
- Each secure listen ports can be configured with their own TLS-Profile and their own validation criteria
- Listen port based multi tenancy is supported on both IPv4 and IPv6 across all TLS/TCP/UDP transport protocols

SIP listen ports

Considerations

- It is mandatory to configure bind at the tenant level to support multi tenancy based on listen ports. Without interface bind at the tenant level, listen port will not be opened.
- Listen port and bind interface must be unique across:
    - Global and tenant level
    - Secure and non-secure
  - i.e., we cannot configure the same TLS/TCP/UDP listen port across multiple tenants or globally. CUBE will report an error as "Port number already in use"
- Tenant level listen port configuration cannot be modified while there are active calls using the dial-peer to which the tenant is associated.

Multi Tenant – SIP listen ports - Configuration

- Configure voice class tls-profile

```
CUBE(config)#voice class tls-profile <tag>
CUBE(config-class)#cn-san validate ?
  bidirectional   Enable CN/SAN validation for both client and server certificate
  client          Enable CN/SAN validation for client certificate
  server          Enable CN/SAN validation for server certificate
```

- Configure voice class tenant, listen port and associate TLS profile to the tenant

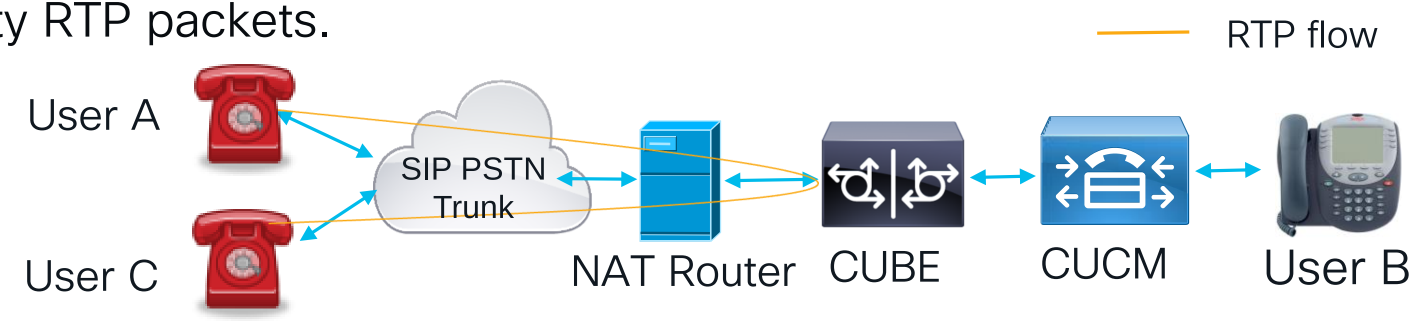
```
CUBE(config)#voice class tenant <tag>
CUBE(config-class)#listen-port ?
    non-secure  Change UDP/TCP SIP listen port (have bind configured under
                this tenant for the config to take effect)
    secure      Change TLS SIP listen port (have bind configured under this
                tenant for the config to take effect

CUBE(config-class)#tls-profile <tag>
    <1-10000>  Specify the tls-profile tag number
```


NAT Traversal using RTP keepalives

NAT Traversal

IOS-XE 17.13.1a / 17.12.2

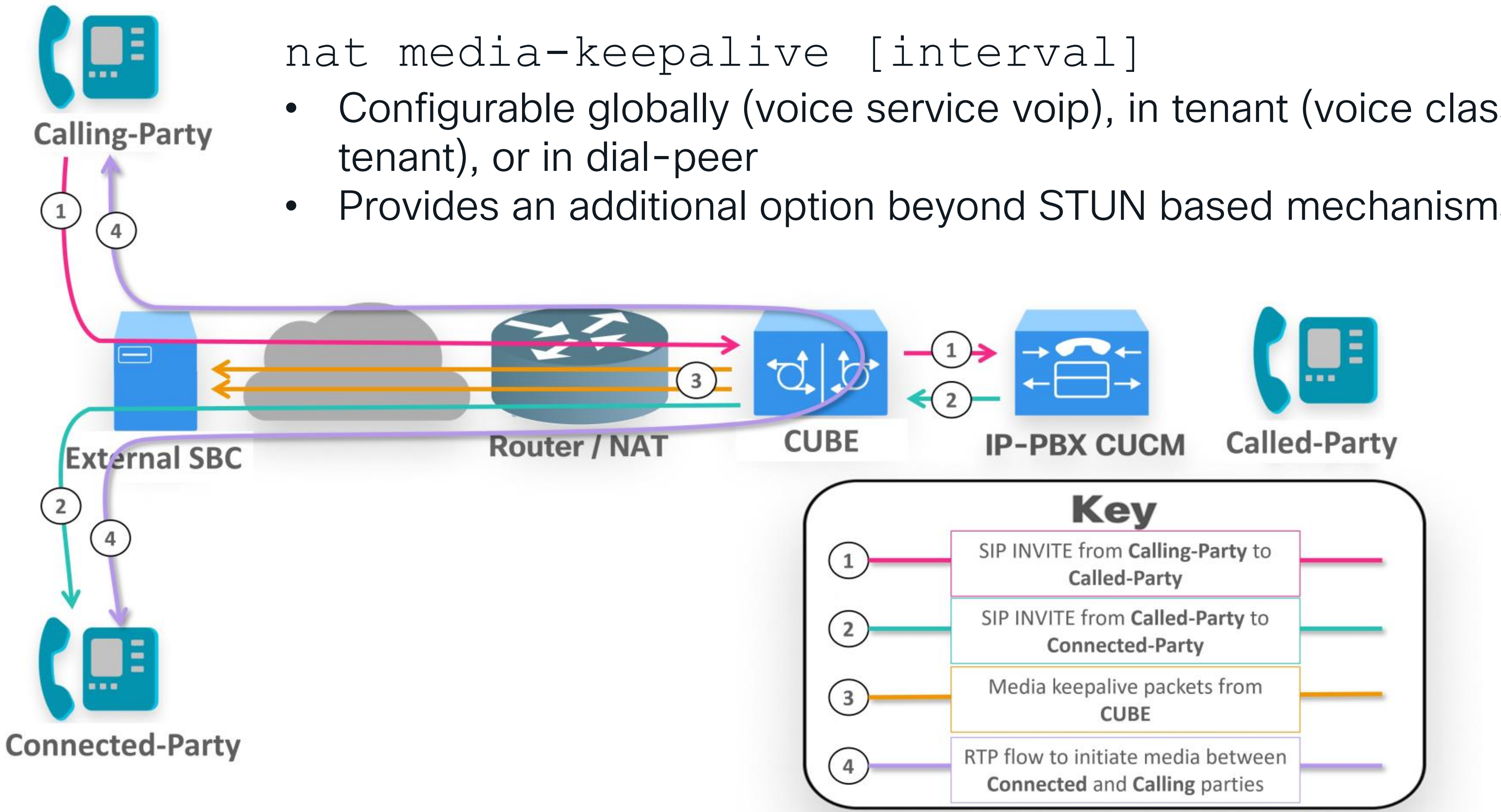
- When a PSTN user A calls an enterprise user B who has setup call forward to an external PSTN user C, the call between A and C will get established, but audio will not flow through.
- A configurable option is provided in CUBE to periodically send the payload-free RTP keepalive packets to keep the pinholes open for media to flow through.
- NAT translates empty RTP packets and opens necessary pin holes for both calling and called party. IMS performs media latching with the incoming empty RTP packets.



Introducing NAT Traversal using RTP keepalives

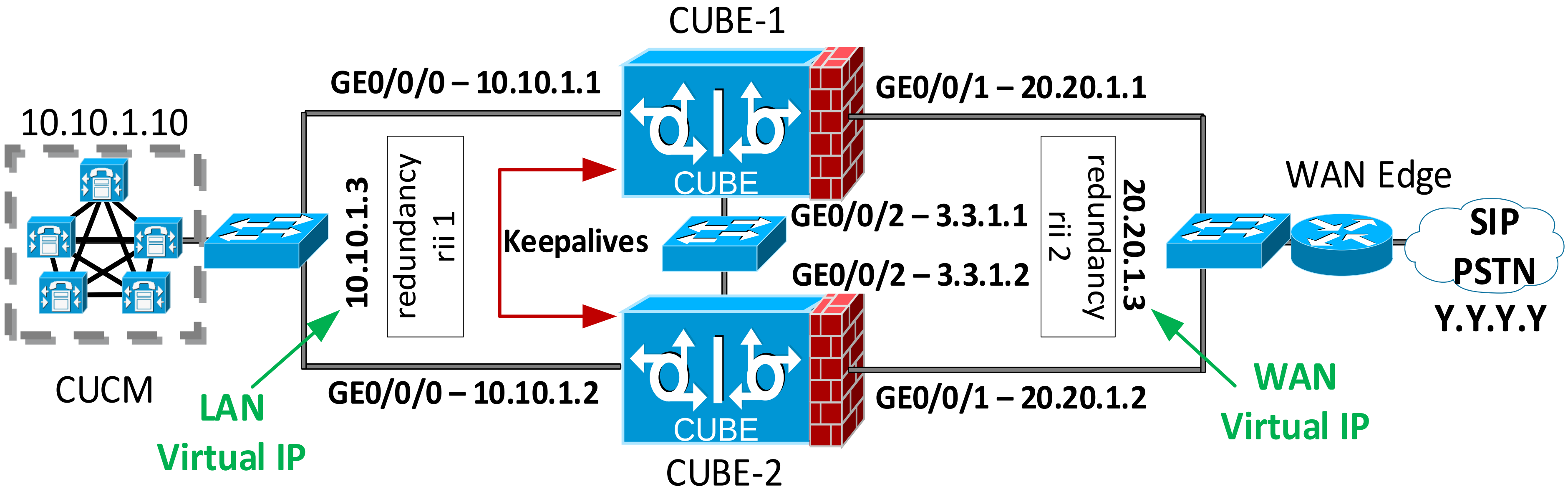
```
nat media-keepalive [interval]
```

- Configurable globally (voice service voip), in tenant (voice class tenant), or in dial-peer
- Provides an additional option beyond STUN based mechanisms



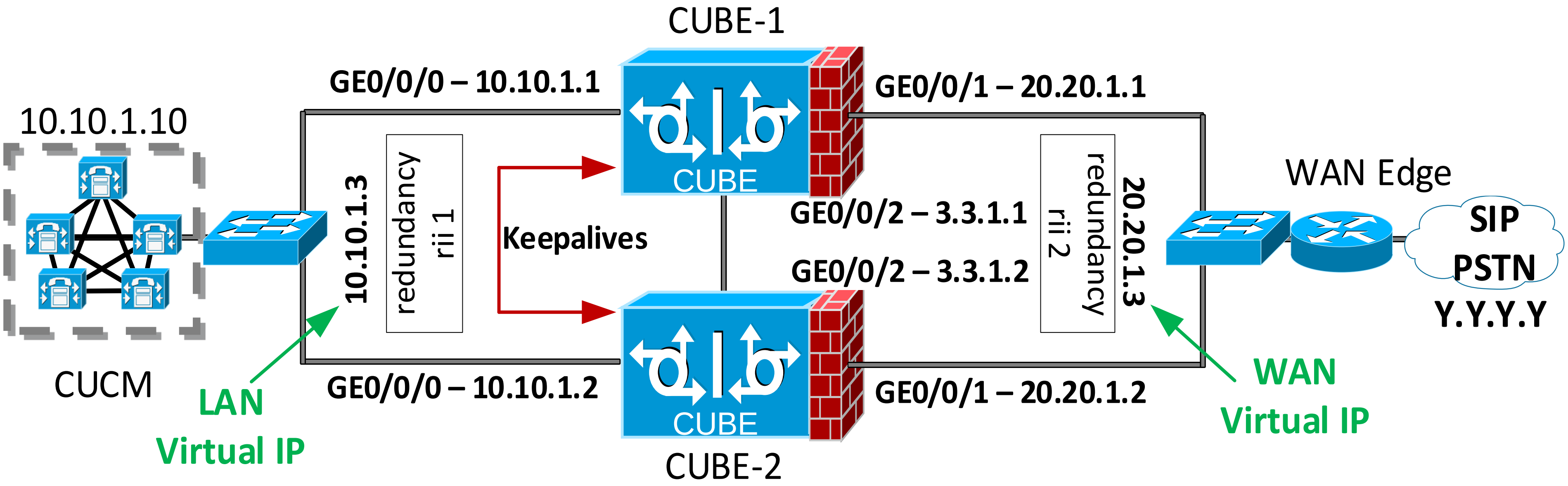
CUBE High Availability (HA) Updates

CUBE HA for Call Preservation



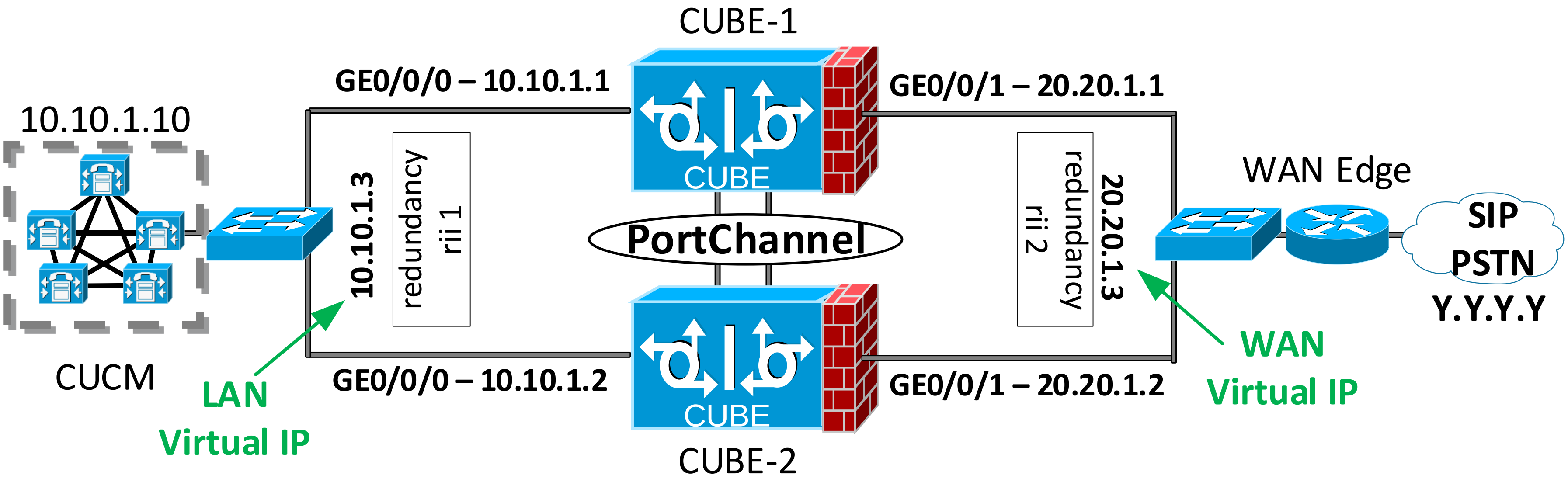
- RG Control/Data interface (G0/0/2) had to be connected via a physical switch
- It can now be connected via a back-to-back cable

Crossover cable for Keepalive interface



- RG Control/Data interface (G0/0/2) had to be connected via a physical switch
- It can now be connected via a back-to-back cable

Port channel for keepalive interfaces



- RG Control/Data interface (G0/0/2) had to be connected via a physical switch
- It can now be connected via a back-to-back cable

CUBE HA is now supported with IPv6

IOS-XE 17.12.1a

- Interface configuration with IPv6

```
CUBE(config)#interface GigabitEthernet0/0/1
CUBE(config-if)# ipv6 address 2001:10:51:100::1/119
CUBE(config-if)# ipv6 enable
CUBE(config-if)# redundancy rii 1
CUBE(config-if)# redundancy group 1 ipv6 2001:10:1:20::153/64 exclusive
```

- Dial-peer configuration with IPv6

```
CUBE(config)#dial-peer voice 106 voip
CUBE(config-dial-peer)#session target ipv6:[2001:10:1:40:250:56ff:fe89:cd27]
CUBE(config-dial-peer)#voice-class sip bind control source-interface
GigabitEthernet0/0/0 ipv6-address 2001:10:1:20::153
CUBE(config-dial-peer)#voice-class sip bind media source-interface
GigabitEthernet0/0/0 ipv6-address 2001:10:1:20::153
```

- SIP-UA configuration with IPv6

```
CUBE(config)# sip-ua
CUBE(sip-ua)# protocol mode ipv6
```

DNS SRV based load balancing on Dial-peers

Introducing DNS SRV based OPTIONS ping

OPTIONS ping for DNS SRV hosts

IOS-XE 17.9.1a

- Pre IOS-XE 17.9
  - CUBE uses the first resource obtained against an SRV lookup to send the option keepalive message. In case the response fails with the first host, CUBE does not try other hosts.
- IOS-XE 17.9.1a or later
  - CUBE attempts OPTION keepalives with the all the hosts to determine their status and use it for routing the calls.
  - This feature can be used by configuring a dial-peer target with an FQDN that resolves to a set of DNS SRV records.
  - A DNS SRV lookup results in multiple targets (A records), each with its own weight, priority.
  - CUBE performs DNS lookup against each record (obtained through SRV lookup) to determine the IPv4/IPv6 addresses and triggers OOD SIP Option message to each destination to monitor the status.

Pre-requisites

- FQDN must be used as `session target` in dial-peers
  - Example: `session target dns:webex.com`
- DNS server with SRV records
- Configuring `voice-class sip options-keepalive profile <tag>` under dial-peer is must

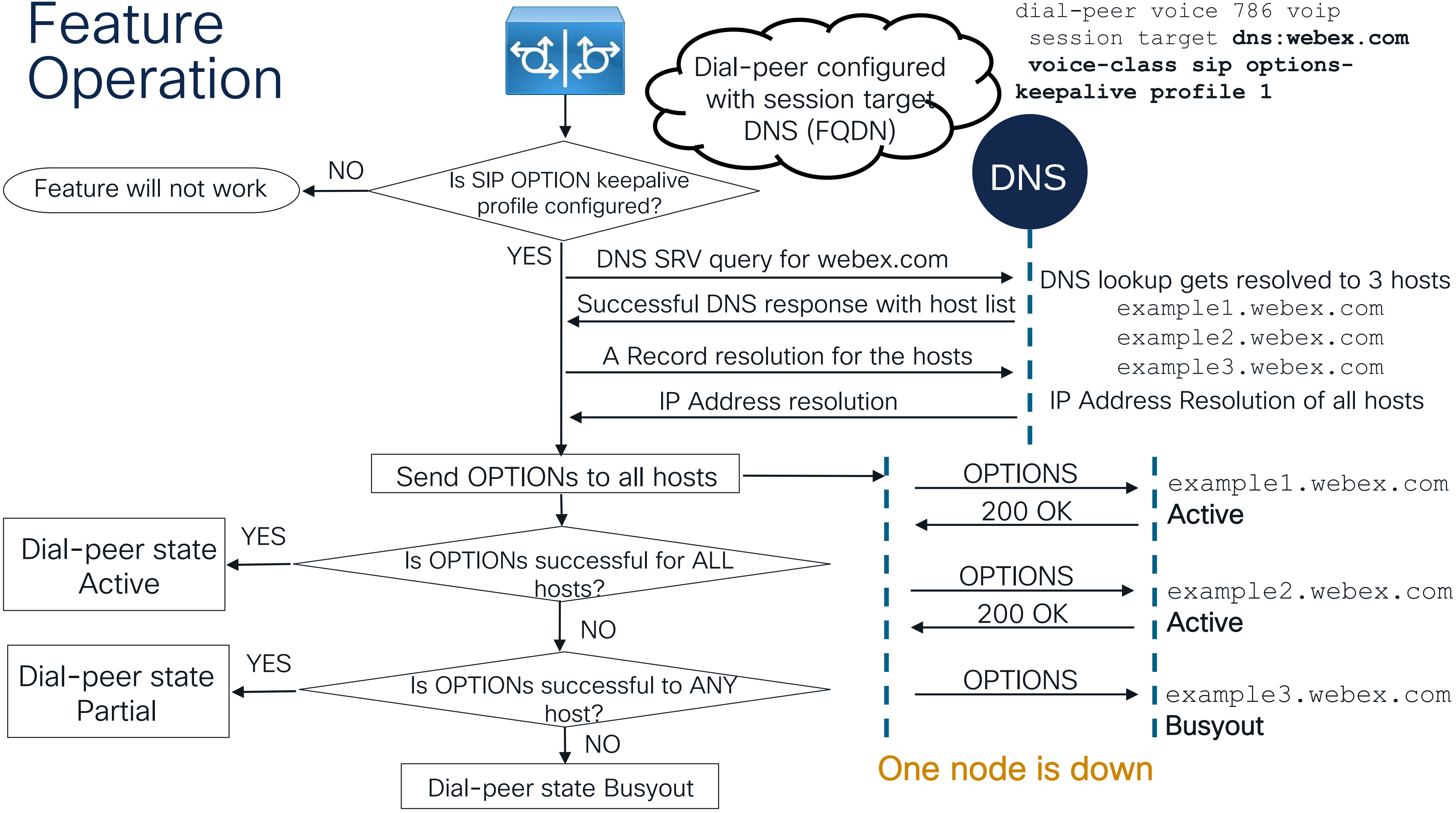
```
CUBE(config)# voice class sip-options-keepalive 1
CUBE(config-class)#description keepalive-webex
CUBE(config-class)#transport tcp
CUBE(config-class)#down-interval 15
CUBE(config-class)#up-interval 5
CUBE(config-class)#retry 1

dial-peer voice 786 voip
 session target dns:webex.com
 session transport tcp
 voice-class sip options-keepalive profile 1
```

DNS SRV Based Option Ping : Status of Hosts

- Each SRV node associated with the DNS target is monitored. It provides the option of marking a dial-peer and host’s status as below:
  - **Active** – When all the hosts from DNS SRV resolution are reachable and send 200 OK for the OPTION message
  - **Busyout** (inactive) – When all the hosts from the DNS SRV resolution DO NOT respond or send an Error response
  - **Partial** – This is a new state, if one of the hosts from the DNS SRV resolution fails to send a 200 OK response
- CUBE will check the status of the nodes when routing a call. If the node is in a busyout state, CUBE will not send the call to that node and move to the next node in the host list

Feature Operation

```
dial-peer voice 786 voip
 session target dns:webex.com
 voice-class sip options-keepalive profile 1
```



Dial-peer show output - Active

- `show dial-peer voip keepalive status <tag> | <tenant>`
- New CLI introduced from 17.9.1, this will list all the hosts that are being monitored using the sip options keepalive profile.
- Case 1 - Dial-peer is active as all the hosts are reachable

```
CUBE#show dial-peer voip keepalive status 786

 TAG        TENANT    DESTINATION                  OOD-SessID   PRI    WT     STATUS
 786        -         dns:webex.com                                          active
                      example3.webex.com           46           10     50     active
                      ipv4:10.64.86.70:5880
                      example2.webex.com           45           10     50     active
                      ipv4:10.65.105.59:5060
                      example1.webex.com           44           10     50     active
                      ipv4:10.65.105.58:5060
```


Dial-peer show output - Partial

- `show dial-peer voip keepalive status <tag> | <tenant>`
- Case 2 - Dial-peer is partially active as one of the hosts is not reachable

```
CUBE#show dial-peer voip keepalive status 786

 TAG        TENANT     DESTINATION                 OOD-SessID    PRI     WT      STATUS
 786        -          dns:webex.com                                             partial
                       example3.webex.com          46            10      50      busyout
                       ipv4:10.64.86.70:5880
                       example2.webex.com          45            10      50      active
                       ipv4:10.65.105.59:5060
                       example1.webex.com          44            10      50      active
                       ipv4:10.65.105.58:5060
```

Dial-peer show output - Busyout

- `show dial-peer voip keepalive status <tag> | <tenant>`
- Case 3 - Dial-peer is busyout as all the hosts are not reachable

```
CUBE#show dial-peer voip keepalive status 786

 TAG       TENANT    DESTINATION                OOD-SessID   PRI   WT    STATUS
 786       -         dns:webex.com                                       busyout
                     example3.webex.com         46           10    50    busyout
                     ipv4:10.64.86.70:5880
                     example2.webex.com         45           10    50    busyout
                     ipv4:10.65.105.59:5060
                     example1.webex.com         44           10    50    busyout
                     ipv4:10.65.105.58:5060
```


OPTIONs Keepalive profile show output

```
CUBE#show voice class sip-options-keepalive 1
Voice class sip-options-keepalive: 1 AdminStat: Up
 Description: keepalive-webex
 Transport: tcp Sip Profiles: 0
 Interval(seconds) Up: 5 Down: 15
 Retry: 1
  Peer Tag    Server Group OOD SessID  OOD Stat    IfIndex
  --------    ------------ ----------  --------    -------
  786                                    None        31
  OOD SessID: 46            OOD Stat:    Busy
   Target: ipv4:10.64.86.70:5880
   Transport: tcp           Sip Profiles: 0
  OOD SessID: 47            OOD Stat:    Active
   Target: ipv4:10.65.105.59:5060
   Transport: tcp           Sip Profiles: 0
  OOD SessID: 48            OOD Stat:    Active
   Target: ipv4:10.65.105.58:5060
   Transport: tcp           Sip Profiles: 0
```

Dial-peer voice summary show output

```
CUBE#show dial-peer voice summary
dial-peer hunt 0
                AD                                              PRE PASS SESS-SER-GRP\   OUT
TAG      TYPE   MIN   OPER PREFIX DEST-PATTERN   FER THRU SESS-TARGET   STAT PORT    KEEPALIVE
3001     voip   down down                          0   syst
3002     voip   down down          6022            0   syst ipv4:10.65.105.25
12851    voip   up    up           +48203577....$  0   systipv4:10.48.53.54                 busyout
786      voip   up    up           50785           0   syst dns:webex.com                   partial
 For server-grp details please execute command:show voice class server-group <tag_id>
 To see complete session target for ipv6 use 'sh running-config | section dial-peer <tag>
```

DNS SRV based Call Routing

DNS SRV Based Call Routing

- The usage of DNS SRV as the target for CUBE helps in load balancing of the outbound SIP call traffic across a trunk.
- CUBE distributes calls across the SRVs based on the **priority, weight,** and **status (only active hosts) of the DNS SRV records**.
- If the priority and weight are the same, then the node will be selected in round-robin fashion.
- If CUBE receives a 503 response or no response for the INVITE, CUBE then marks that node as “Busyout” and attempts the call on the next node that is marked as active. The call is rejected if CUBE does not receive any response from any of the elements.

Call distribution based on DNS SRV lookup

Case 1 : Record routes with same priority and same weight

Configuration:

```
_sip._tcp.example1.webex.com   524   IN   SRV   10  50  5060  example1.webex.com
_sip._tcp.example2.webex.com   524   IN   SRV   10  50  5060  example2.webex.com
_sip._tcp.example3.webex.com   524   IN   SRV   10  50  5880  example3.webex.com
```

Total calls:- 3284

Call Counts on all 3 User Agent Server

example1.webex.com : 1083

example2.webex.com : 1099

example3.webex.com : 1102

Call distribution based on DNS SRV lookup

Case 2 : Record routes with same priority but different weights

Configuration:

```
_sip._tcp.example1.webex.com   524  IN   SRV  10 80 5060 example1.webex.com
_sip._tcp.example2.webex.com   524  IN   SRV  10 50 5060 example2.webex.com
_sip._tcp.example3.webex.com   524  IN   SRV  10 50 5880 example3.webex.com
```

Total calls:- 3004

Call Counts on all 3 User Agent Server

example1.webex.com : 2391

example2.webex.com : 321

example3.webex.com : 292

Call distribution based on DNS SRV lookup

Case 3 : One Record Route with lower priority and the other two Record Routes with higher priority and same weight across

Configuration:

```
_sip._tcp.example1.webex.com   524   IN   SRV   70  50  5060  example1.webex.com
_sip._tcp.example2.webex.com   524   IN   SRV   10  50  5060  example2.webex.com
_sip._tcp.example3.webex.com   524   IN   SRV   10  50  5880  example3.webex.com
```

Total calls:- 1000

Call Counts on all 3 User Agent Server

example1.webex.com : 0

example2.webex.com : 499

example3.webex.com : 501

Call distribution based on DNS SRV lookup

Case 4 : Record Routes with different priorities but same weight across

Configuration:

```
_sip._tcp.example1.webex.com   524  IN   SRV  10 50 5060 example1.webex.com
_sip._tcp.example2.webex.com   524  IN   SRV  20 50 5060 example2.webex.com
_sip._tcp.example3.webex.com   524  IN   SRV  30 50 5880 example3.webex.com
```

Total calls:- 1000

Call Counts on all 3 User Agent Server

example1.webex.com : 1000

example2.webex.com : 0

example3.webex.com : 0

Certificate-based LGW

Add Trunk

Hussain_Cert-based Successfully Created.

Visit Route Group page to add trunk(s) to a route group.
Visit Locations page to configure PSTN connection to individual locations.
Visit Dial Plans page to use this trunk as the routing choice for a dial plan.

```
dial-peer voice 2000 voip
 description To WxC Edge Proxy SRV Address
 session protocol sipv2
 session target dns:us01.sipconnect.bcld.webex.com
```

Webex Calling edge proxy address (FQDN)

peering1.us.sipconnect.bcld.webex.com:5062
peering2.us.sipconnect.bcld.webex.com:5062
peering3.us.sipconnect.bcld.webex.com:5062
peering4.us.sipconnect.bcld.webex.com:5062

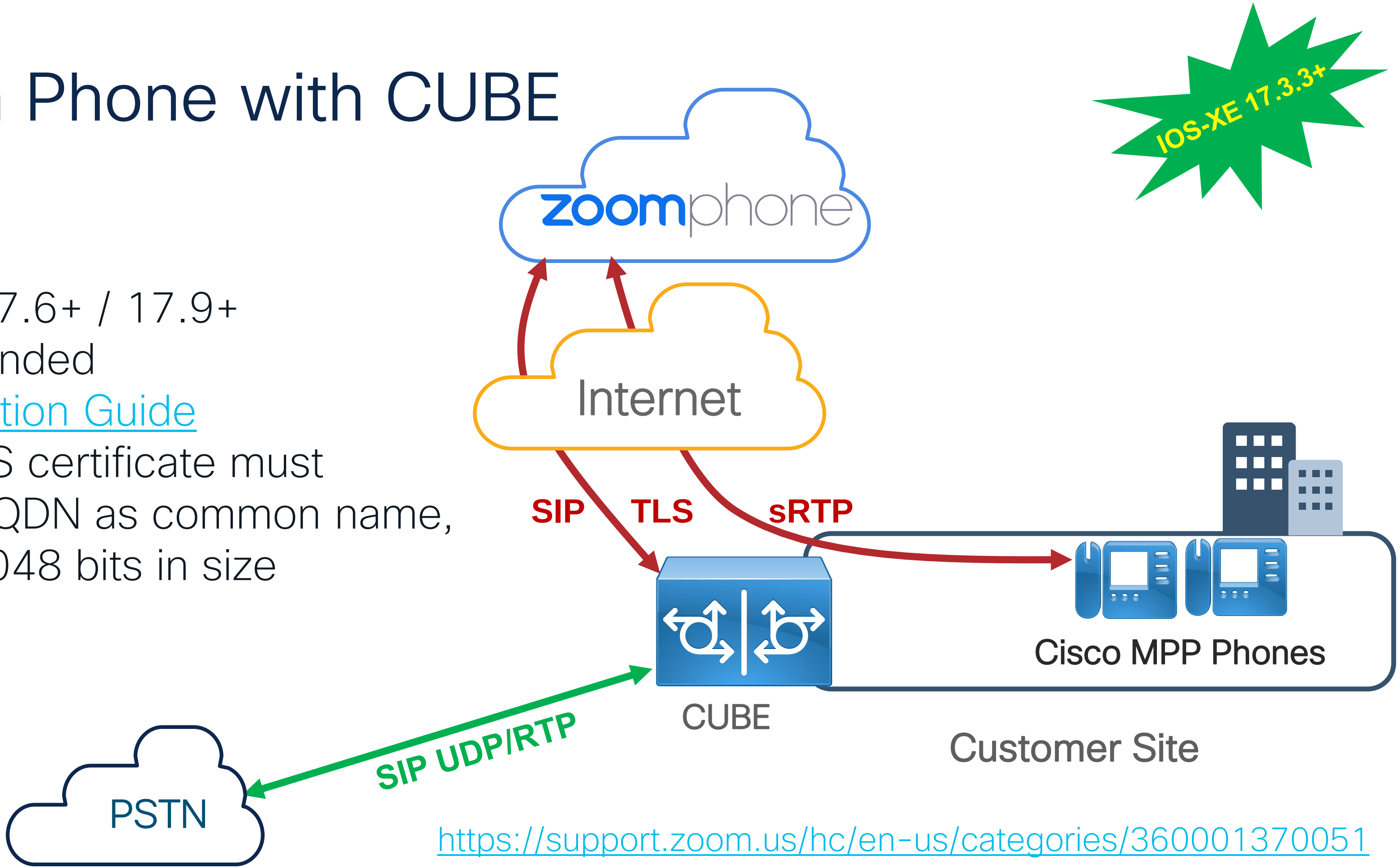
Webex Calling edge proxy address (SRV)

us01.sipconnect.bcld.webex.com

Enabling third-party Cloud Calling with CUBE

Zoom Phone with CUBE

- IOS-XE 17.6+ / 17.9+ recommended
- Configuration Guide
- CUBE TLS certificate must contain FQDN as common name, and be 2048 bits in size

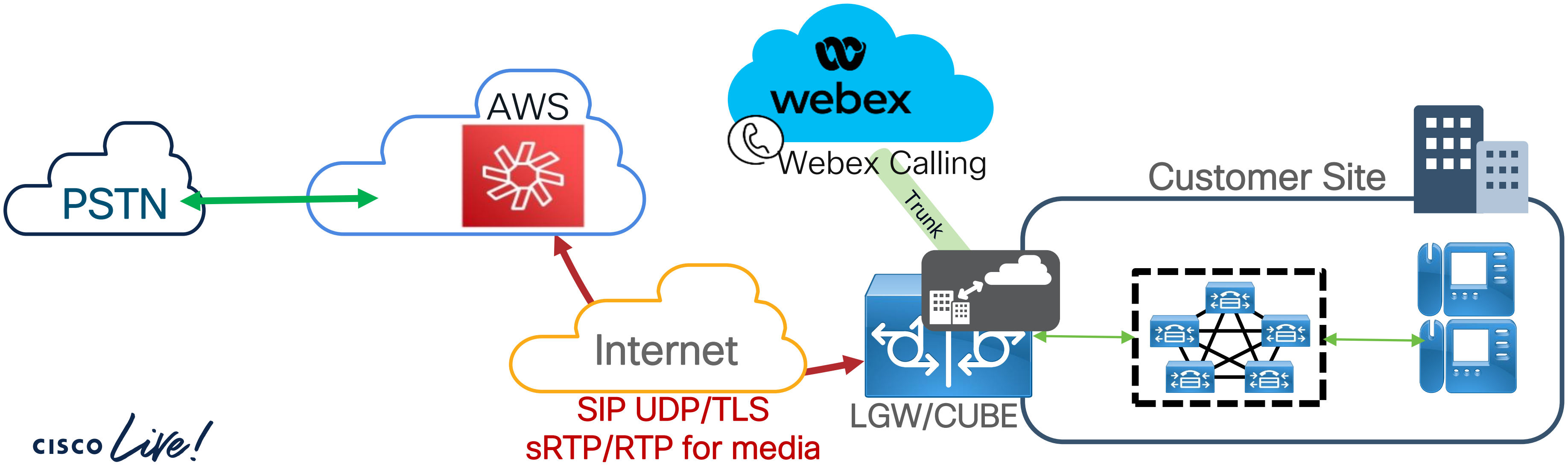


https://support.zoom.us/hc/en-us/categories/360001370051

Amazon Chime Voice Connector

IOS-XE 17.7+

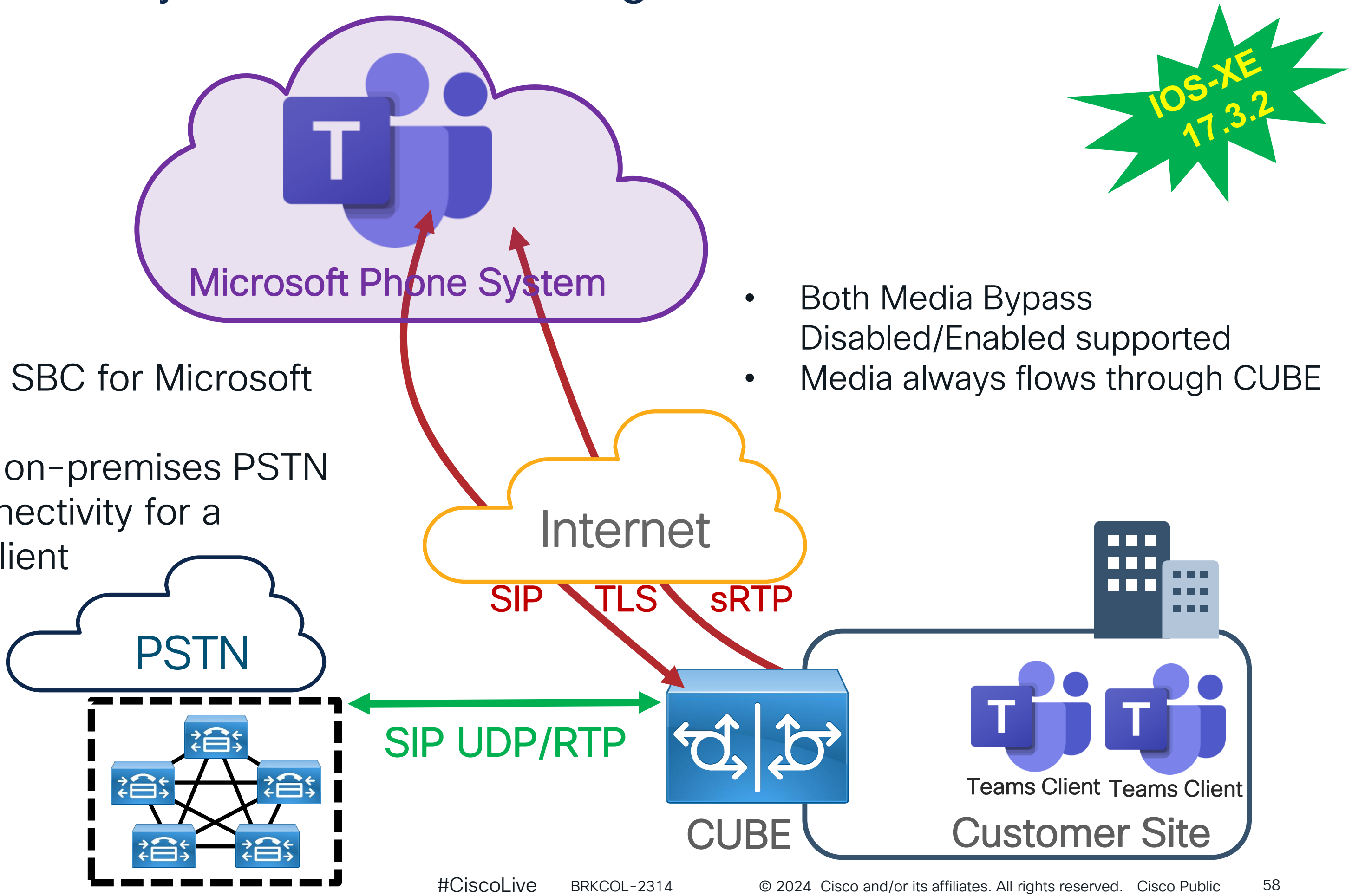
- Amazon Chimes provides PSTN service to an on-premises or a cloud-based phone system connected via a CUBE
- CUBE can be on-premises or hosted in AWS (vCUBE in AWS)
- IOS-XE 17.9+ recommended, but other IOS-XE releases also supported
- Configuration Guide
- https://aws.amazon.com/chime/chime-sdk/resources/#Configuration_Guides



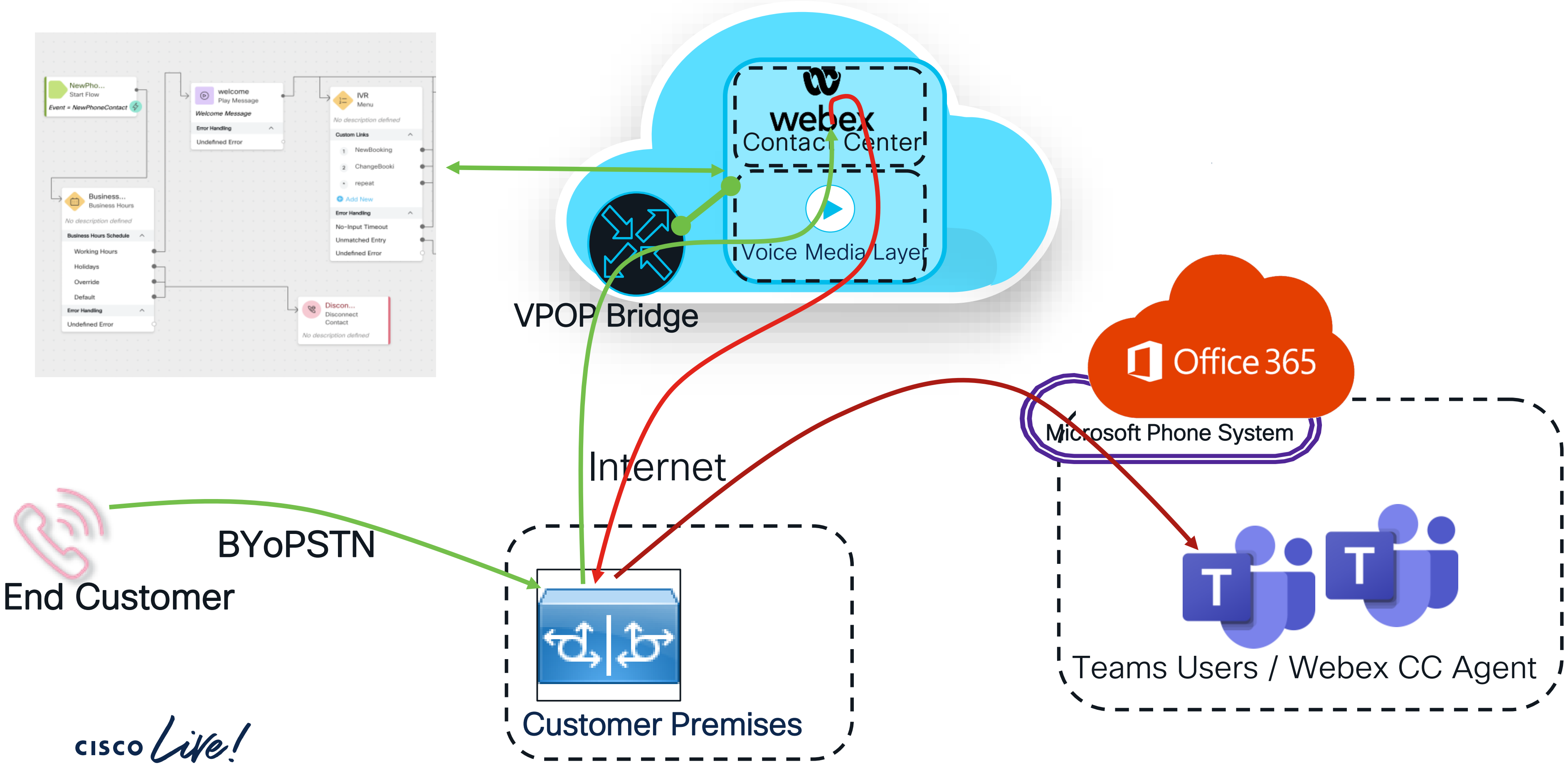
Microsoft Phone System Direct Routing with CUBE

- CUBE is a certified SBC for Microsoft Direct Routing
- You can configure on-premises PSTN and/or IP PBX connectivity for a Microsoft Teams client

- Both Media Bypass Disabled/Enabled supported
- Media always flows through CUBE



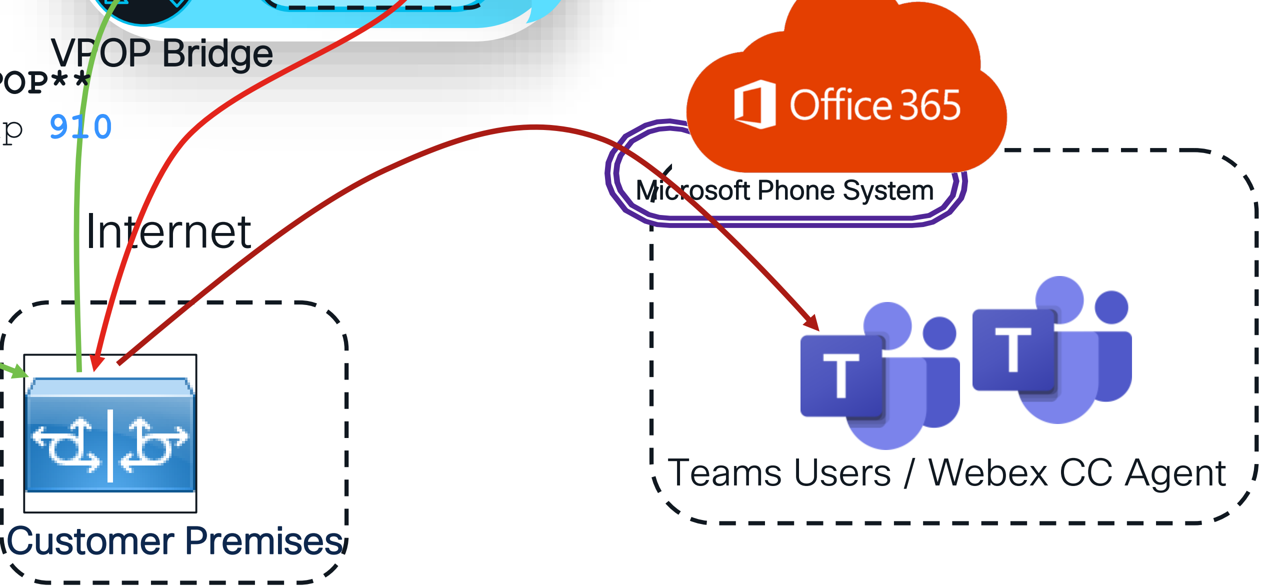
Webex Contact Center (WxCC) with MS teams



Inbound WxCC to MS Team call

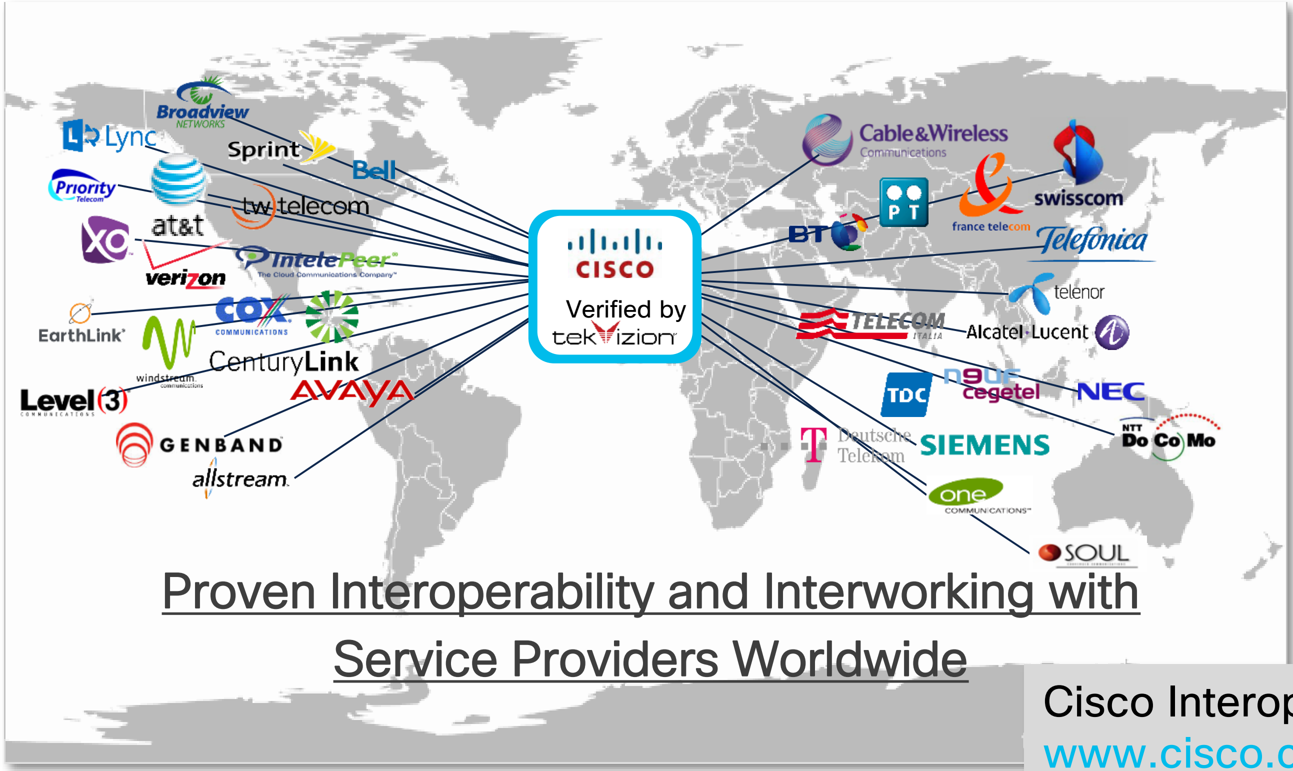
```
voice class e164-pattern-map 910
 description Towards US VPOP
 e164 +17863057867 ! IVR Number
!
voice class uri 410 sip
 pattern +17863057867 ! WxCC IVR Number
!
dial-peer voice 401 voip
 description **Incoming from ITSP**
 incoming uri request 410

dial-peer voice 901 voip
 description **Towards US VPOP**
 destination e164-pattern-map 910
 session server-group 101
```

```
voice class uri ProdUSURI sip
 host ipv4:208.92.126.68
 host ipv4:208.92.126.69
voice class e164-pattern-map 200
 e164 +16074208976 ! Agent Number

dial-peer voice 200 voip
 description To MS Teams Proxy 1
 preference 1
 session target dns:sip.pstnhub.microsoft.com:5061
 destination e164-pattern-map 200
 voice-class sip tenant 200
 srtp

dial-peer voice 900 voip
 description Inbound from US VPOP
 incoming uri via ProdUSURI
```




```
voice class server-group 101
 ipv4 208.92.126.68
 ipv4 208.92.126.69
description - WxCC US VPOP
```

CUBE Interoperability Portal for application notes



- Zoom Phone
- Microsoft Direct Routing
- Amazon Chime Voice Connector
- vCUBE-on-AWS
- vCUBE-on-Azure
- **Multi-tenant Direct Routing**
- **Multi-tenant Certificate-based LGW**
- **Multi-tenant Registration-based LGW**

Cisco Interoperability Portal:
www.cisco.com/go/interoperability

Managing Gateways from the Webex Control Hub

Introducing Gateway Connectors

- Gateway connectors are small applications that run in the gateway Guest Shell to maintain a connection to Control Hub, co-ordinate events and collect status information.
- Guest Shell is independent of IOS-XE running on the platform
- NETCONF and YANG data models are used as opposed to the Command Line (CLI) to manage the gateways, thus, allowing APIs to manage and configure the gateways
- Two types of connectors exist
  - Management Connector - takes care of gateway enrollment to the cloud and lifecycle management of the telemetry connector
  - Telemetry Connector – used for pushing configs and getting command requests from the CH to the gateway

Connector Considerations

- ISR 1100 series are not supported
- CUBE High Availability (HA) mode is not supported
- Controller or SD-WAN mode is not supported (only IOS-XE Autonomous mode is supported)
- Currently two services are supported:
  - Registration-based Local Gateway Configuration Validation
  - Survivability Gateway Configuration template (BRKCOL-2993)
- IOS-XE version required:
  - Local Gateways—Cisco IOS XE 17.6.1a or later
  - Survivability Gateways—Cisco IOS XE 17.9.3a or later

Connector Installation Prerequisites

- The platform must have the following configured:
  - DNS Server `ip name-server <IP Address>`
  - HTTP Proxy

```
ip http client proxy-server <server address> proxy-port <port-number>
ip http client username <username>
ip http client password <password>
```

  - Default AAA lists to authenticate and authorize NETCONF access

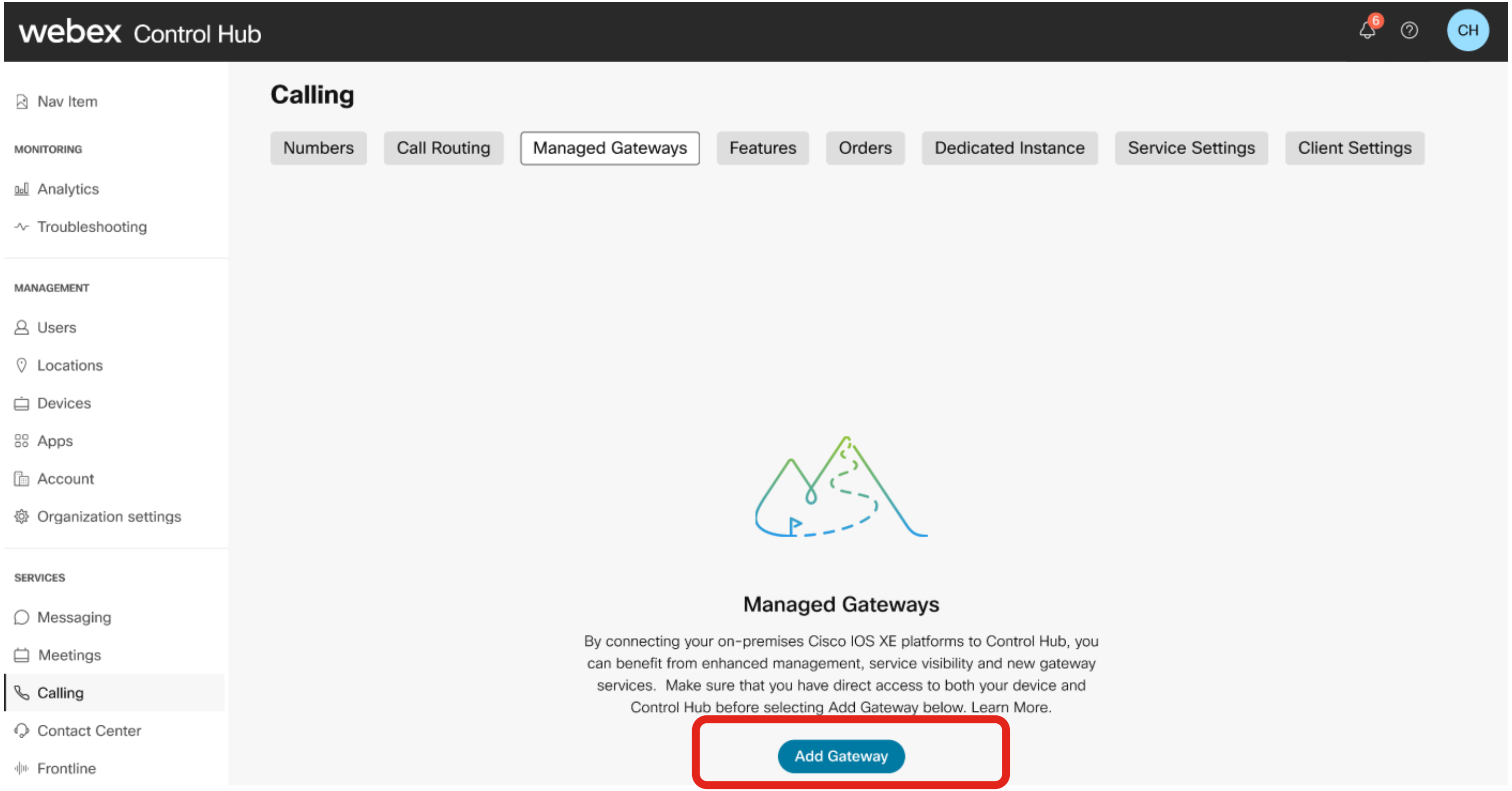
```
aaa new-model
aaa authentication login default radius local
aaa authorization exec default radius local if-authenticated
username test privilege 15 secret <password>
```

  - Import the IOS-XE public CA bundle

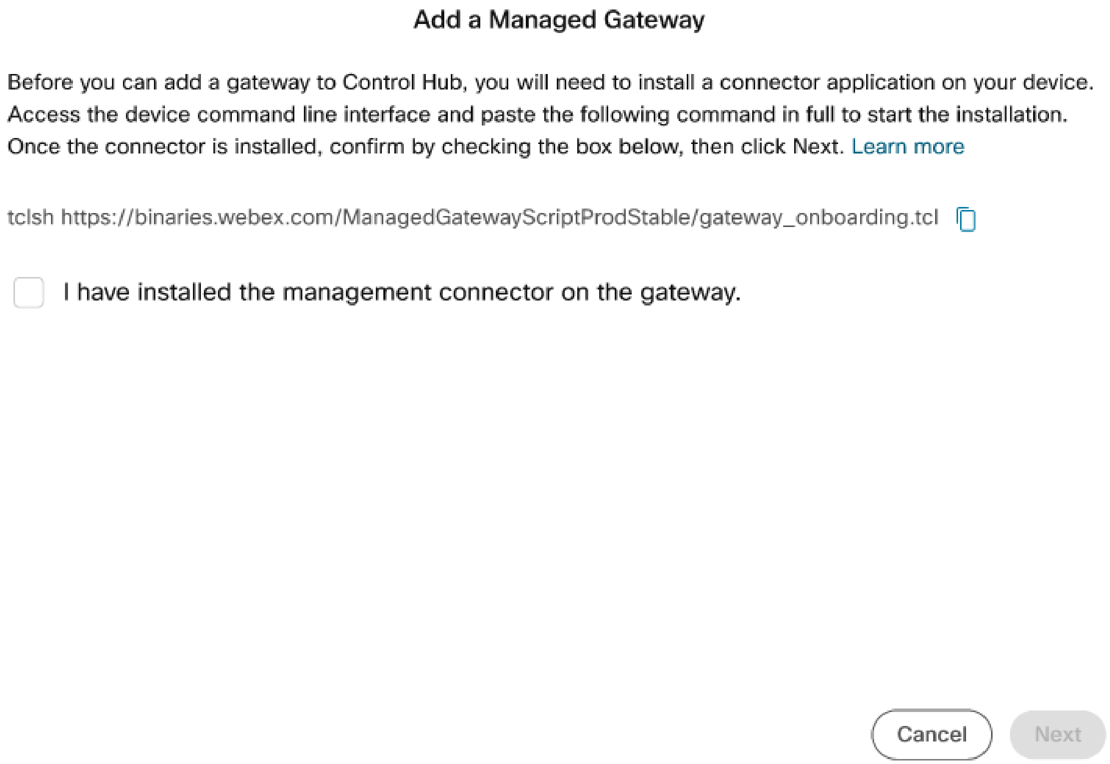
```
crypto pki trustpool import url
http://www.cisco.com/security/pki/trs/ios.p7b
```

Add a New Gateway Instance in Control Hub

Under **Services**, click **Calling** and then click the **Managed Gateways** Tab



In the **Add a Managed Gateway** window, copy the command to install the connector onto the Gateway



Run the Management Connector deployment Script

- Run the TCL script
  - tclsh https://binaries.webex.com/ManagedGatewayScriptProdStable/gateway_onboarding.tcl
- Follow the wizard

```
C8KV-Hussain#
C8KV-Hussain#$m/ManagedGatewayScriptProdStable/gateway_onboarding.tcl
Loading https://binaries.webex.com/ManagedGatewayScriptProdStable/gateway_onboarding.tcl !!
 Cisco IOS XE Software Version: 17.9.20221213
 Script Version: 3.0.3
 Precondition check status: Passed
 Downloading Gateway connector installer package...
```

Select the External Interface to reach Webex Cloud

```
        ================================================================
                      Webex Gateway Connector Installation
        ================================================================


Choose the external-interface from the below list of available interfaces:
        ================================================================
         Number    Interface                 IP-Address          Status
        ================================================================
              1    GigabitEthernet1          10.52.12.203        up
        ================================================================

Enter a number to choose the external interface: 1
```

- The script creates a Virtual Port Group interface that shares the same IP as the chosen interface. It is used for the routing of GuestShell container traffic
- The script displays only the interfaces which are in "up" state and have IP addresses assigned

Confirm or Edit DNS and Proxy settings

```
These DNS settings were detected in the gateway configuration:
144.254.71.184 173.38.200.100

Do you want to use these settings for the connector? [Y/n]: Y

These proxy settings were detected in the gateway configuration:

Proxy Server : proxy.esl.cisco.com
Proxy Port   : 80

Do you want to use these settings for the connector? [Y/n]: Y
```

Specify the Connector IP Address and Credentials

```
Enter Connector IP address: 10.52.12.216


Enter Gateway username: hussain
Enter Gateway password: *******
Confirm Gateway password: ******
```

```
Enabling guestshell...this may take upto 4 minutes, please wait for completion.
```

Connector Successfully Installed

```
=====================================================================
                  Webex Managed Gateway Connector
=====================================================================


      *** Cloud connector is installed successfully. ***
    ------------------------------------------------------------
                  *** Interface Status ***
    ------------------------------------------------------------
       Interface                IP-Address           Status
    ------------------------------------------------------------
       GigabitEthernet1         10.52.12.203         up
       VirtualPortGroup0        10.52.12.203         up
       Connector                10.52.12.216         up

    ------------------------------------------------------------


                     *** App Status ***
    ------------------------------------------------------------
                Service                  Status
    ------------------------------------------------------------
                Guestshell               RUNNING
                Management Connector     RUNNING
    ------------------------------------------------------------
```

Webex Managed Gateway Connector Options

```
=====================================================================
                  Webex Managed Gateway Connector
=====================================================================
     Options
       s :   Display Status Page
       v :   View and Modify Cloud Connector Settings
       e :   Enable Guestshell
       d :   Disable Guestshell
       l :   Collect Logs
       r :   Clear Logs
       u :   Uninstall Connector
       q :   Quit


=====================================================================
                  Select an option from the menu:
```

vCUBE on AWS/Azure Connector Considerations

- For vCUBE on AWS, you need to associate a secondary IP address
  - To use Virtual CUBE on the Amazon Web Services (AWS) as your Local Gateway, you must associate a secondary private IP address with the gateway interface. You can use this IP address as the connector IP address.
  - Associate an Elastic public IP address with the secondary IP address so that the secondary IP address is publicly available for gateway enrollment. **Follow the steps in the below URL prior to using the private IP address as the Connector IP address during the connector installation**
  - https://help.webex.com/en-us/article/xftgfc/Enroll-Cisco-IOS-managed-gateways-to-Webex-Cloud#associate-ip-addresses-for-virtual-cube-on-aws
- In Azure, secondary IP cannot have Internet access and hence, we need to follow the workaround from Microsoft documented at https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/no-internet-access-multi-ip

vCUBE on Azure Connector Considerations

```
! provision dummy lo0 interface first
interface loopback0
ip address 192.168.35.1 255.255.255.0

! run connector install script

! assign connector ip as 192.168.35.2
(and link to loopback 0)

# tclsh
https://binaries.webex.com/ManagedGatewayScriptProdStable/gateway_onboarding.tcl

! Credentials for connector should be the
same as the platform

! after installation remove lo0 interface
and assign ip from it into vpg0:
no int lo0
interface VirtualPortGroup0
ip address 192.168.35.1 255.255.255.0
ip nat inside
```

```
interface GigabitEthernet2
ip address 10.48.53.163 255.255.254.0
ip nat outside

ip access-list standard GSNAT
 10 permit 192.168.35.0 0.0.0.255

! disable local http(s) server as we
will be doing NAT for 443 port
no ip http server
no ip http secure-server

ip nat inside source list GSNAT
interface GigabitEthernet2 overload

ip nat inside source static tcp
192.168.35.2 443 interface
GigabitEthernet2 443
```

Enroll the Gateway in the Control Hub

In the **Add a Managed Gateway** window, check the **I have installed the management connector on the gateway** check box and click **Next.**

Add a Managed Gateway

Before you can add a gateway to Control Hub, you will need to install a connector application on your device. Access the device command line interface and paste the following command in full to start the installation. Once the connector is installed, confirm by checking the box below, then click Next. Learn more

```
tclsh https://binaries.webex.com/ManagedGatewayScriptProdStable/gateway_onboarding.tcl
```

- [x] I have installed the management connector on the gateway.

Cancel Next

At the **Add a Managed Gateway** screen, enter the connector IP address that you entered during the connector installation procedure, and a preferred display name for the gateway

Add a Managed Gateway

Enter the following details for your installed connector. Click Next to open the connector web interface where you can complete device enrollment.

Enter the connector IP address

10.52.12.216

You will need to be able to reach this address directly from your browser.

Enter a display name for the gateway

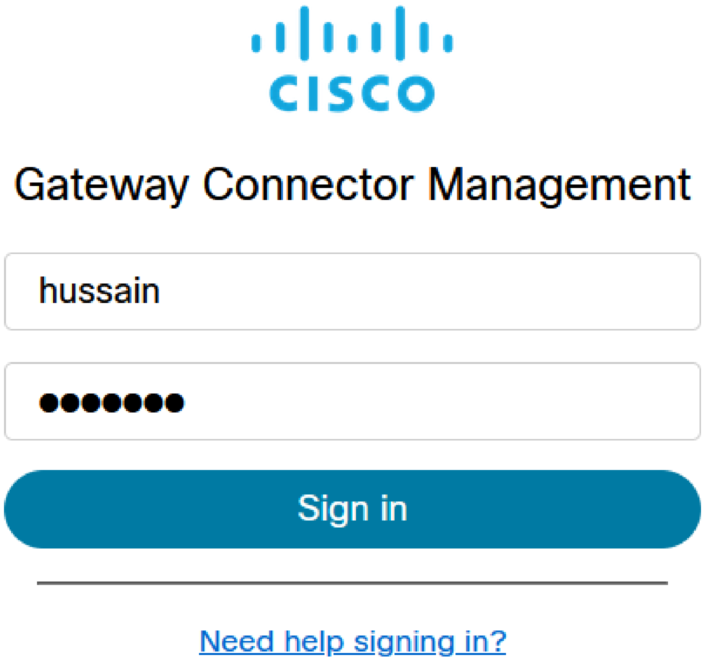
Hussain-Cat8kv

The name is for display purposes only.

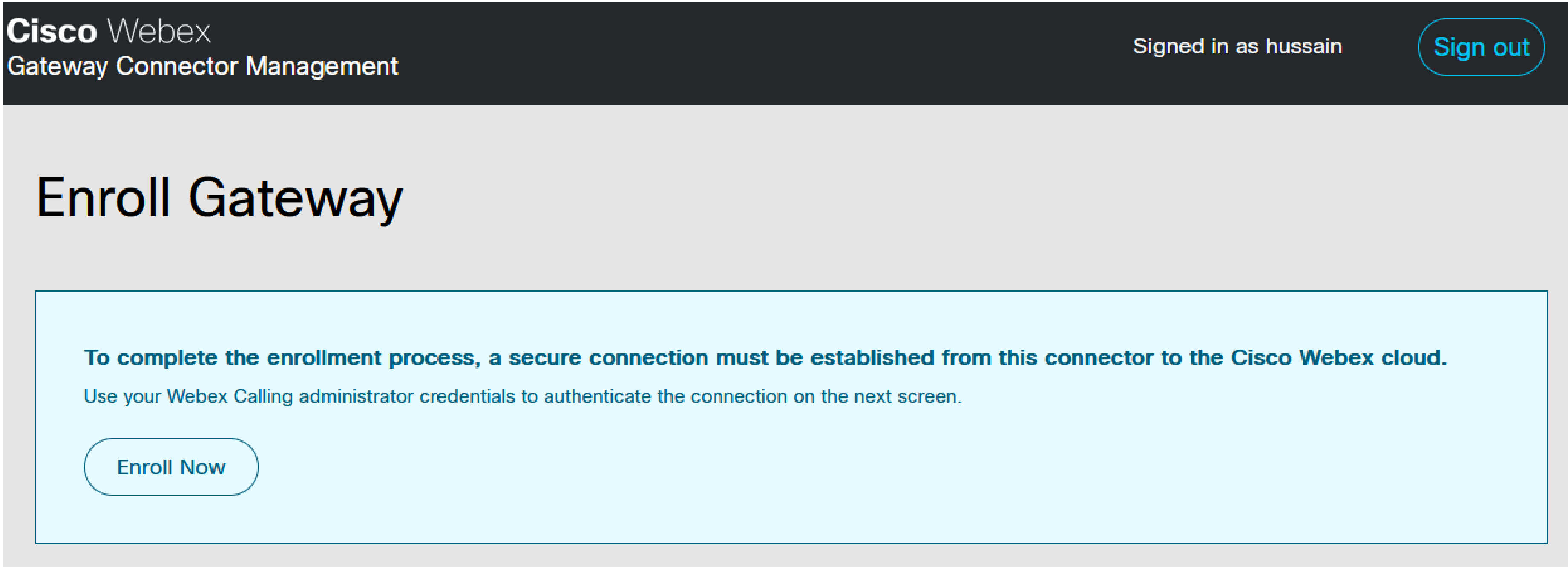
Once enrollment is complete, gateways will appear in the Managed Gateway list.

Cancel   Next

At the Connector Management page, enter the Gateway Admin **Username** and **Password** that you specified during the connector installation procedure



Click the **Enroll Now** button within an hour



Sign in using a Webex Administrator account

Check the **Allow Access to the Gateway Management Connector** check box

Gateway Management Connector

Allow Access to Gateway Management Connector

Permissions are required to allow your Cisco Webex organization to create, read, update, and delete user accounts, as well as read and update information about your organization.

Organization

WxCSA Team Sandbox

FQDN or IP Address

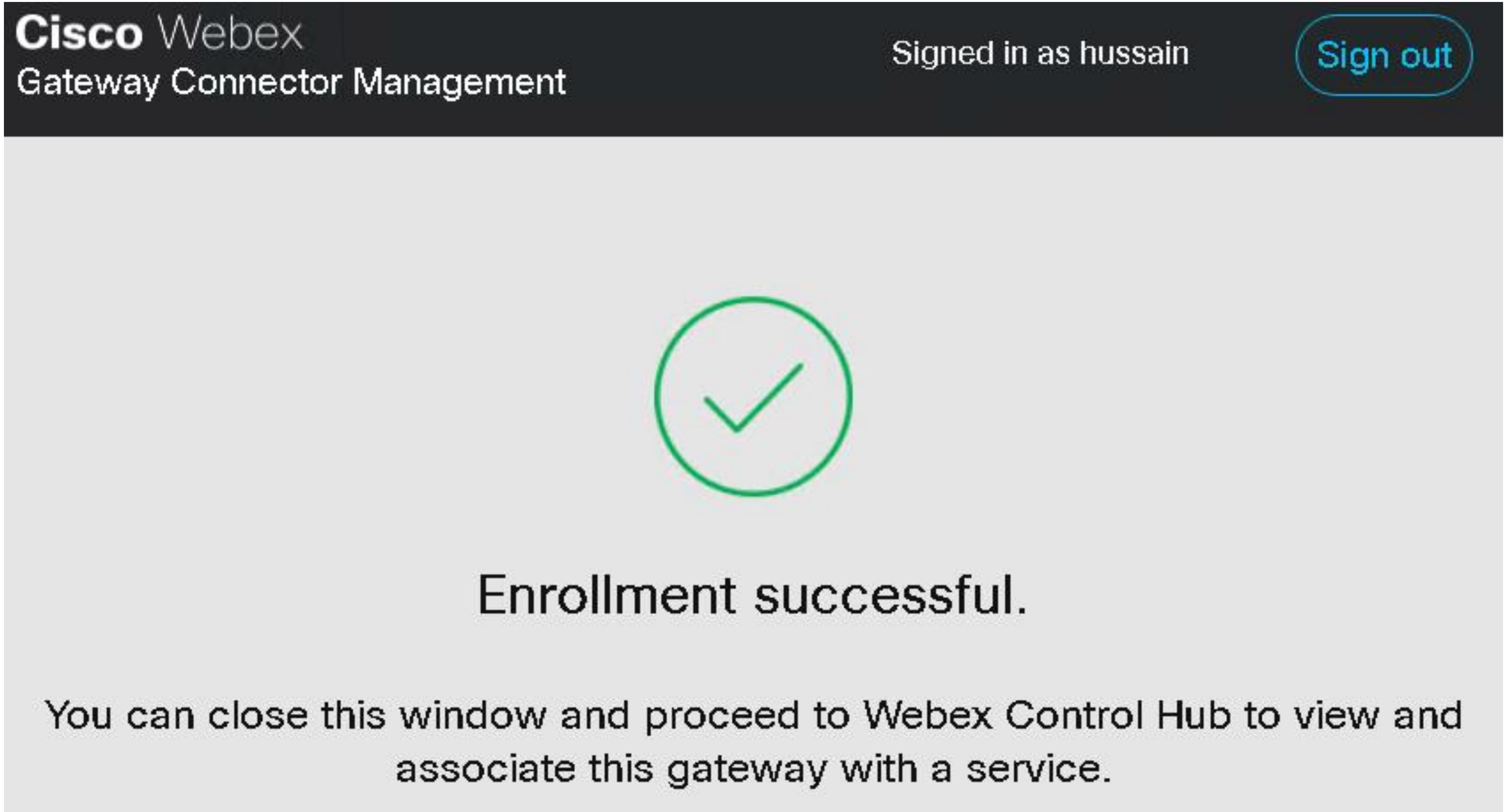
10.52.12.216

- [x] Allow Access to the Gateway Management Connector

Only allow access to hosts you know and trust

Continue

Enrollment Successful



Managed Gateways

Calling

Numbers | Locations | Call Routing | **Managed Gateways** | Features | PSTN | Service Settings | Client Settings

Search | All Gateways | 10 Gateway(s) | Events History | Add Gateway

Gateway Name	Version	Connector Sta...	Service	Assigned to	Actions
Amsterdam SGW	17.9.3	Online	Survivability Gateway	Location: Amsterdam Office	···
Hussain-Cat8kv		-	-	-	···
Lisbon SGW	17.9.3	Online	Survivability Gateway	Location: Lisbon Office	···
London SGW	17.9.3	Offline	Survivability Gateway	Location: London Branch Office	···
Madrid SGW	17.9.3	Online	Survivability Gateway	Location: Madrid Office	···
Munich SGW	17.9.3	Online	Survivability Gateway	Location: Munich Office	···
Paris SGW	17.9.3	Online	Survivability Gateway	Location: Paris Office	···
Rome SGW	17.9.3	Online	Survivability Gateway	Location: Rome Office	···
Vienna SGW	17.9.3	Online	Survivability Gateway	Location: Vienna Office	···

Validate Registration-based LGW Configuration through Control Hub

Managed Gateway now **Online**

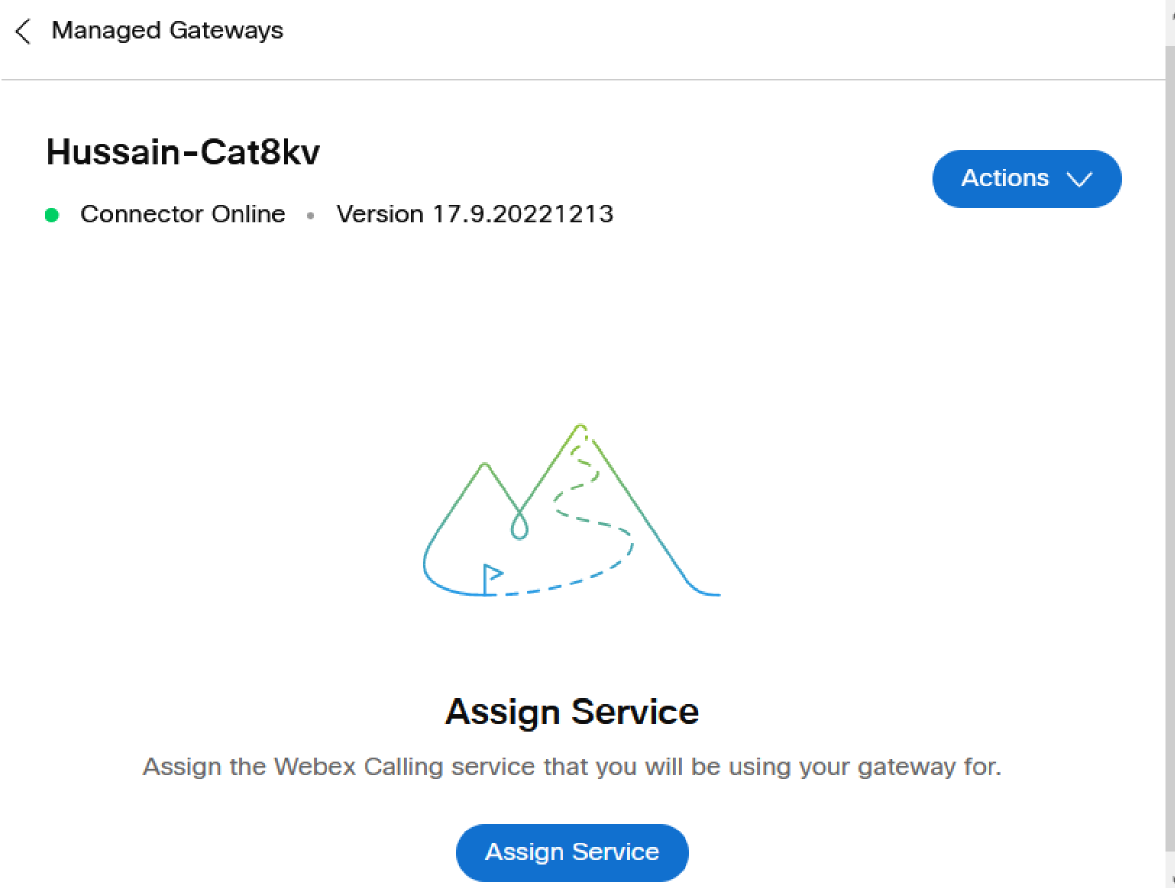
Calling

Numbers | Locations | Call Routing | **Managed Gateways** | Features | PSTN | Service Settings | Client Settings

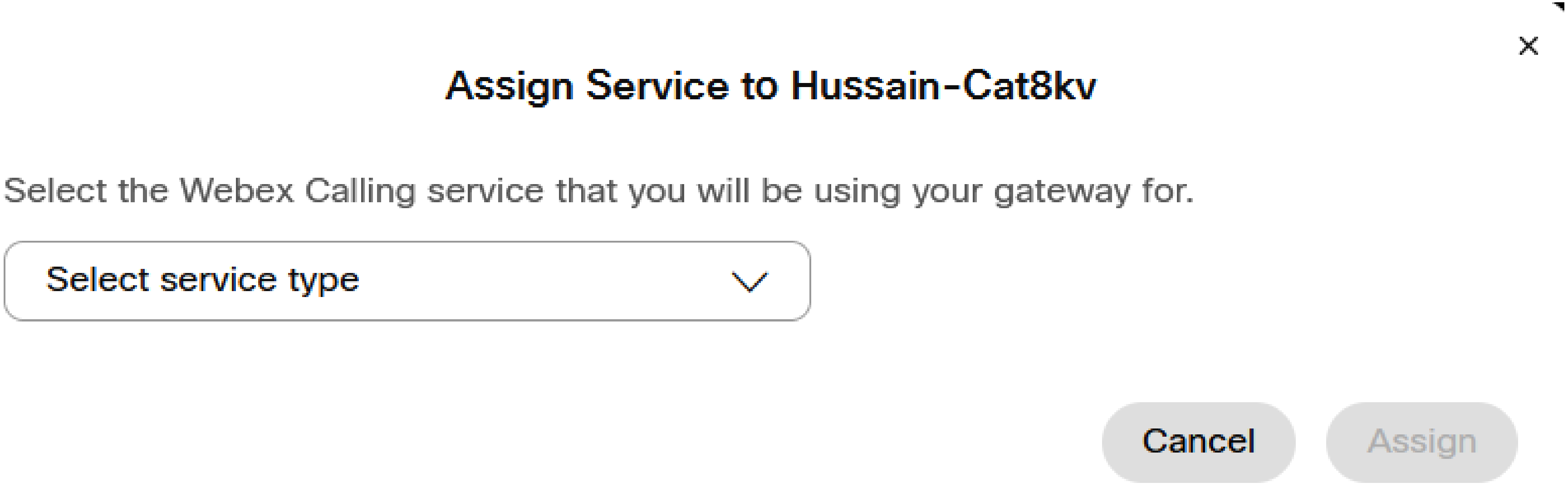
Search | All Gateways | 10 Gateway(s) | Events History | Add Gateway

Gateway Name	Version	Connector Sta...	Service	Assigned to	Actions
Amsterdam SGW	17.9.3	Online	Survivability Gateway	Location: Amsterdam Office	...
Hussain-Cat8kv	17.9.20221...	Online	-	-	...
Lisbon SGW	17.9.3	Online	Survivability Gateway	Location: Lisbon Office	...
London SGW	17.9.3	Offline	Survivability Gateway	Location: London Branch Office	...
Madrid SGW	17.9.3	Online	Survivability Gateway	Location: Madrid Office	...
Munich SGW	17.9.3	Online	Survivability Gateway	Location: Munich Office	...
Paris SGW	17.9.3	Online	Survivability Gateway	Location: Paris Office	...

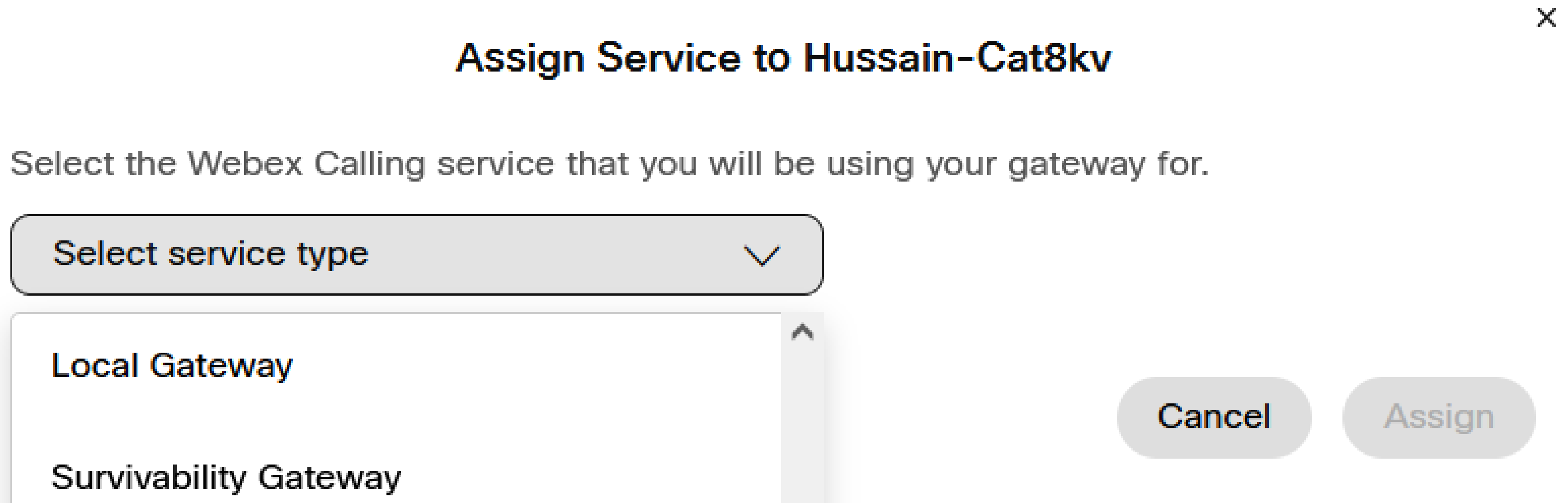
Assign a Service to the Managed Gateway



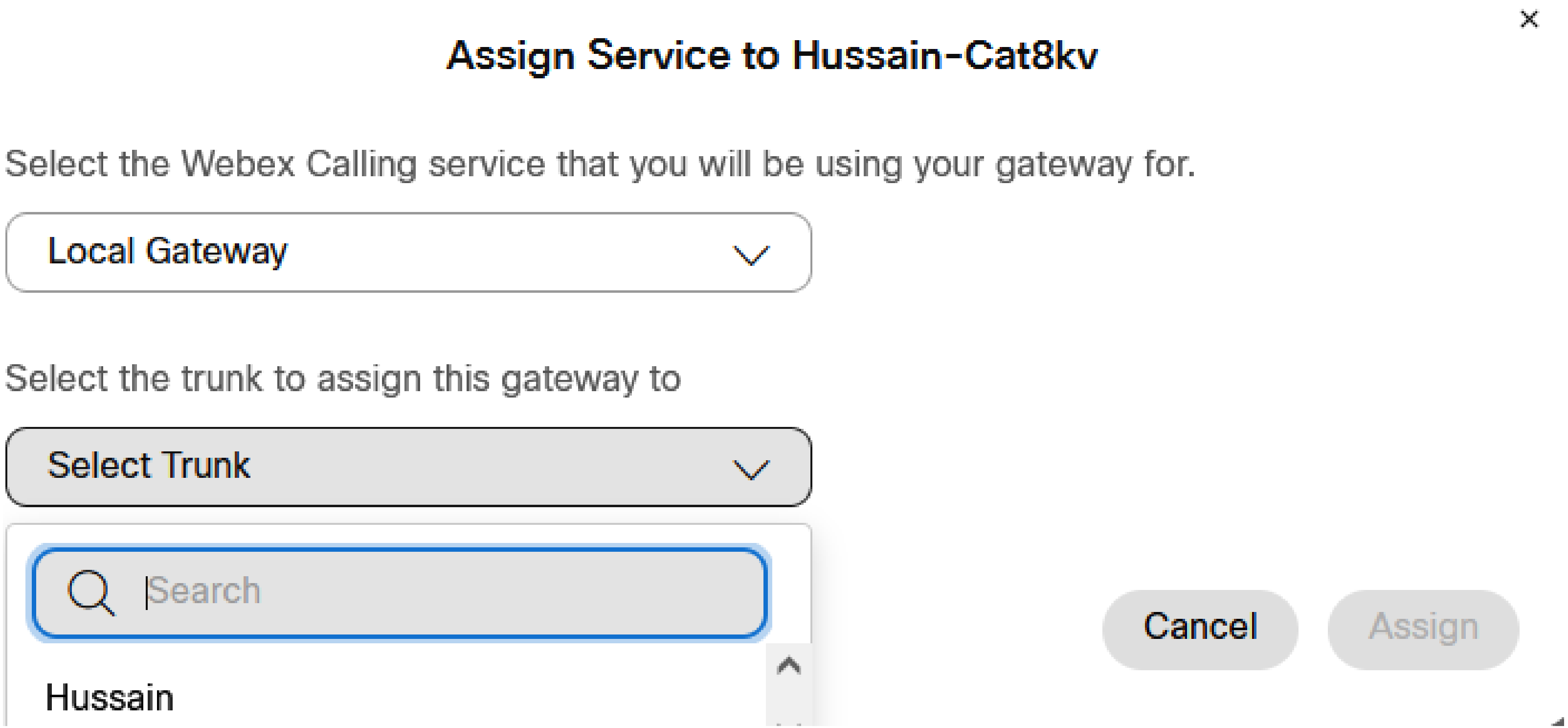
Select a Service Type



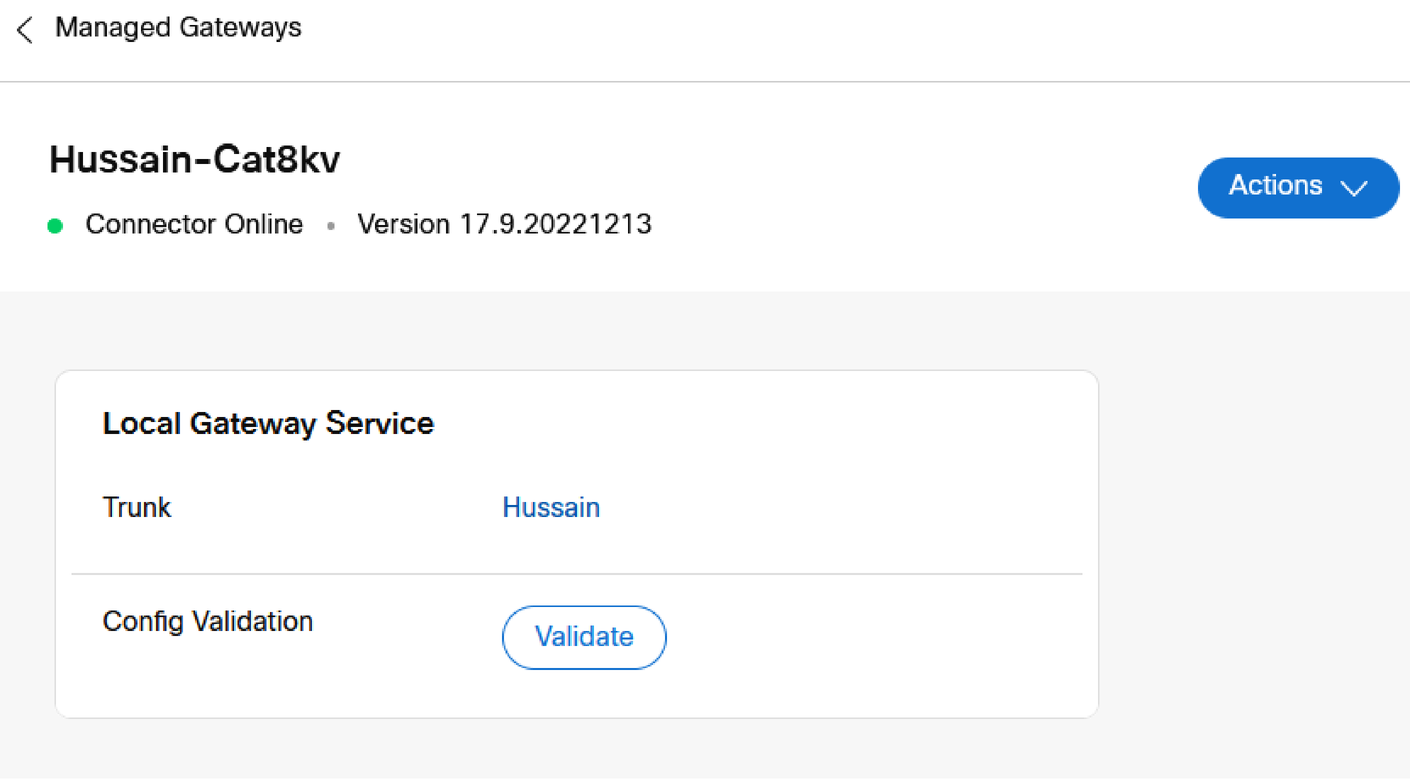
Service Type: LGW or SGW



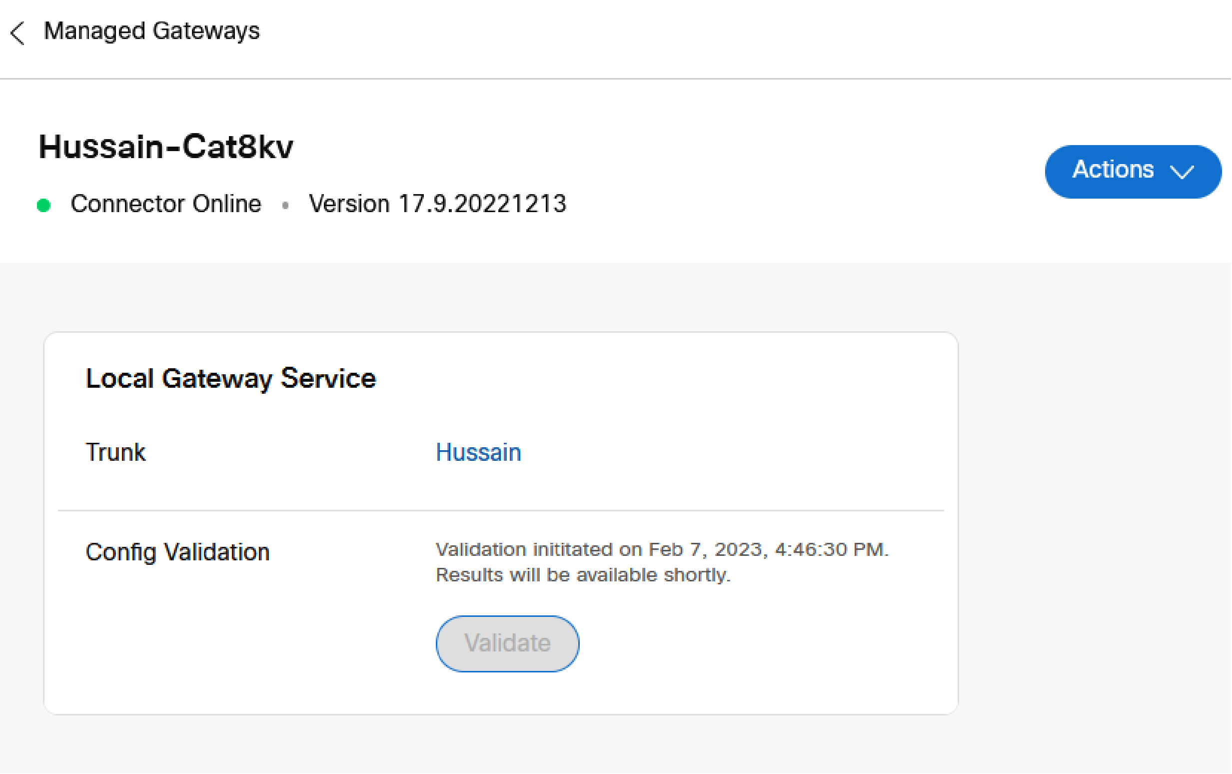
For Service Type Local Gateway, specify the **Trunk**



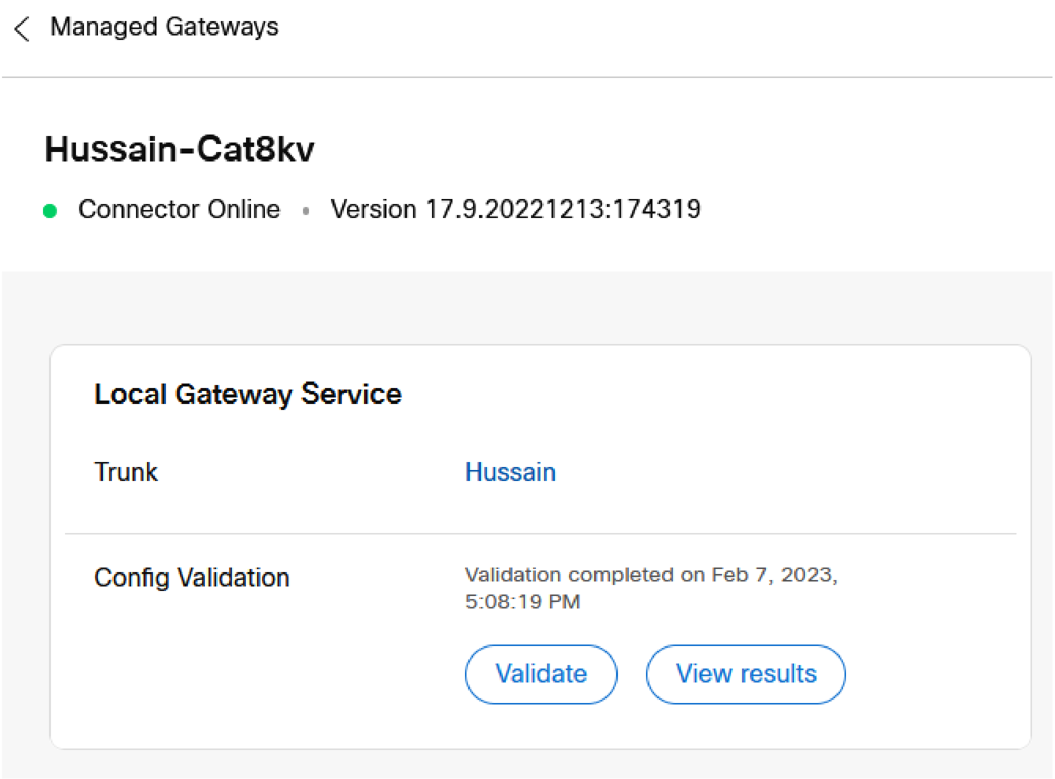
Validate Registration-based LGW Configuration



Validation takes a few minutes



View Validation results



In the Validated Configuration page, verify if there are any misconfigurations

Validated Configuration

sip-ua
No issues found

voice service voip
No issues found

voice class sip-profiles 200
1 misconfigured

Misconfigured: Rule mismatches with required rule.

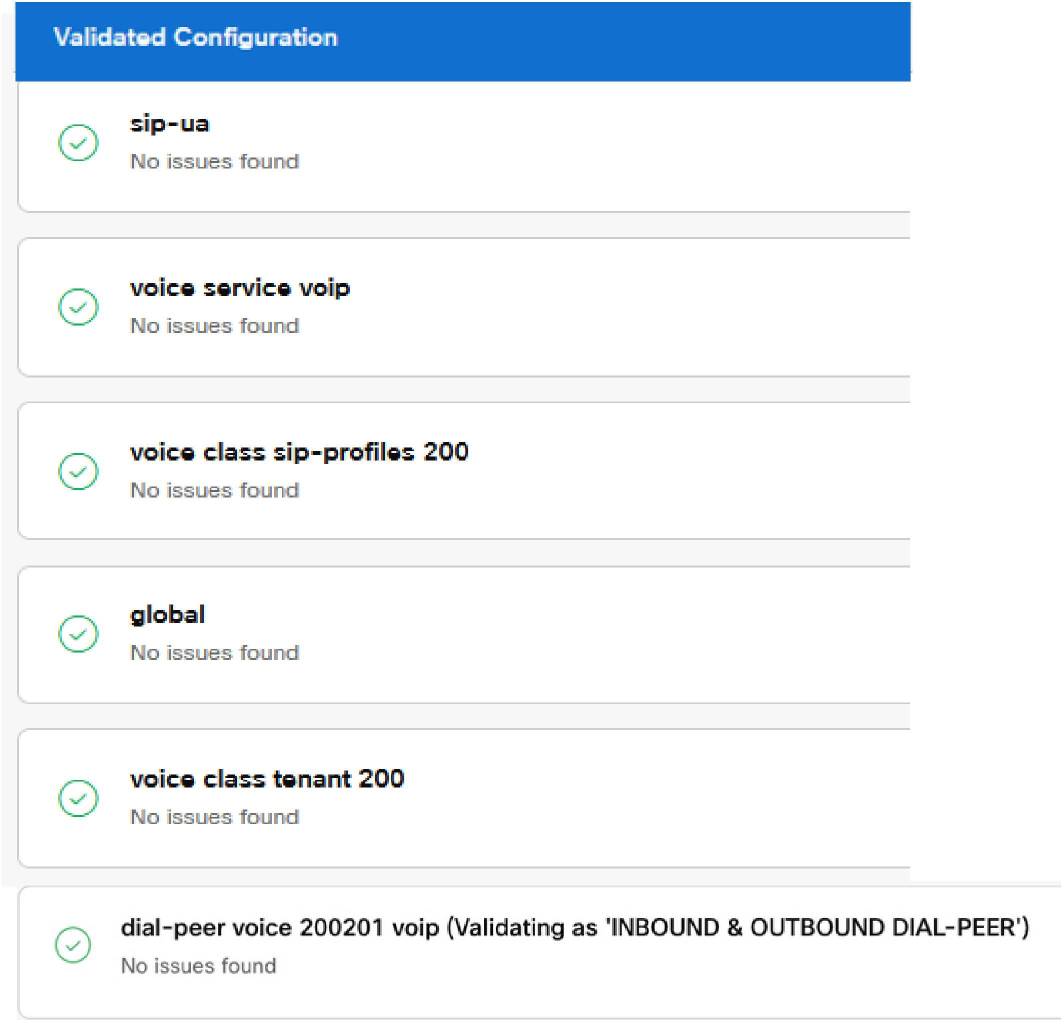
```
rule 11 request ANY sip-header From modify "<sips:" "<sip:\1"
```

Reference configuration

Copy

```
voice class sip-profiles 200
 rule 1 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
 rule 2 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 3 request ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 4 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"
 rule 5 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 6 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 7 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
 rule 8 request ANY sip-header From modify ">" ";otg=hussain5773_lgu>"
```

Fix misconfigurations within the Local Gateway and run validation again

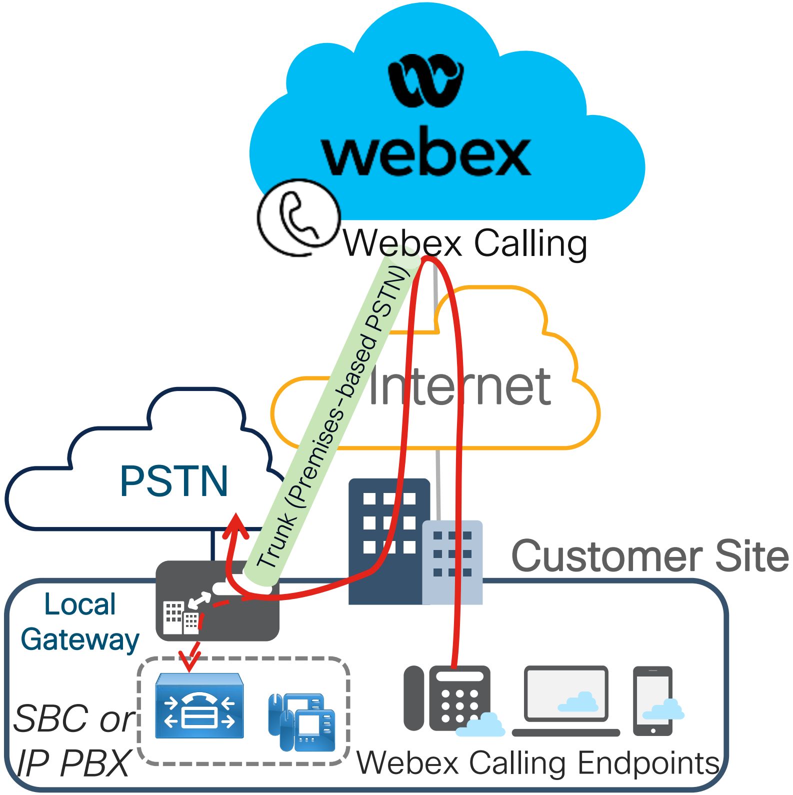


Local Gateway for Webex Calling

Premises-based PSTN Trunking models

Webex Calling Trunk - Local Gateway

(Premises-based PSTN) Deployment



- Provides connectivity to a customer-owned premises-based PSTN service
- May also provide connectivity to an on-premises IP PBX or dedicated SBC/PSTN GW
- Enables on-prem to Webex Calling transition
- **Endpoint registration is NOT proxied through Local Gateway.** Endpoints directly register to Webex Calling over the Internet.

Premises-based PSTN Trunking Models

- There are two types of Premises-based PSTN trunking models:
  - Registration-based trunks
  - Certificate-based trunks
- Both models provide similar functionality, but they differ in scale and device support

Comparing Local Gateway trunking models

Functionality	Registration-based	Certificate-based
Concurrent Calls	Concurrent calls of up to 250 per trunk (OTT Internet)	Up to 6500 concurrent calls per trunk
Device Type	Supports only CUBE (except ASR1000 series)	Supports all CUBE and 3rd party SBCs
Authentication model	Digest-based authentication model, which relies on a shared username and password used to authenticate registration and calls.	Certificate-based authentication model
Public DNS service requirements	None	Domain claims required. A DNS A or SRV record must be configured in public DNS server

Network, firewall, and NAT requirements

Registration-based	Certificate-based
Any NAT or Public IP is supported. • Dynamic NAT is preferred since it's easier for setup and requires less firewall configs For ingress traffic, inbound pinholes(from WxC to LGW) are opened by the firewall based on outbound registration messages Pinhole opening is recommended for all Webex Calling IP address and ports.	Public internet-facing network including a public IP or Static NAT.

Both requires firewall to allow both ingress and egress traffic (Webex calling to Local Gateway and vice versa).

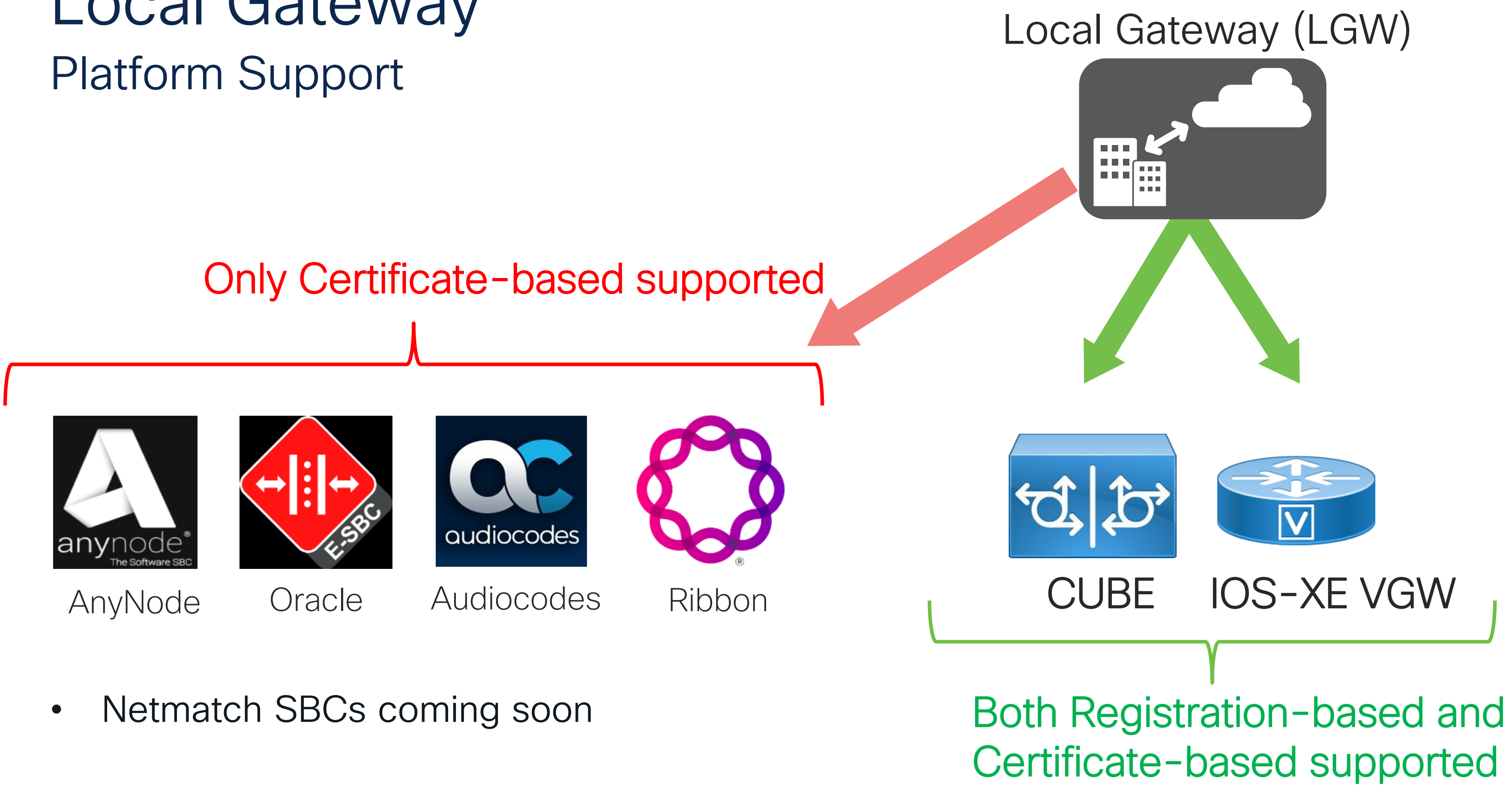
CA and certificate requirements

Registration-based	Certificate-based
	Local gateway must have a signed certificate using one of the certificate authorities listed in Root Certificate Authorities. • Wild-card certificates are not supported • Certificates must be signed per guidelines as mentioned in Configure Trunks, Route Groups, and Dial Plans for Webex Calling

CA bundle that signed the Webex service's certificate has to be uploaded to the Local Gateway.

Local Gateway

Platform Support



- Netmatch SBCs coming soon

Calling Capacity requirements

- Registration-based and Certificated-based trunking models have different concurrent call capacities as shown below

Concurrent calls per local gateway / trunk	Trunk type Preference	Minimum Link Quality
~ 2000-6500	Certificate-based	Interconnect
250 to ~ 2000	Certificate-based	Over the top Internet (OTT)
up to 250	Registration-based	OTT

Connection qualifications

- Over the top (OTT) Internet and interconnect (e.g. Webex Edge Connect) must meet the following link quality conditions

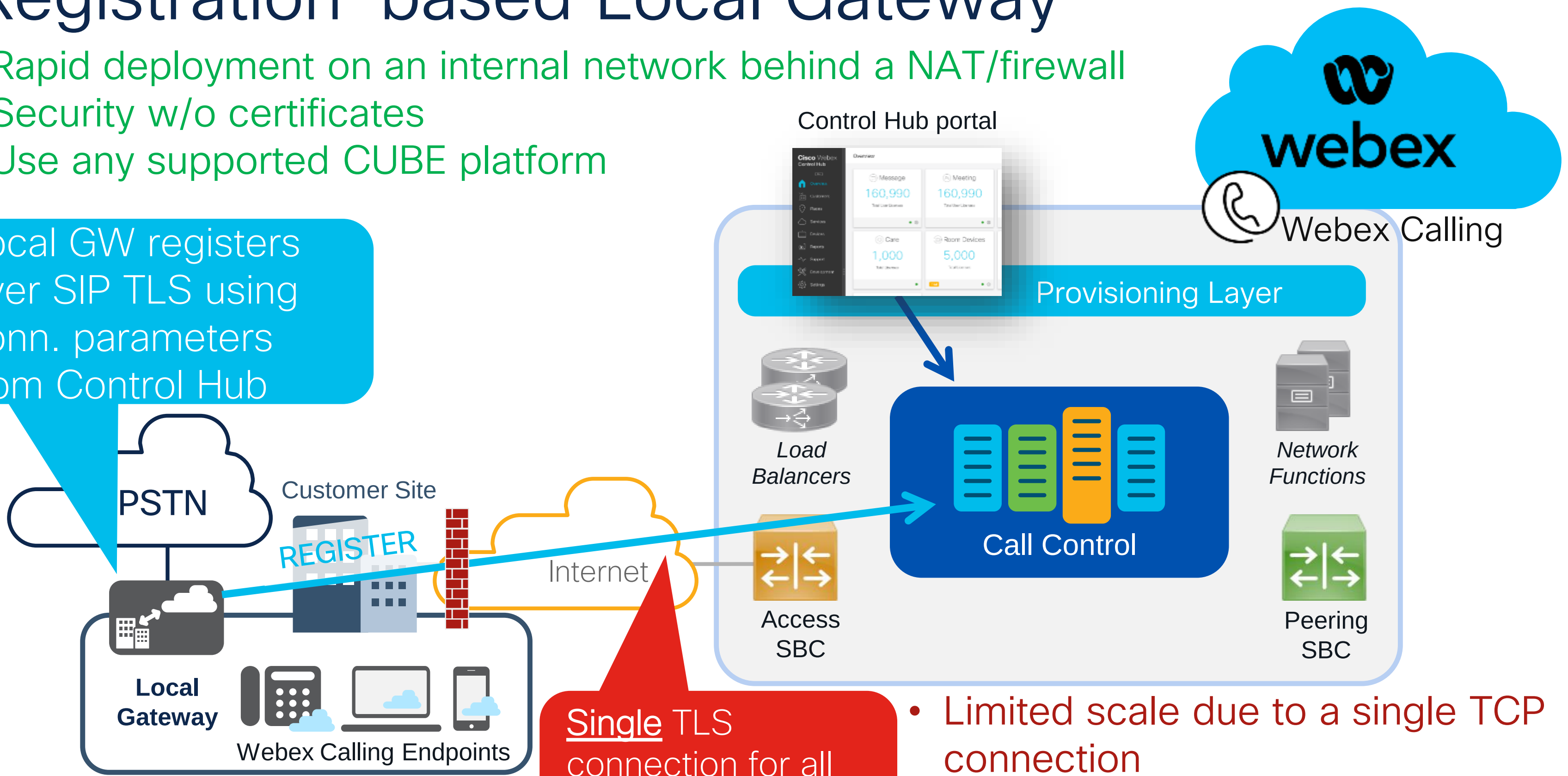
Connection Type	Latency	Jitter	Packet loss
OTT	100 ms (max)	100 ms (max)	0.2%
Interconnect	30 ms	5 ms	Zero packet loss

Multiple Registration-based LGWs on a single CUBE

Registration-based Local Gateway

- Rapid deployment on an internal network behind a NAT/firewall
- Security w/o certificates
- Use any supported CUBE platform

Local GW registers over SIP TLS using conn. parameters from Control Hub



Single TLS connection for all signaling between LGW and cloud

- Limited scale due to a single TCP connection
- Sensitive to network impairments (TCP throughput ∝ latency/loss)

Save the Trunk parameters to build the CUBE CLI for LGW

Parameters on this display required for building LGW CLI

Add Trunk

Hussain Successfully Created.

Visit Route Group page to add trunk(s) to a route group.

Visit Locations page to configure PSTN connection to individual locations.

Visit Dial Plans page to use this trunk as the routing choice for a dial plan.

Trunk Info

Status

● unknown

Trunk Group OTG/DTG

hussain2572_lgu

Outbound Proxy Address

la01.sipconnect-us10.cisco-bcld.com

Registrar Domain

40462196.cisco-bcld.com

Line/Port

Hussain6346_LGU@40462196.cisco-bcld.com

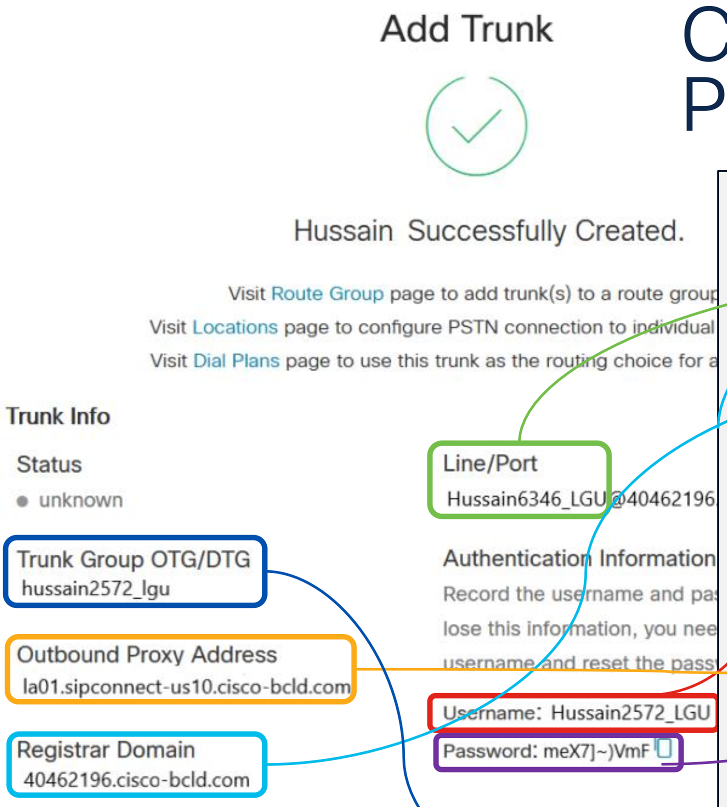
Authentication Information

Record the username and password below. If you lose this information, you need to retrieve the username and reset the password.

Username: Hussain2572_LGU

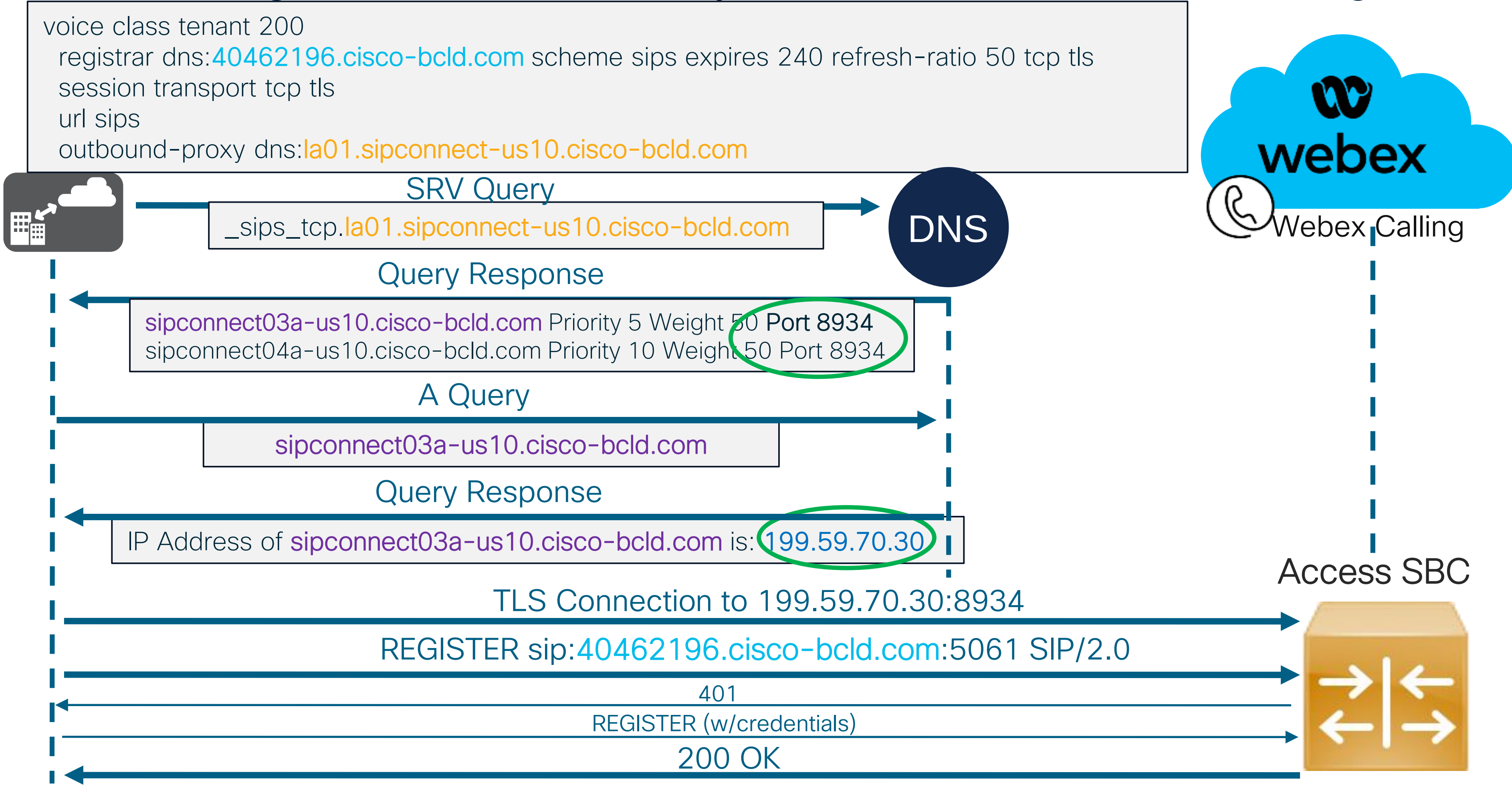
Password: meX7]~)VmF

Control Hub Trunk Info Connection Parameters → LGW CLI Config



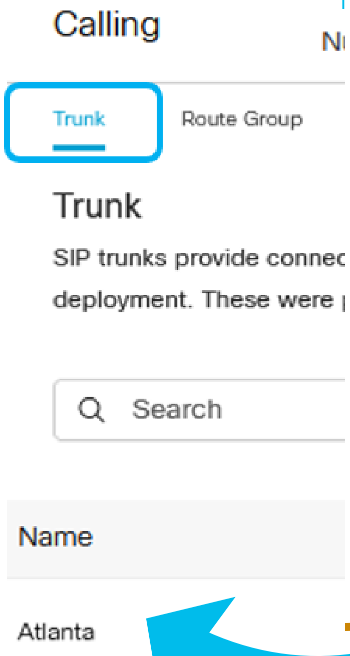

```
voice class tenant 200
  registrar dns:40462196.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls
  credentials number Hussain6346_LGU username Hussain2572_LGU password 0 meX7]~)VmF realm
BroadWorks
  authentication username Hussain2572_LGU password 0 meX7]~)VmF realm BroadWorks
  authentication username Hussain2572_LGU password 0 meX7]~)VmF realm 40462196.cisco-bcld.com
  sip-server dns:40462196.cisco-bcld.com
  connection-reuse
  srtp-crypto 200
  session transport tcp tls
  url sips
  error-passthru
  bind control source-interface GigabitEthernet0/0/1
  bind media source-interface GigabitEthernet0/0/1
  no pass-thru content custom-sdp
  sip-profiles 200
  outbound-proxy dns:la01.sipconnect-us10.cisco-bcld.com
...
voice class sip-profiles 200
 rule 1 request ANY sip-header SIP-Req-URI modify "sips:" "sip:"
 rule 10 request ANY sip-header To modify "<sips:" "<sip:"
 rule 11 request ANY sip-header From modify "<sips:" "<sip:"
 rule 12 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"
 rule 13 response ANY sip-header To modify "<sips:" "<sip:"
 rule 14 response ANY sip-header From modify "<sips:" "<sip:"
 rule 15 response ANY sip-header Contact modify "<sips:" "<sip:"
 rule 16 request ANY sip-header From modify ">" ";otg=hussain2572_lgu>"
 rule 17 request ANY sip-header P-Asserted-Identity modify "<sips:" "<sip:"
```

Establishing Secure Connectivity b/w LGW and Webex Calling



What constitutes a Registration-based LGW within a CUBE platform?

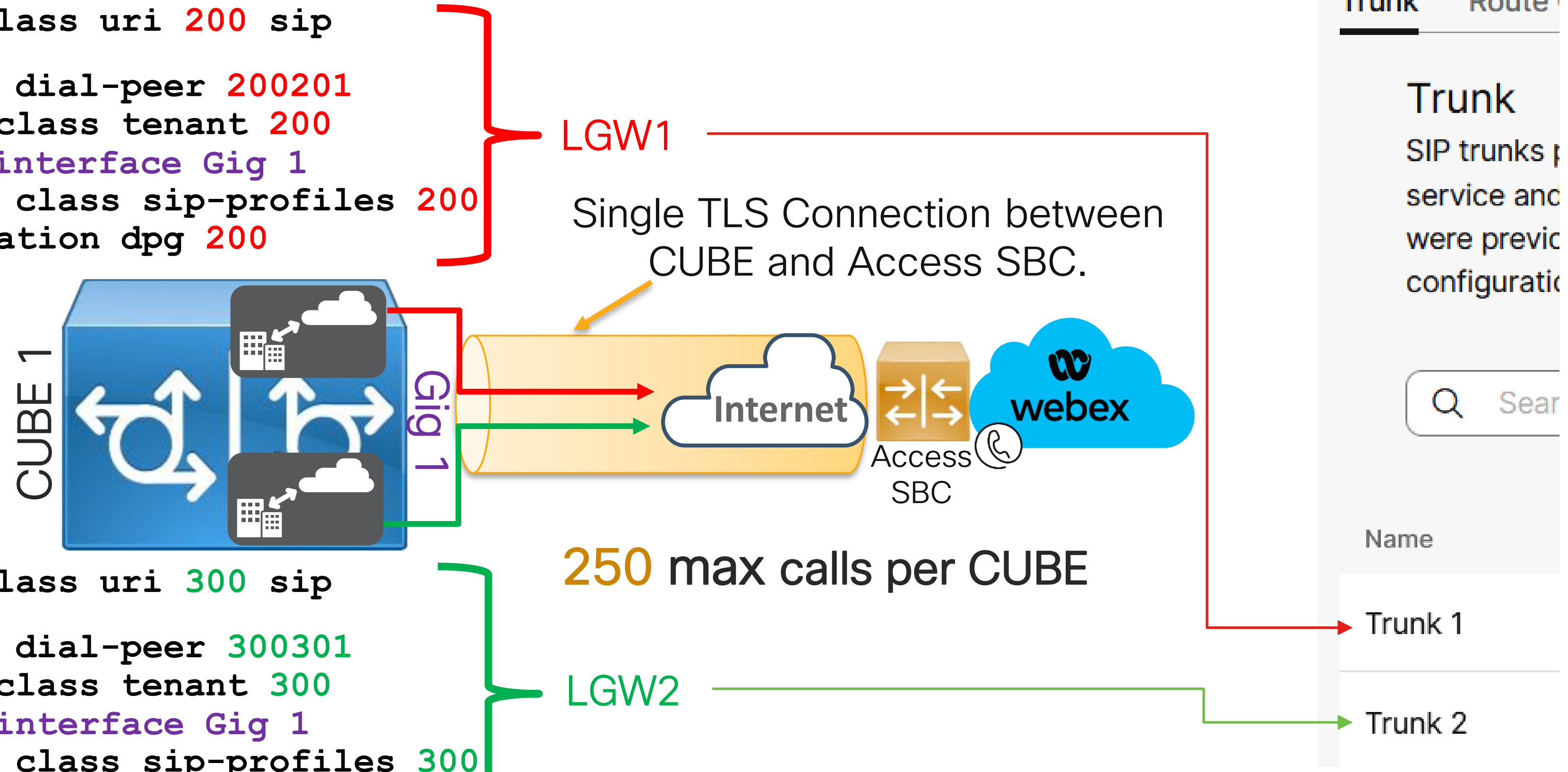
```
voice class sip-profiles 200
  rule 20 request ANY sip-header From modify ">" ";otg= hussain2572_lgu >"
voice class tenant 200
   registrar dns:XXXXXX scheme sips expires 240 refresh-ratio 50 tcp tls
   credentials number XXXXXX username XXXXXX password 0 XXXXXX realm BroadWorks
   authentication username XXXXXX password 0 XXXXXX realm BroadWorks
   authentication username XXXXXX password 0 XXXXXX realm XXXXXX
   sip-server dns:XXXXXX
   session transport tcp tls
   url sips
   bind control source-interface GigabitEthernet1
   bind media source-interface GigabitEthernet1
   sip-profiles 200
   outbound-proxy dns:XXXXXX
voice class uri 200 sip
   pattern dtg=hussain2572_lgu
dial-peer voice 200201 voip
   description In/Out WxC
   max-conn 250
   destination-pattern BAD.BAD
   session protocol sipv2
   session target sip-server
   destination dpg 100
   incoming uri request 200
   voice-class sip tenant 200
```



Single CUBE platform with two LGWs

1 TLS Connection to Access SBC = 250 max calls

```
voice class uri 200 sip

Inbound dial-peer 200201
 voice class tenant 200
  bind interface Gig 1
   voice class sip-profiles 200
 destination dpg 200
```




```
voice class uri 300 sip

Inbound dial-peer 300301
 voice class tenant 300
  bind interface Gig 1
   voice class sip-profiles 300
 destination dpg 300
```

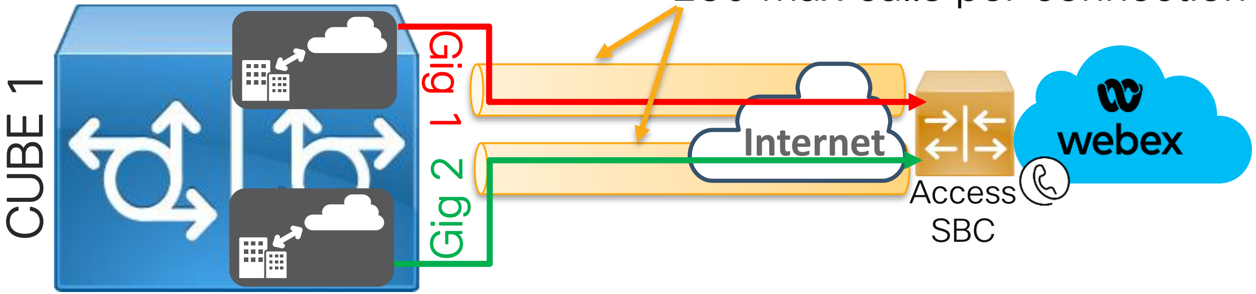
Single CUBE platform with two LGWs

2 TLS Connections to Access SBC = 500 max calls

```
voice class uri 200 sip

Inbound dial-peer 200201
 voice class tenant 200
  bind interface Gig 1
   voice class sip-profiles 200
 destination dpg 200
```

LGW1

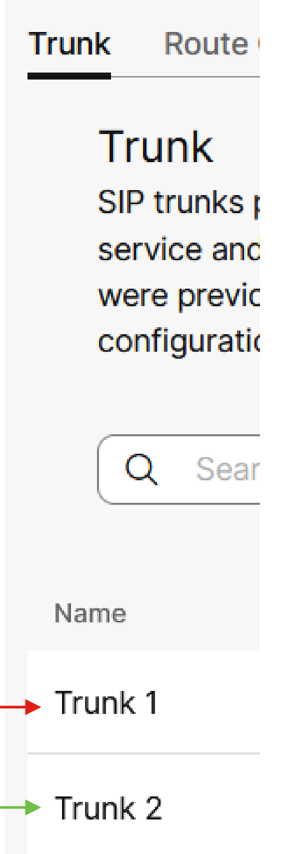
Each LGW with its own TLS connection = 250 max calls per connection



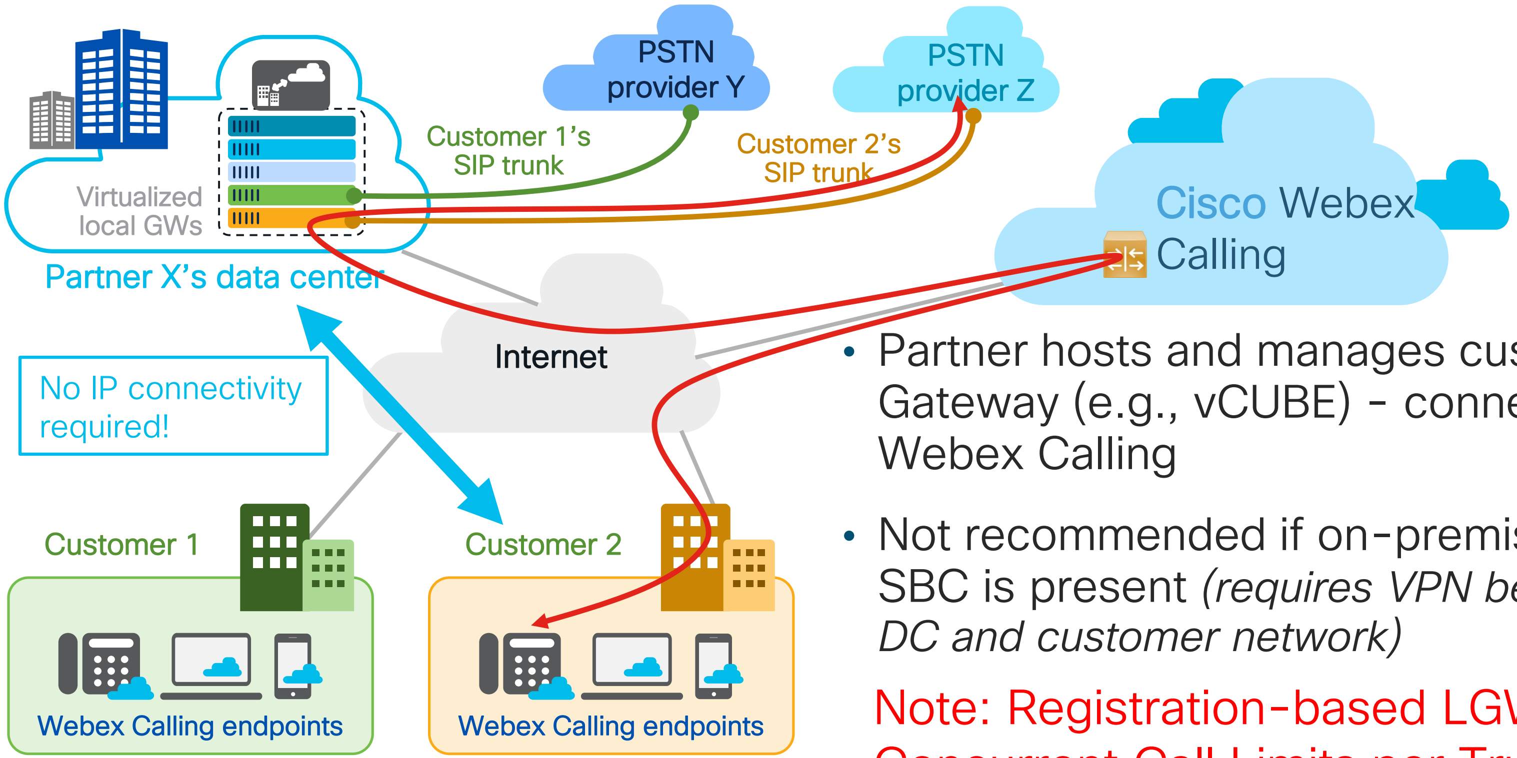

```
voice class uri 300 sip

Inbound dial-peer 300301
 voice class tenant 300
  bind interface Gig 2
   voice class sip-profiles 300
 destination dpg 300
```

LGW2

500 max calls per CUBE



Partner hosted Local Gateway (Multi-tenant)



- Partner hosts and manages customer's Local Gateway (e.g., vCUBE) - connected OTT to Webex Calling
- Not recommended if on-premises PBX or SBC is present *(requires VPN between Partner DC and customer network)*

Note: Registration-based LGW Concurrent Call Limits per Trunk and per TLS connection Apply

Single vCUBE instance with two LGWs – Total 500 calls

IOS-XE 17.8.1a or later

Trunk1 - LGW1=250 calls

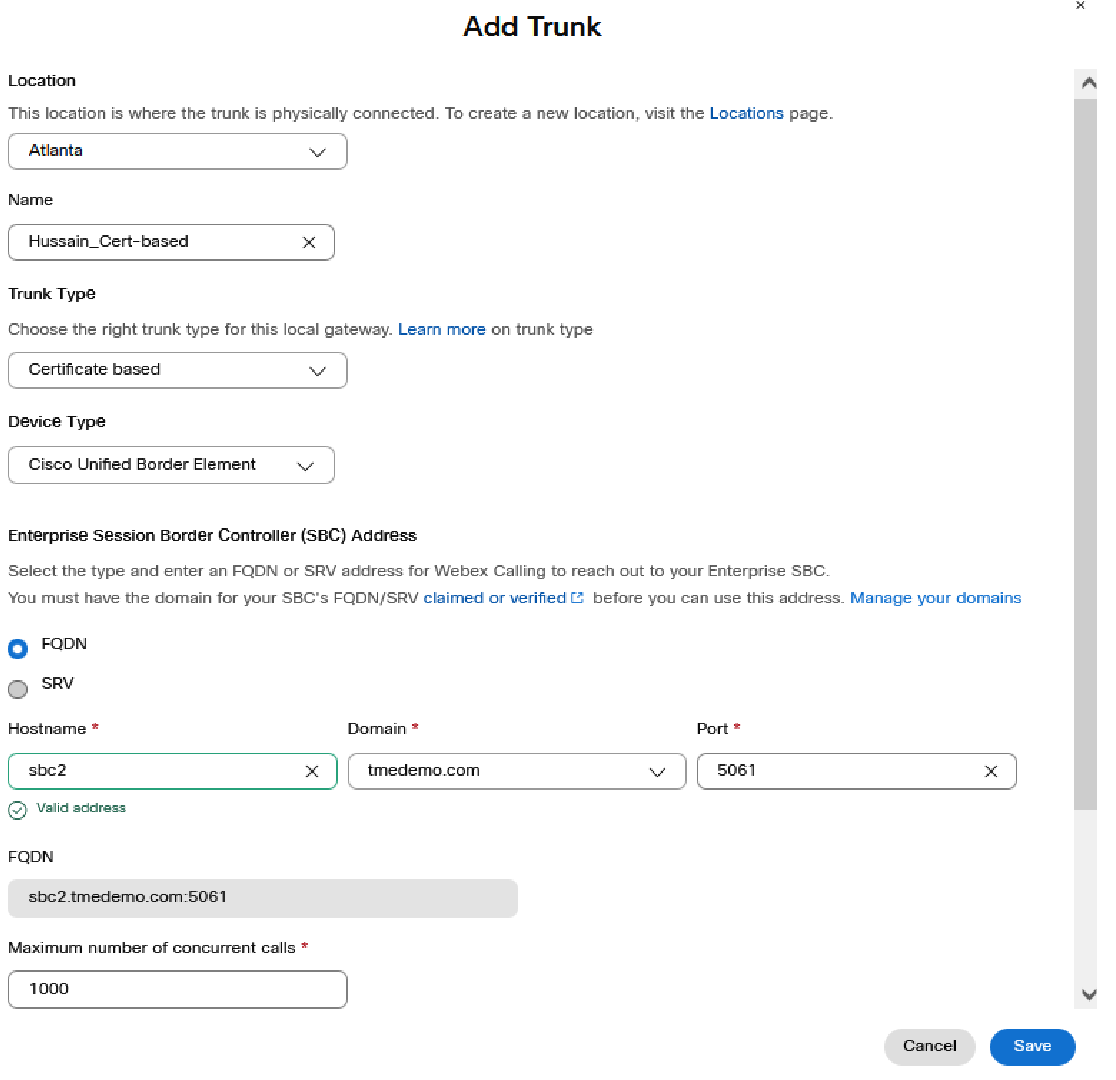
```
dial-peer voice 200201 voip
 description In/Out WxC
 max-conn 250
 destination-pattern BAD.BAD
 session protocol sipv2
 session target sip-server
 destination dpg 100
 incoming uri request 200
 voice-class sip tenant 200

voice class tenant 200
 bind control source-interface GigabitEthernet1
 bind media source-interface GigabitEthernet1
  listen-port secure 5062
  tls-profile 2

voice class tls-profile 2
  trustpoint CUBE-TLS
```

Trunk 2 - LGW2=250 calls

```
dial-peer voice 300301 voip
 description In/Out WxC
 max-conn 250
 destination-pattern BAD.BAD
 session protocol sipv2
 session target sip-server
 destination dpg 300
 incoming uri request 300
 voice-class sip tenant 300

voice class tenant 300
 bind control source-interface GigabitEthernet1
 bind media source-interface GigabitEthernet1
  listen-port secure 5070
  tls-profile 3

voice class tls-profile 3
  trustpoint CUBE-TLS
```

Certificate-based Local Gateway

Add a Certificate-based Trunk to a Location



Adding a Trunk

Add Trunk

Location

This location is where the trunk is physically connected. To create a new location, visit the Locations page.

Atlanta

Name

Hussain_Cert-based

Trunk Type

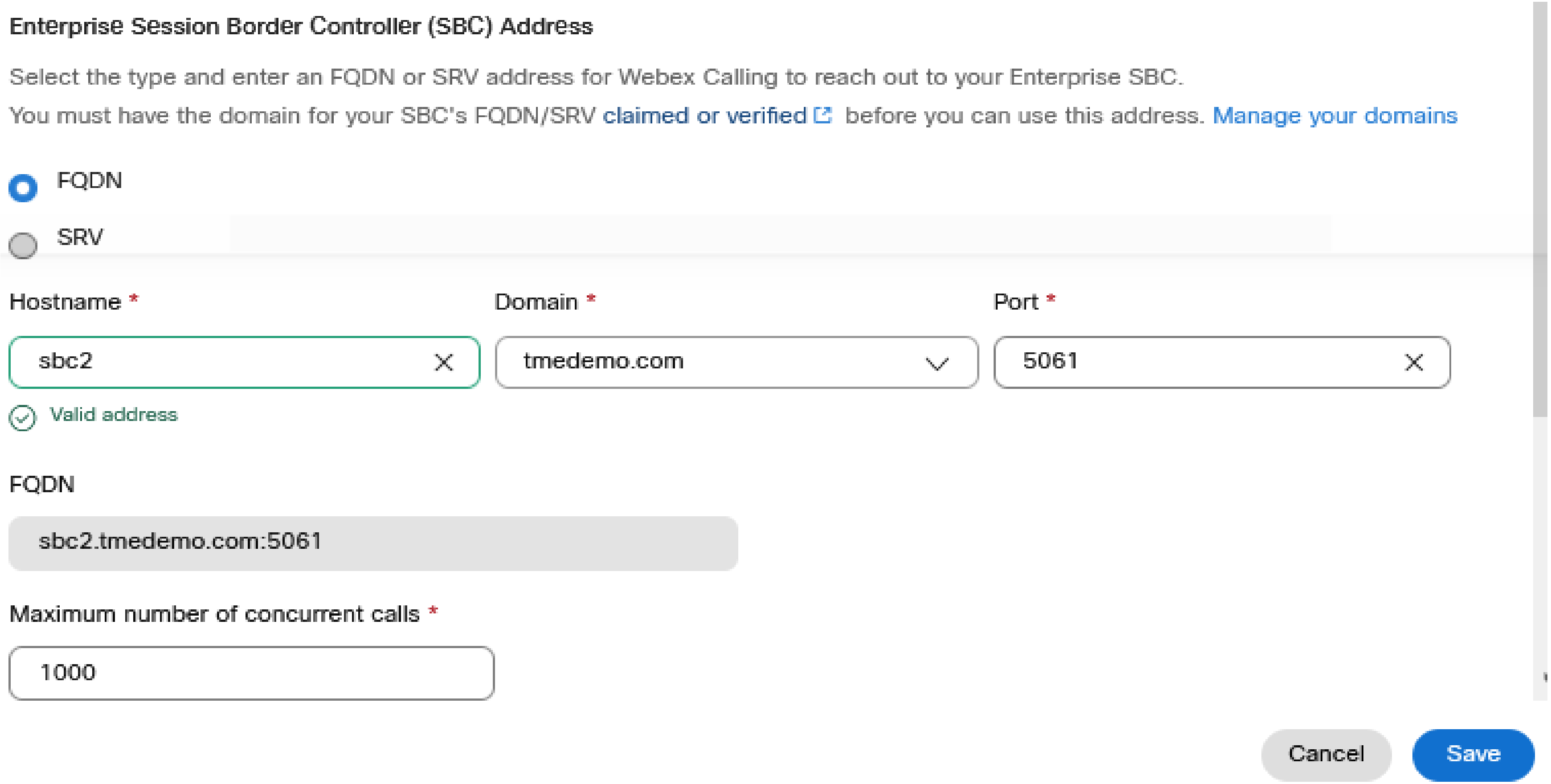
Choose the right trunk type for this local gateway. Learn more on trunk type

Certificate based

Device Type

Cisco Unified Border Element

Define the LGW hostname and select to resolve the LGW through an FQDN or an SRV



Save the Webex Calling Edge Addresses displayed

Add Trunk

Hussain_Cert-based Successfully Created.

Visit Route Group page to add trunk(s) to a route group.
Visit Locations page to configure PSTN connection to individual locations.
Visit Dial Plans page to use this trunk as the routing choice for a dial plan.

Trunk Info

Status

● Unknown

Webex Calling edge proxy address (FQDN)

IOS-XE 17.6+

peering1.us.sipconnect.bcld.webex.com:5062
peering2.us.sipconnect.bcld.webex.com:5062
peering3.us.sipconnect.bcld.webex.com:5062
peering4.us.sipconnect.bcld.webex.com:5062

IOS-XE 17.9+

Webex Calling edge proxy address (SRV)

us01.sipconnect.bcld.webex.com

Webex Calling Trunk - Local Gateway (Certificate-based)

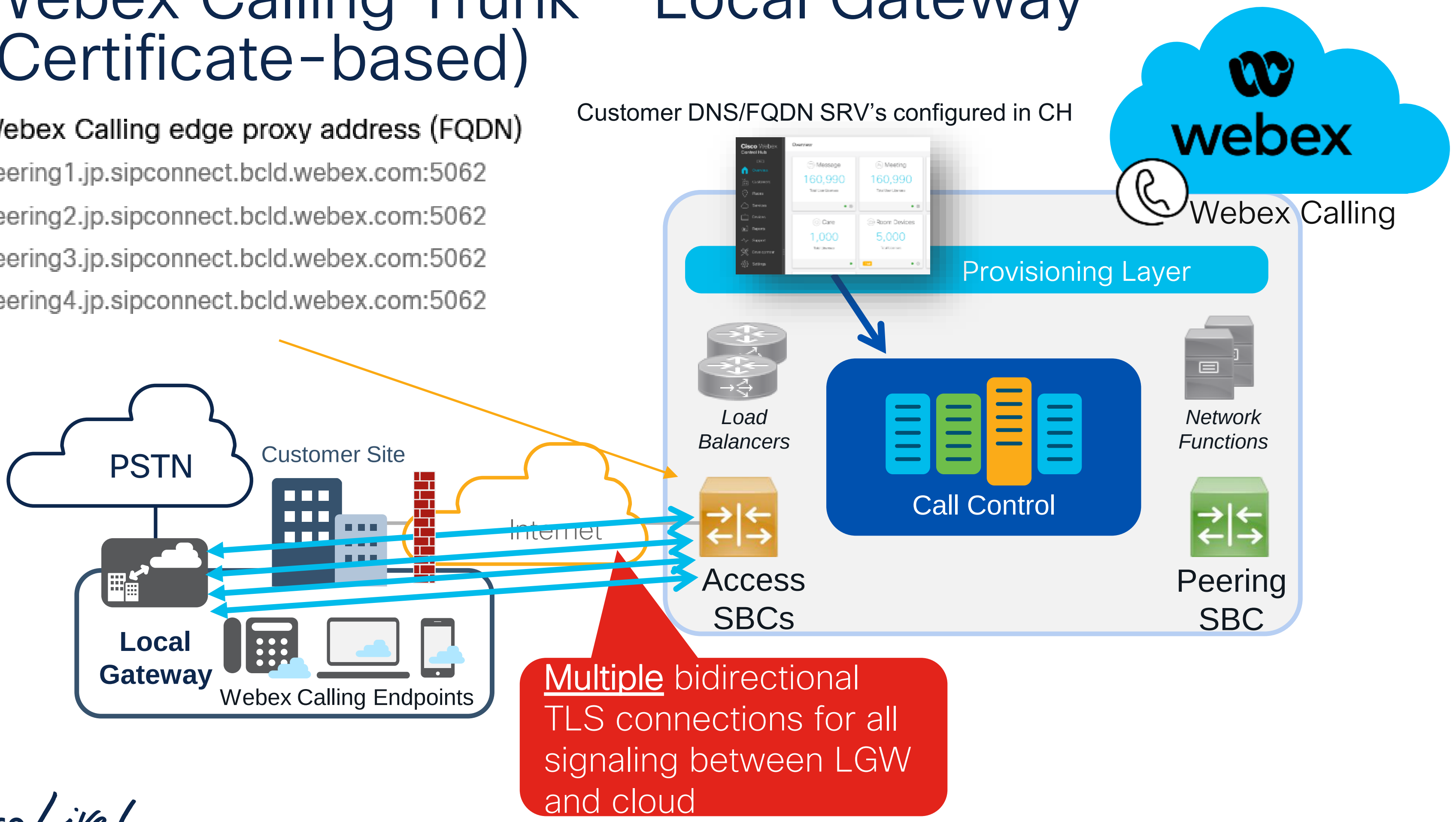
Webex Calling edge proxy address (FQDN)

peering1.jp.sipconnect.bcld.webex.com:5062

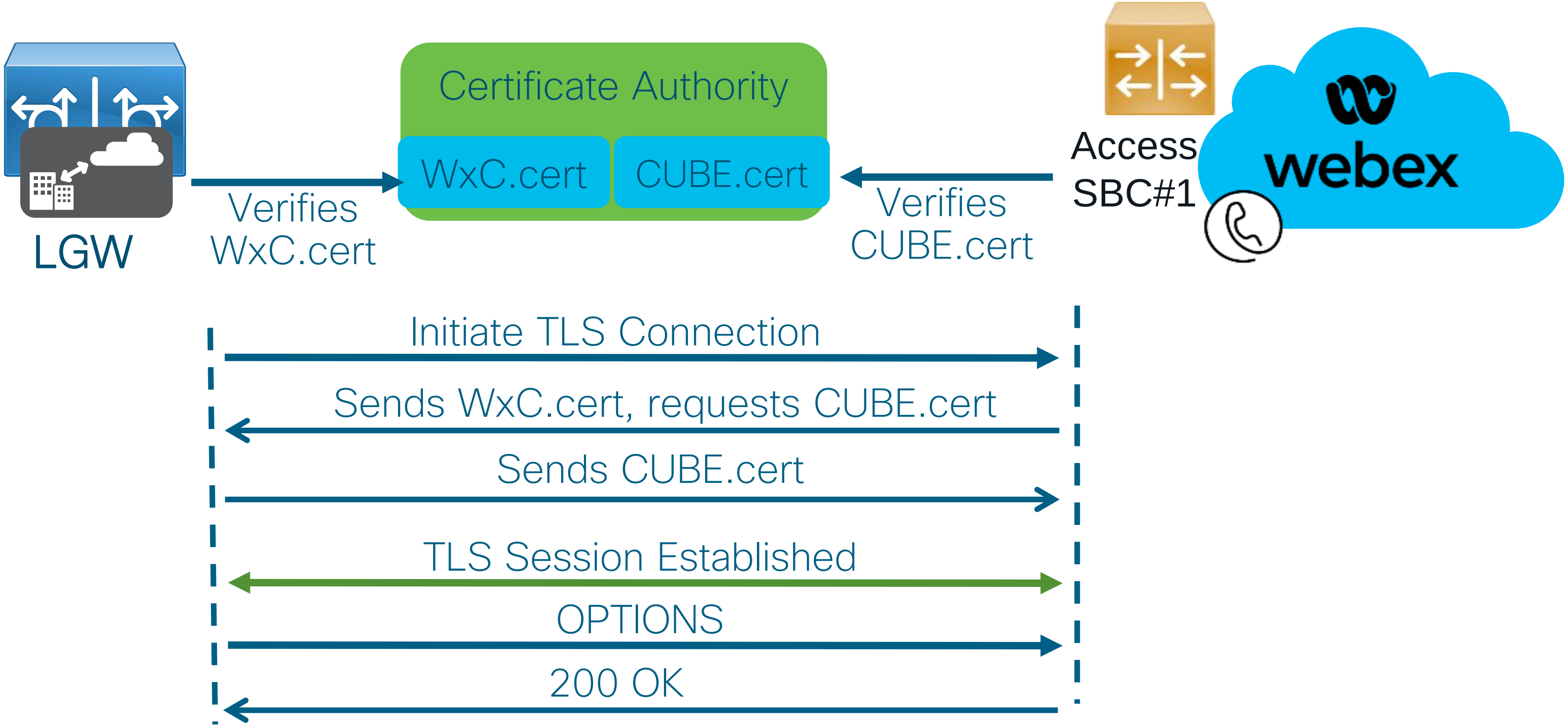
peering2.jp.sipconnect.bcld.webex.com:5062

peering3.jp.sipconnect.bcld.webex.com:5062

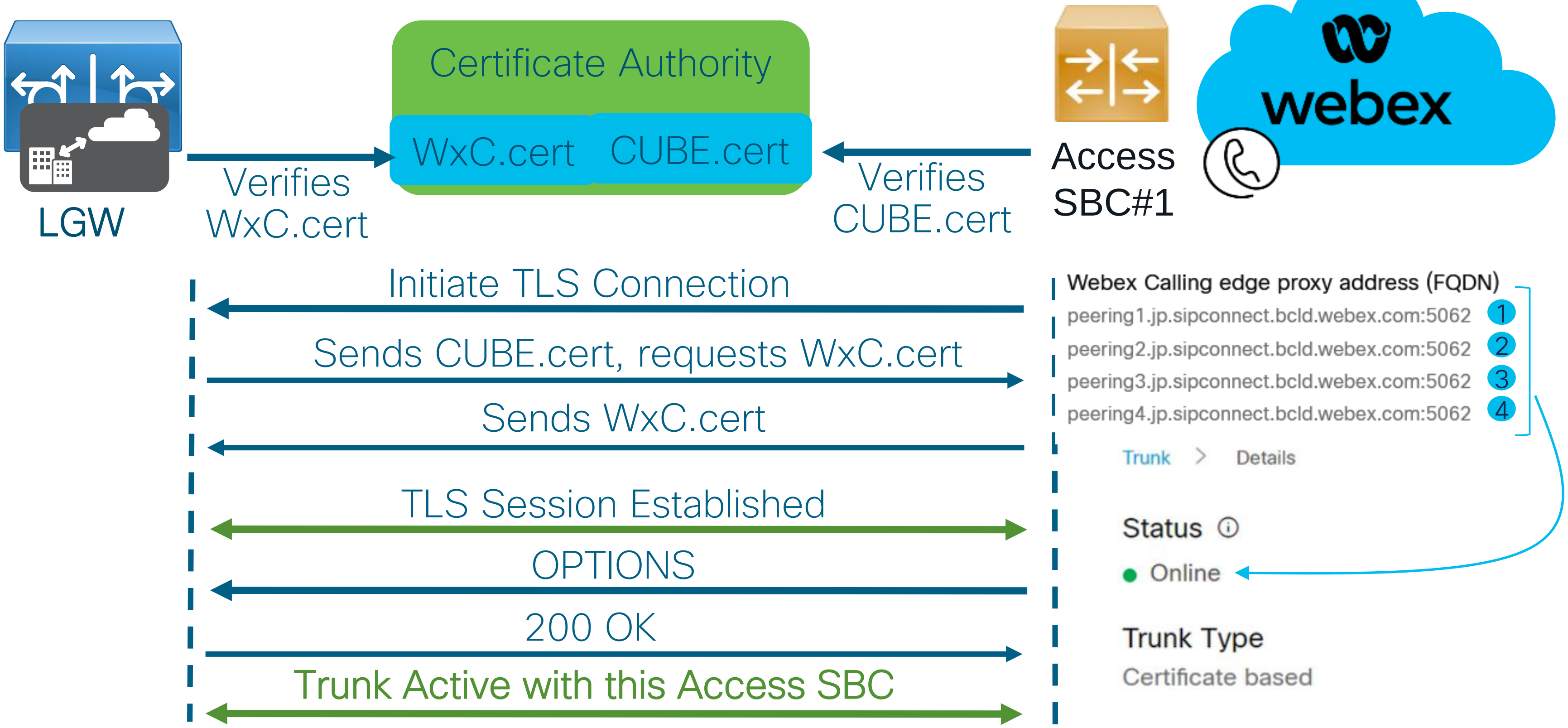
peering4.jp.sipconnect.bcld.webex.com:5062



Certificate-based Local Gateway (Trunk Establishment) – 1st WxC Access SBC - Outbound from LGW to WxC



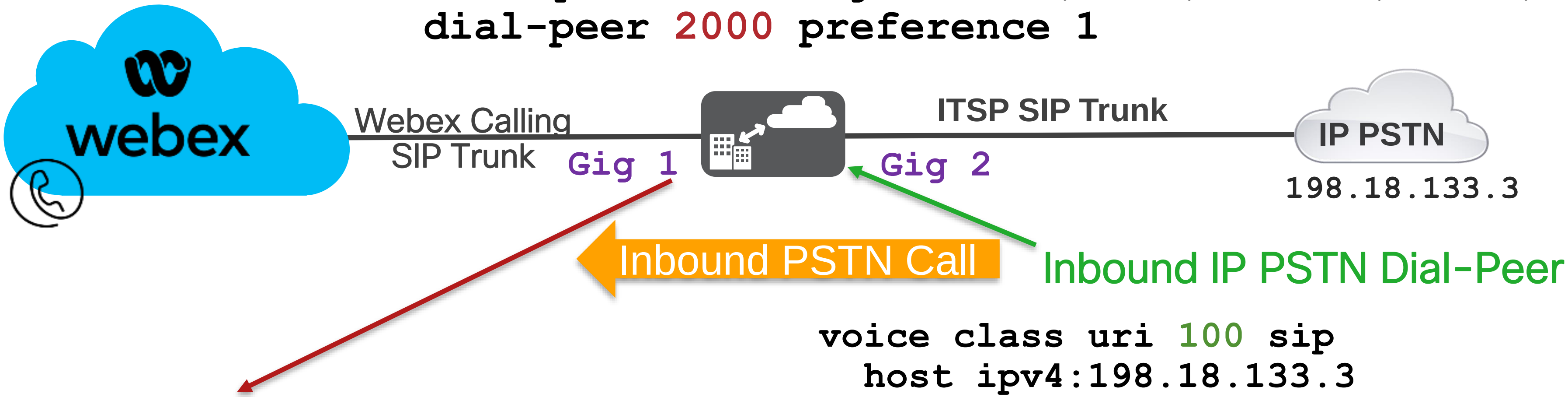
Certificate-based Local Gateway (Trunk Establishment) – 1st WxC Access SBC - Inbound from WxC to LGW



Now repeat the process with the 2nd, the 3rd, and the 4th WxC Access SBC

Inbound LGW PSTN Call

```
voice class dpg 200
 description Incoming IP PSTN(DP100) to WxC(DP2000)
 dial-peer 2000 preference 1
```




```
voice class uri 100 sip
  host ipv4:198.18.133.3

dial-peer voice 100 voip
 description Incoming from IP PSTN
 incoming uri via 100
 destination dpg 200
```

Outbound WxC Dial-Peers

```
dial-peer voice 2000 voip
 description Outbound dial-peer
 ! to Webex Calling Proxy SRV
 session target dns:us01.sipconnect.bcld.webex.com
```

Outbound LGW PSTN Call

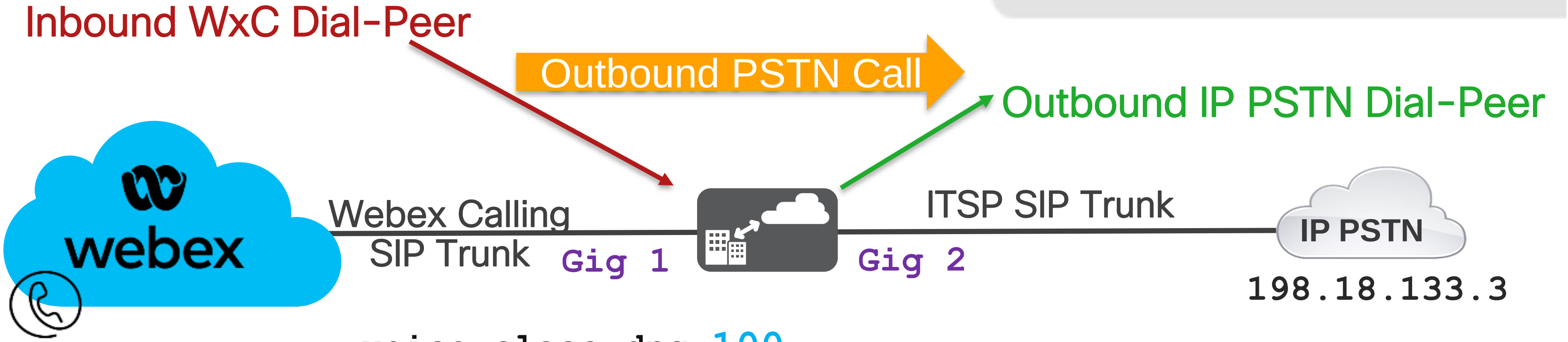
```
voice class uri 200 sip
  pattern sbc2.tmedemo.com
```

```
dial-peer voice 101 voip
 description Outgoing to IP PSTN
 destination-pattern BAD.BAD
 session target ipv4:198.18.133.3
```

```
dial-peer voice 200 voip
 description inbound from Webex Calling
 destination dpg 100
 incoming uri request 200
```

FQDN

sbc2.tmedemo.com:5061




```
voice class dpg 100
 description Incoming WxC(DP200) to IP PSTN(DP101)
 dial-peer 101 preference 1
```

Site Survivability for Webex Calling

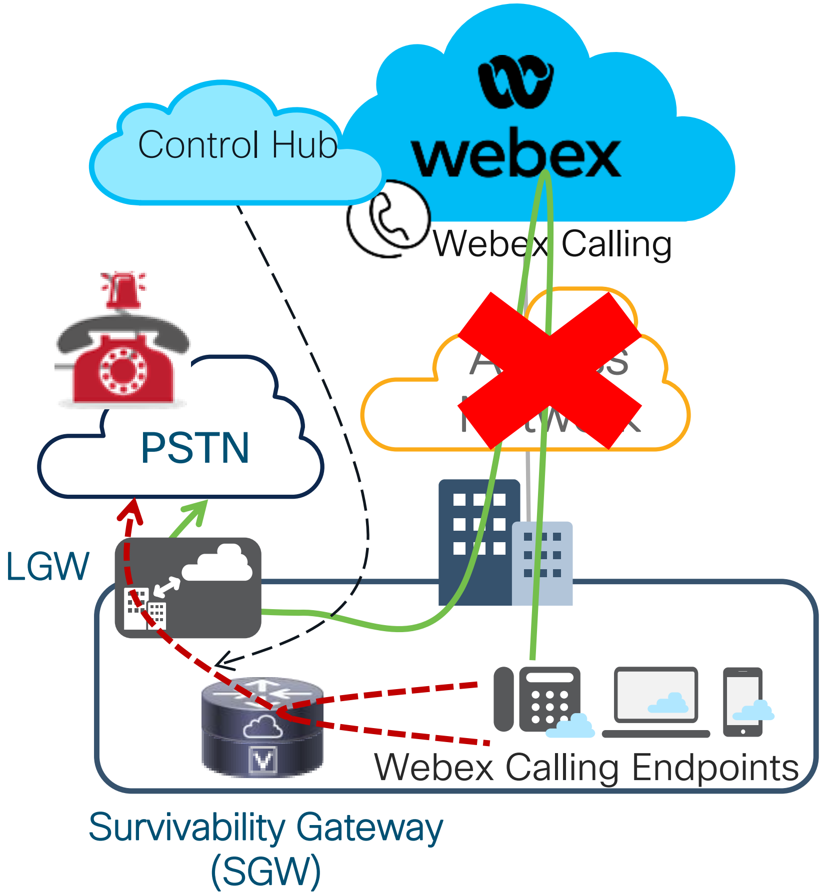
cisco Live!

Site Survivability
Solution Overview

Site Survivability Solution Overview

- A Survivability Gateway (SGW) is installed at a customer site
- The SGW is managed by and gets configuration details from the Control Hub (Webex Cloud)
- In the event of a network outage:
  - Internal/external calls are routed via the SGW
  - Emergency calls are routed via the SGW

Active Mode
Survivability Mode



Endpoint Support

Type	Model	Version
Desk Phones	6821, 6821, 6841, 6851, 6861, 6861 Wi-Fi, 6871, 7811, 7821, 7841, 7861, 8811, 8841, 8851, 8861, 8845, 8865	12.0(1)
Webex App	Windows, Mac	43.2

SGW - Minimum IOS-XE version 17.9.3 or 17.11.1 onwards

IOS-XE 17.10.1 will not be supported

Survivability Gateway (SGW)

Platform Support

Survivability Gateway (SGW)

- Hardware and software requirements:
  - ISR 4321, 4331, 4351, 4431, 4451(IOS XE 17.9.4a / 17.12.2)
  - ISR4461 (IOS XE 17.9.4a /17.12.2)
  - Catalyst 8200/8300 series (IOS XE 17.9.4a/17.12.2)

  - Catalyst 8000v Edge (vCUBE) (IOS XE 17.9.4a / 17.12.2)

IOS-XE Software Release Mapping

CUBE Version	Initial IOS-XE Release for this CUBE version and Release date		Subsequent IOS-XE Release for this CUBE version
14.6	17.9.1a	July 2022	17.9.4a
14.6	17.10.1a	Nov 2022	
14.6	17.11.1a	March 2023	
14.7	17.12.1a	July 2023	17.12.2
14.8	17.13.1a	Nov 2023	
14.9	17.14.1a	March 2024	

Last release for ISR4K except ISR4461

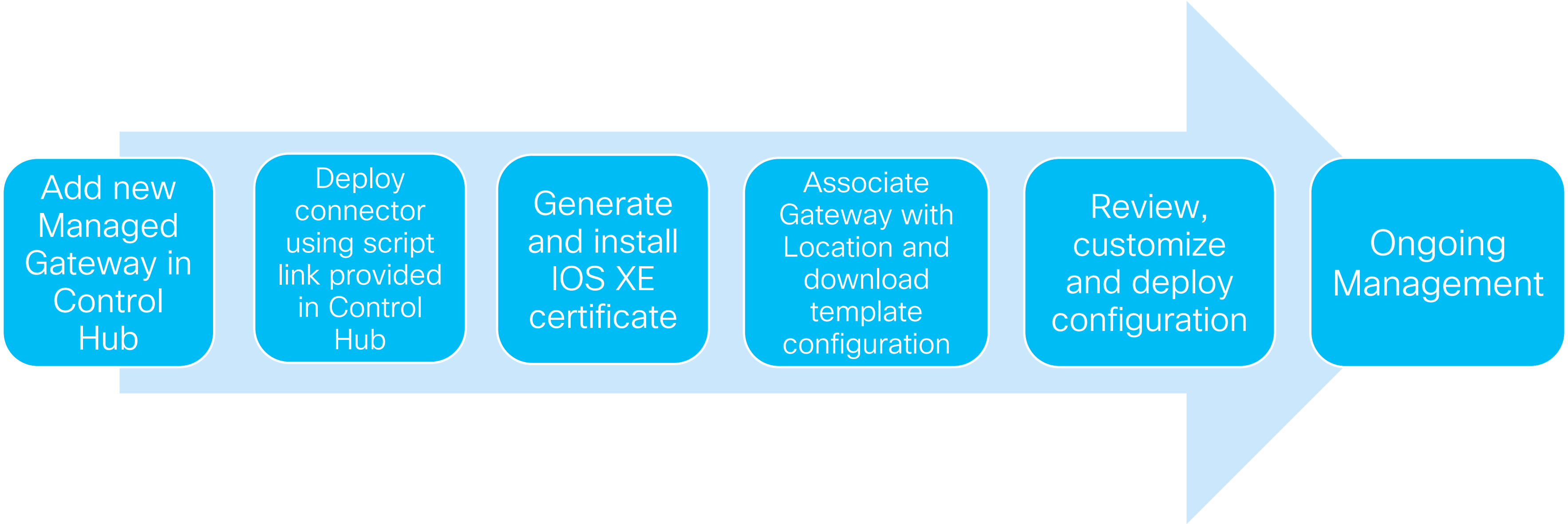
- Upgrade your Webex Calling Survivability Gateways to Cisco IOS-XE 17.12.3 or later releases for enhanced security encryption. If Cisco IOS-XE is not upgraded, SGW will lose connectivity to the Webex Cloud once enhanced security encryption is enabled

Site Survivability
Deployment Workflow

cisco Live!

Site Survivability Configuration

Starting from Managed Gateways context



Assign Survivability Service to the Gateway from within the Control Hub

Managed Gateway now **Online**

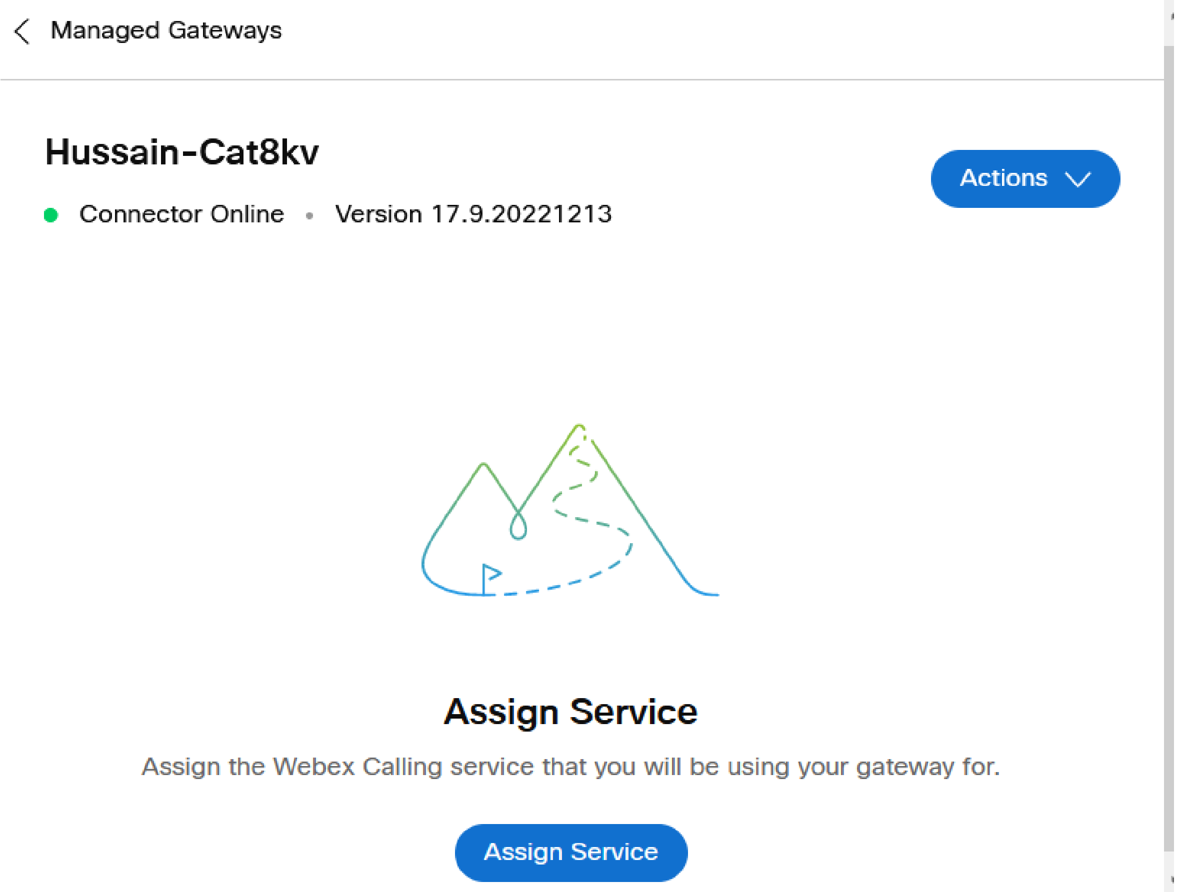
Calling

Numbers | Locations | Call Routing | **Managed Gateways** | Features | PSTN | Service Settings | Client Settings

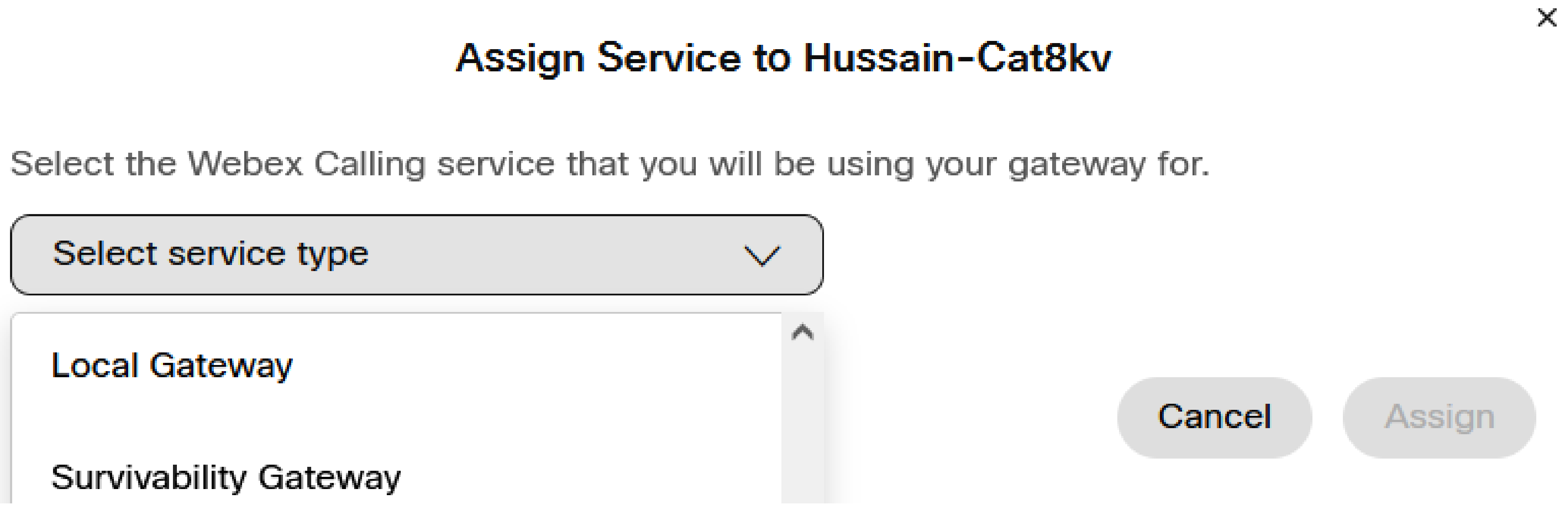
Search | All Gateways | 10 Gateway(s) | Events History | Add Gateway

Gateway Name	Version	Connector Sta...	Service	Assigned to	Actions
Amsterdam SGW	17.9.3	Online	Survivability Gateway	Location: Amsterdam Office	...
Hussain-Cat8kv	17.9.20221...	Online	-	-	...
Lisbon SGW	17.9.3	Online	Survivability Gateway	Location: Lisbon Office	...
London SGW	17.9.3	Offline	Survivability Gateway	Location: London Branch Office	...
Madrid SGW	17.9.3	Online	Survivability Gateway	Location: Madrid Office	...
Munich SGW	17.9.3	Online	Survivability Gateway	Location: Munich Office	...
Paris SGW	17.9.3	Online	Survivability Gateway	Location: Paris Office	...

Assign a Service to the Managed Gateway

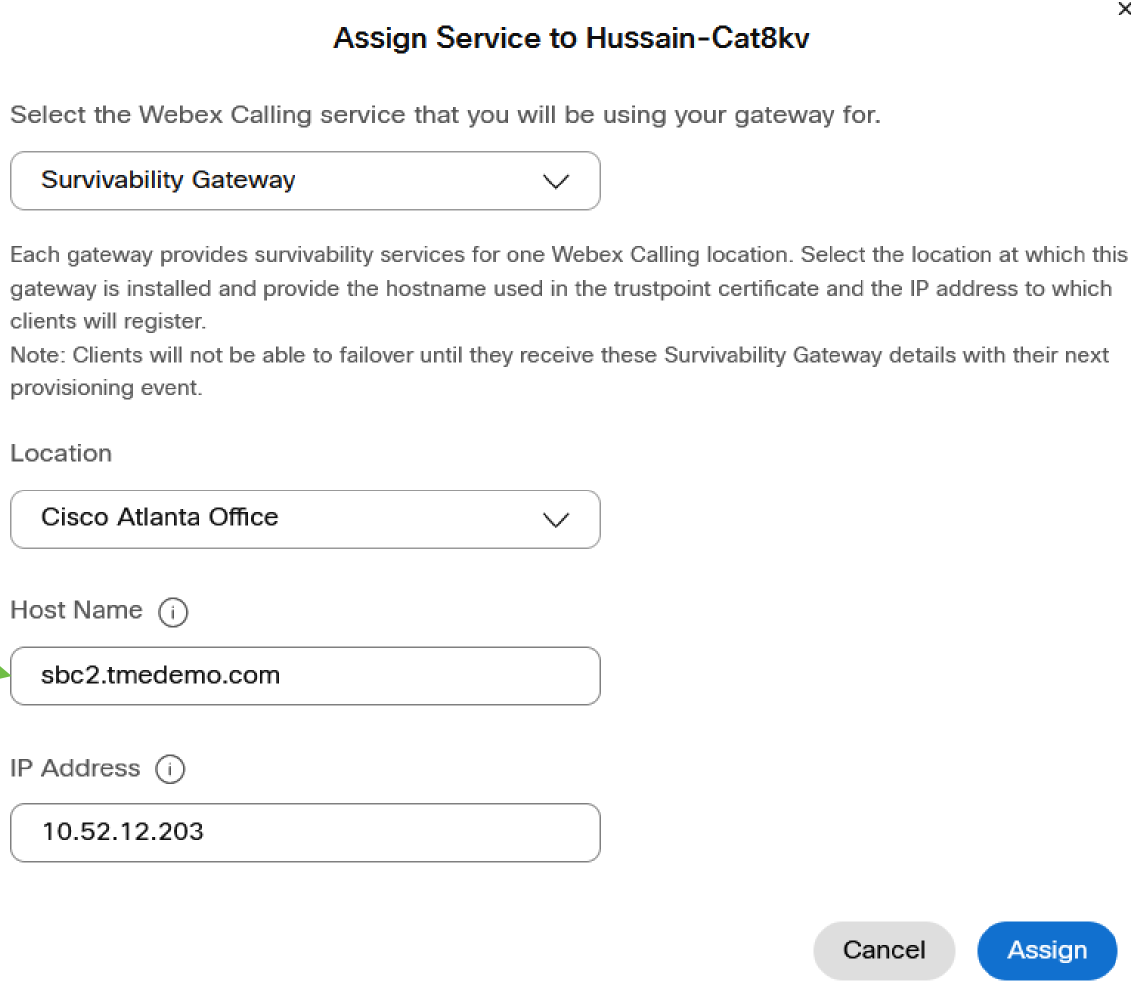


Service Type: LGW or SGW



Select Survivability Gateway as the Service

- Endpoints belonging to this Location will map to this SGW
- Host Name: This would be the hostname / FQDN used in the certificate required for establishing the TLS connection with clients
- IPv4 address of the gateway interface where the endpoints will register



Endpoint Config update

Assign Service to H

Select the Webex Calling service that you will be u

Survivability Gateway

Each gateway provides survivability services for one Webe gateway is installed and provide the hostname used in the clients will register.
Note: Clients will not be able to failover until they receive t provisioning event.

Location

Cisco Atlanta Office

Host Name

sbc2.tmedemo.com

IP Address

10.52.12.203

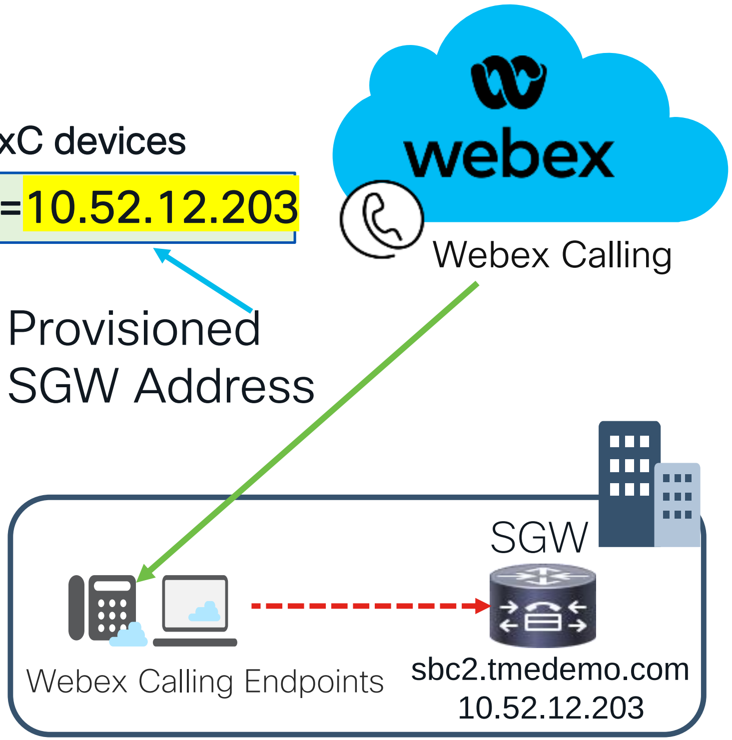
Survivability Proxy Value for WxC devices

sbc2.tmedemo.com:8933:A=10.52.12.203

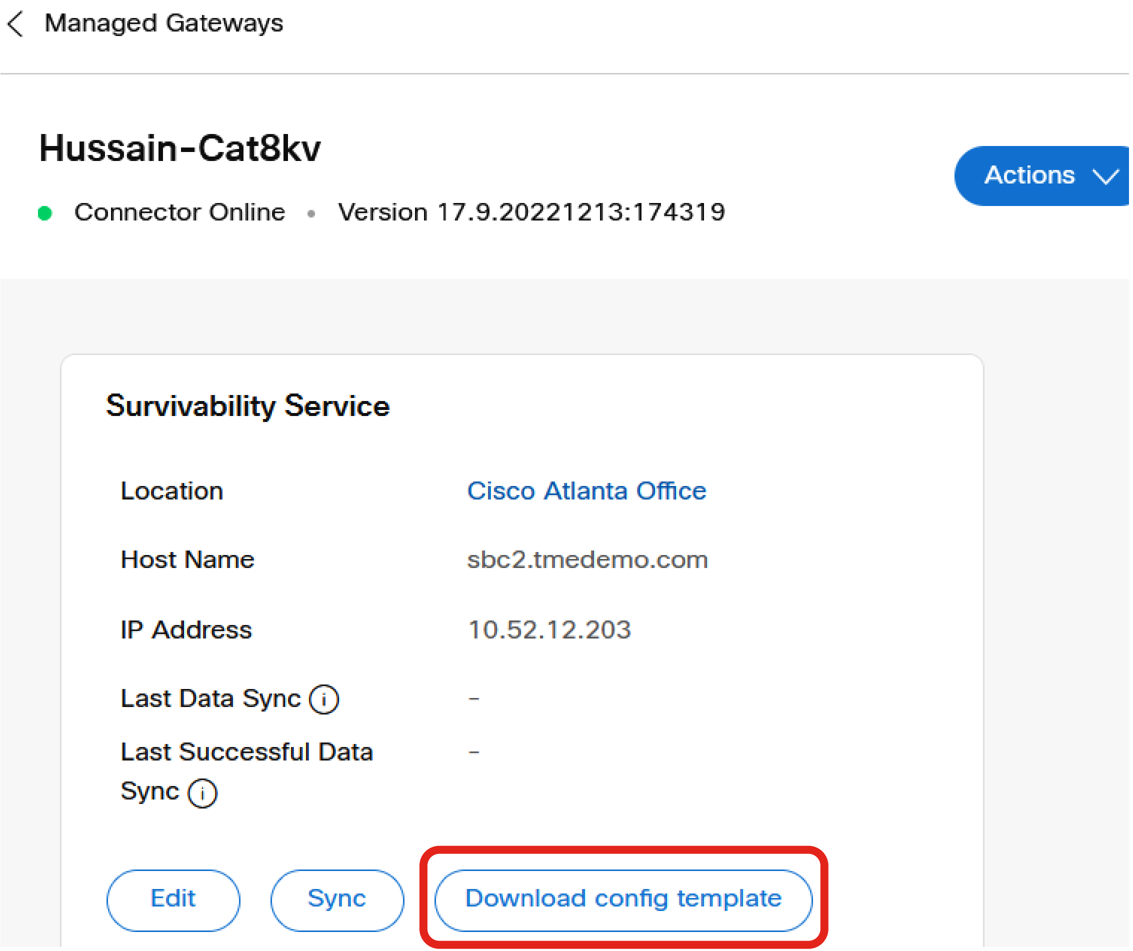
Provisioned SGW hostname (FQDN)

SGW Port (Fixed)

Provisioned SGW Address



Survivability Service Added



SGW Sample Config Template

```
!Global Configurations
voice service voip
 ip address trusted list
   ipv4 <ip_address> <subnet_mask>
  allow-connections sip to sip
 supplementary-service media-renegotiate
 no supplementary-service sip refer
 trace
 sip
  registrar server
!
sip-ua
 transport tcp tls v1.2
 connection-reuse
 crypto signaling default trustpoint webex-
SGW
!
voice register global
 mode webex-sgw
 max-dn 50
 max-pool 50
!
!Create generalized call permissions
!
dial-peer cor call-custom
name local_call
name emergency_call
name international_call
name <custom1>
name <custom2 >
!
dial-peer cor list local_call_permissions
member local_call
member emergency_call
!
```

```
dial-peer cor list
international_call_permissions
member local_call
member emergency_call
member international_call
!
dial-peer cor list
<custom_call_permissions1>
!
dial-peer cor list
<custom_call_permissions2>
!
! Voice Register Pool (Default per location)
voice register pool 100
Id network 0.0.0.0 mask 0.0.0.0
corlist incoming local_call_permissions
dtmf-relay rtp-nte
voice-class codec 1
!
!Voice Register Pools (Per Specific Users)
voice register pool 1
id extension-number 1234
dtmf-relay rtp-nte
voice-class codec 1
corlist incoming
international_call_permissions
!
voice register pool 2
id e164-number +15101234567
dtmf-relay rtp-nte
voice-class codec 1
corlist incoming <custom_call_permissions1>
!
voice register pool 3
Id e164-number +15101234568
dtmf-relay rtp-nte
voice-class codec 1
corlist incoming
<<custom_call_permissions2>
```

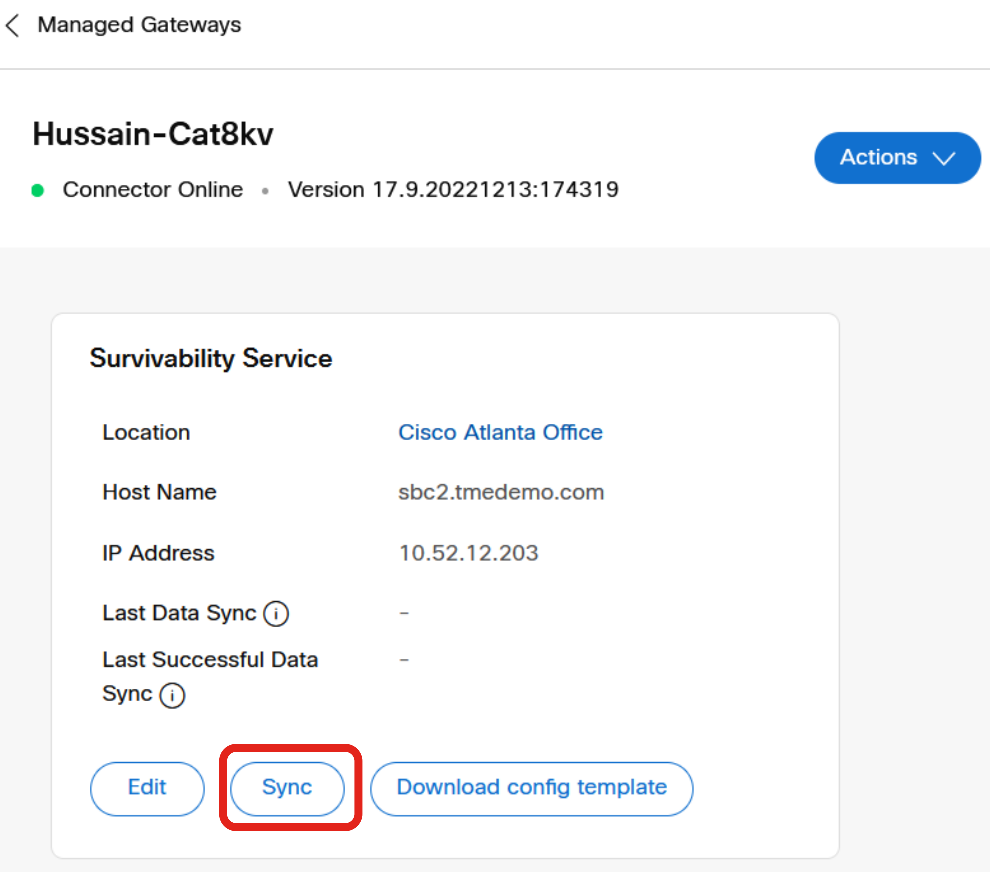
```
! Outbound dial-peers for customized call
! permissions
dial-peer voice 100 voip
description local call
destination e164-pattern-map 500
port 0/1/6:23
cor outgoing call_local
 !
dial-peer voice 300 voip
description international call
destination e164-pattern-map 600
session target ipv4:10.65.125.225
cor outgoing call_international
!
dial-peer voice 300 voip
description custom dial plan
destination e164-pattern-map 700
session target ipv4:10.65.125.225
cor outgoing call_custom1
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g711alaw
 codec preference 3 opus
!
dial-peer cor list call_local
member local_call
!
dial-peer cor list call_international
member international_call
!
dial-peer cor list call_emergency
member emergency_call
!
dial-peer cor list call_custom1
nember <custom1>
!
```

```
! Emergency Locations
voice emergency response location 1
      elin 1 14085550100
       subnet 1 192.168.1.0 255.255.255.0
!
voice emergency response location 2
     elin 1 1408555011
     subnet 1 192.168.2.0 255.255.255.0
!
! Emergency Response Zone
voice emergency response zone 1
    location 1
    location 2
!
dial-peer voice 300 pots
 description Outbound dial-peer for E911 call
 emergency response zone 1
 destination e164-pattern-map 300
 cor outgoing call_emergency
!
dial-peer voice 301 pots
   description Inbound dial-peer for E911 call
   emergency response callback
   incoming called e164-pattern-map 301
   direct-inward-dial
!
! Emergency Dial plans
voice class e164-pattern-map 300
      e164 911
      e164 988
!
voice class e164-pattern-map 301
     e164 1408555011
     e164 1408555010
!
```

cisco Live!

SGW Sync Operation

- Sync option manually triggers a data download.
  - Start / finish can be verified in the gateway log
  - Status card can take up to 10 mins to update following a manual Sync.
  - Data is downloaded automatically every night by the gateway.



Co-locating Survivability Gateway (SGW) and Local Gateway (LGW)

Destination Dial-peer Group Limitation

```
voice class dpg 10000
  description Voice Class DPG for SJ
  dial-peer 1002 preference 1
  dial-peer 1003
!
dial-peer voice 100 voip
 description Inbound DP
 incoming called-number 1341
 destination dpg 10000
```

```
dial-peer voice 786 voip
 destination-pattern 1341
 session protocol sipv2
 session target ipv4:10.1.1.1
!
dial-peer voice 1002 voip
 destination-pattern 3333
 session protocol sipv2
 session target ipv4:10.1.1.2
!
dial-peer voice 1003 voip
 destination-pattern 4444
 session protocol sipv2
 session target ipv4:10.1.1.3
```

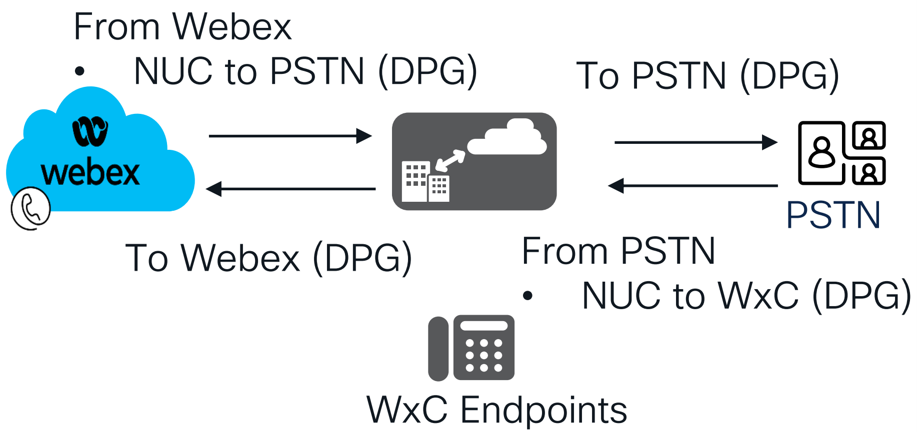
3. Outbound DP is selected

1. Incoming Dial-peer is first matched

2. Now the DPG associated with the INBOUND DP is selected

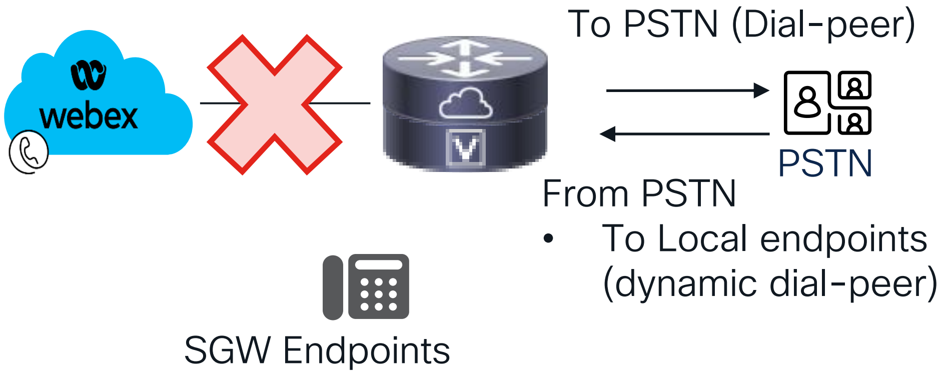
cisco Live!

Call Routing Overview – Existing LGW and SGW Operation



Standalone Local Gateway in Cloud mode

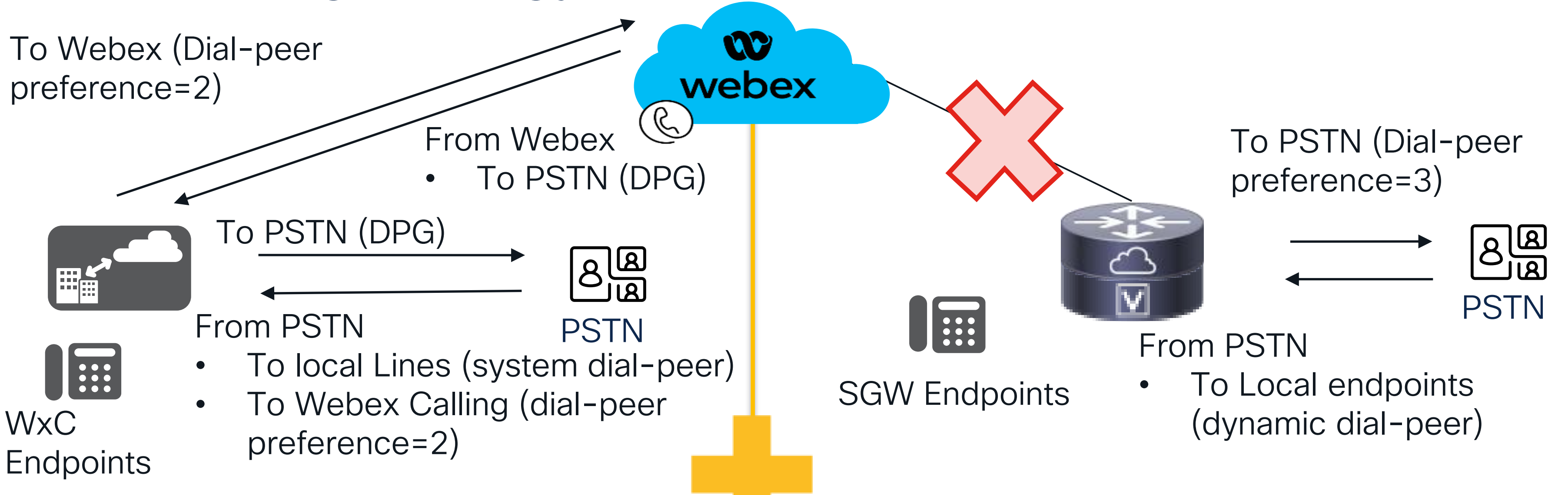
- Nailed up connections (NUC) using Dial peer groups
- Simplistic approach, does not require admins to have knowledge of Webex Calling or PBX dial plans or configure these patterns on the LGW
- Challenge: No way to exit DPG and match system (dynamic) dial peers when Lines register locally on the router



Site Survivability Gateway during Cloud/WAN outage

- Local extension calling – Webex Calling SGW Phones use system (dynamic) dial-peers (no config needed)
- Outbound line to PSTN use Dial-peer based routing
- Inbound PSTN routes to local lines first. Lines (dynamic dial-peers) always have precedence

Call Routing Strategy for a Co-located LGW/SGW Operation



LGW operation (Cloud-connected)

- Transition from dial-peer groups (NUC) to dial-peers with preferences on PSTN ingress leg
- Allows search of local registered endpoints (not accessible from the DPG)
- Routing guidance provided for greenfield deployments (without premise PBX)

Site Survivability operation (Cloud/WAN outage)

- Local extension calling use dynamic dial-peers (no additional config needed)
- Endpoint to PSTN use dial-peers with preference=3
- Incoming PSTN would match Local endpoints (preference 0) first

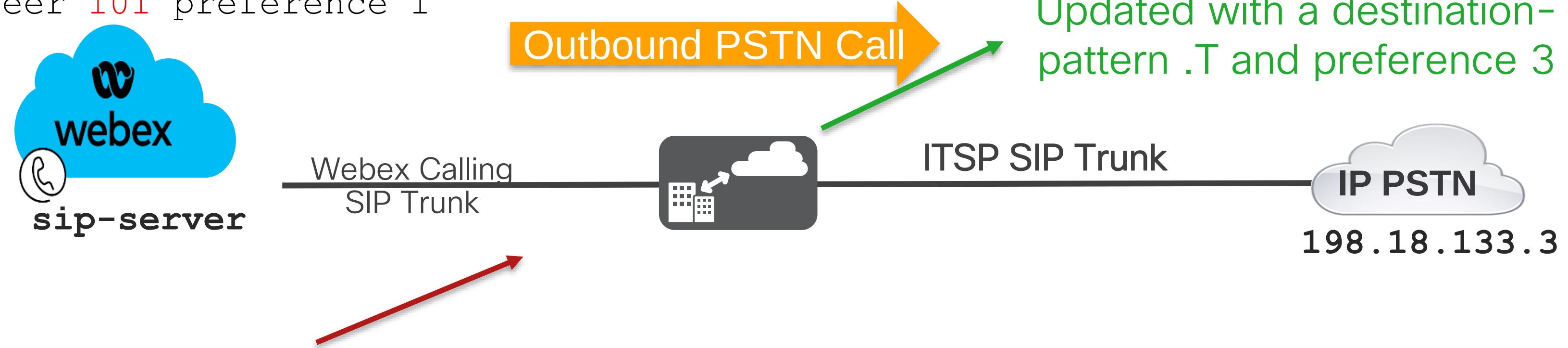
LGW - WxC to PSTN

```
voice class uri 200 sip
  pattern dtg=hussain2572_lgu
```

```
dial-peer voice 101 voip
 description Outgoing to IP PSTN
 destination-pattern .T
 preference 3
 session target ipv4:198.18.133.3
```

```
voice class dpg 100
 description Incoming WxC(DP200201) to IP PSTN(DP101)
 dial-peer 101 preference 1
```

Outbound IP PSTN Dial-Peer Updated with a destination-pattern .T and preference 3




```
dial-peer voice 200201 voip
  description Inbound from Webex Calling
  max-conn 250
  destination dpg 100
  incoming uri request 200
  voice-class sip tenant 200
  srtp
```

WxC Dial-Peer Inbound – No Changes

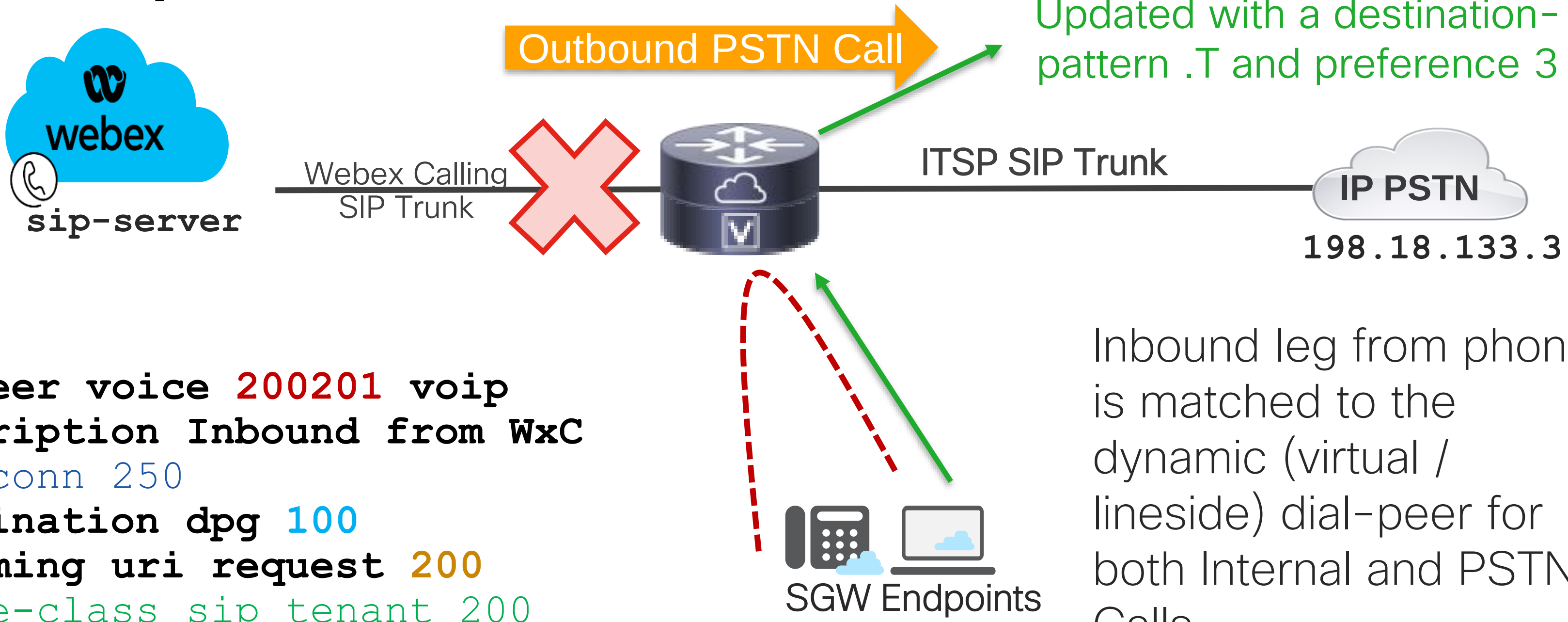
SGW to PSTN Dial-peer

```
voice class uri 200 sip
  pattern dtg=hussain2572_lgu
```

```
voice class dpg 100
 description Incoming WxC(DP200201) to IP PSTN(DP101)
 dial-peer 101 preference 1
```

```
dial-peer voice 101 voip
 description Outgoing DP to IP PSTN
 destination-pattern .T
 preference 3
 session target ipv4:198.18.133.3
```

Outbound IP PSTN Dial-Peer Updated with a destination-pattern .T and preference 3




```
dial-peer voice 200201 voip
  description Inbound from WxC
  max-conn 250
  destination dpg 100
  incoming uri request 200
  voice-class sip tenant 200
```

Inbound leg from phone is matched to the dynamic (virtual / lineside) dial-peer for both Internal and PSTN Calls

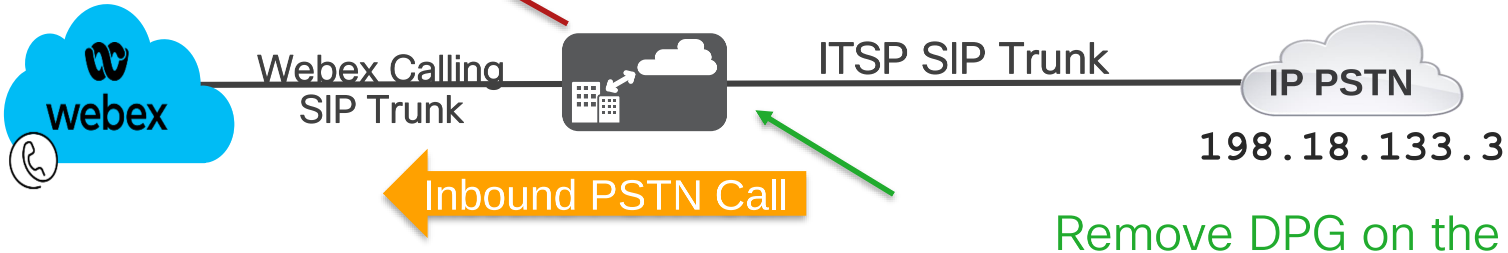
LGW - Inbound from PSTN to WxC

```
dial-peer voice 200201 voip
  description Inbound/Outbound WxC
  destination dpg 100
  incoming uri request 200
  voice-class sip tenant 200
  destination-pattern .T
  preference 2
```

Webex Calling facing dial-peer

- Update destination-pattern from BAD.BAD to .T and add preference 2

```
voice class dpg 200
 description Incoming IP PSTN(DP100) to WxC(DP200201)
 dial-peer 200201 preference 1
```



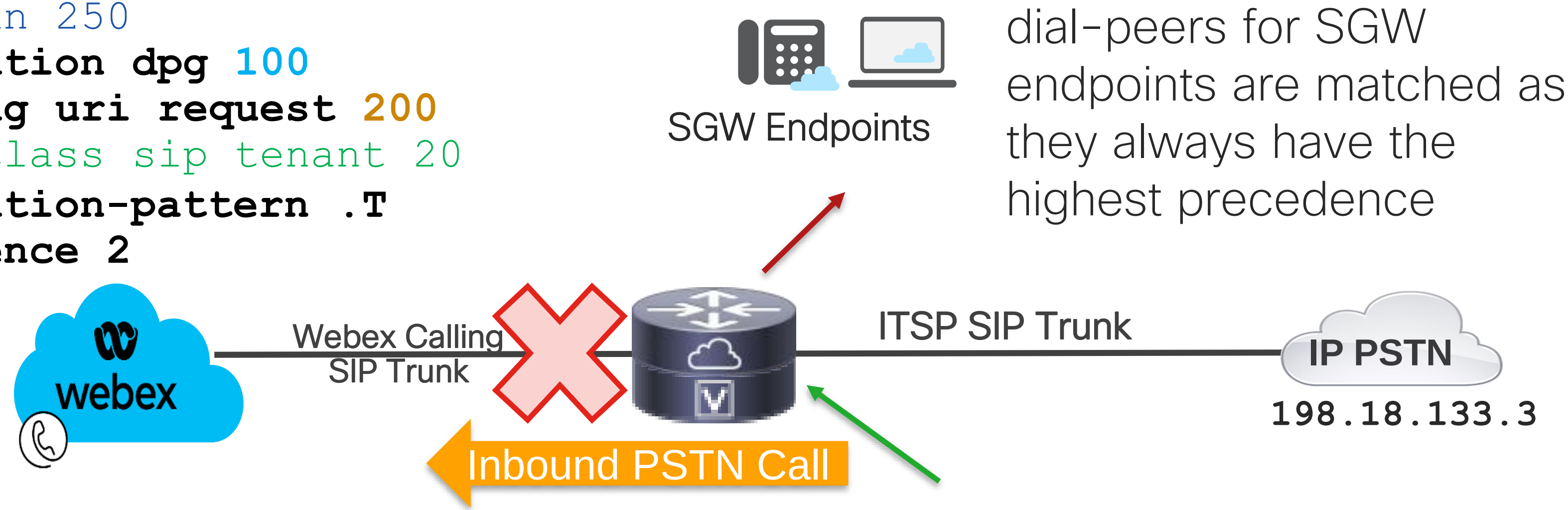
Remove DPG on the inbound PSTN dial-peer

```
voice class uri 100 sip
  host ipv4:198.18.133.3

dial-peer voice 100 voip
  description Incoming dial-peer from IP PSTN
  incoming uri via 100
  destination dpg 200
```

SGW - Inbound from PSTN to Endpoint

```
dial-peer voice 200201 voip
  description Inbound/Outbound WxC
  max-conn 250
  destination dpg 100
  incoming uri request 200
  voice-class sip tenant 20
  destination-pattern .T
  preference 2
```

dynamic (virtual / lineside) dial-peers for SGW endpoints are matched as they always have the highest precedence

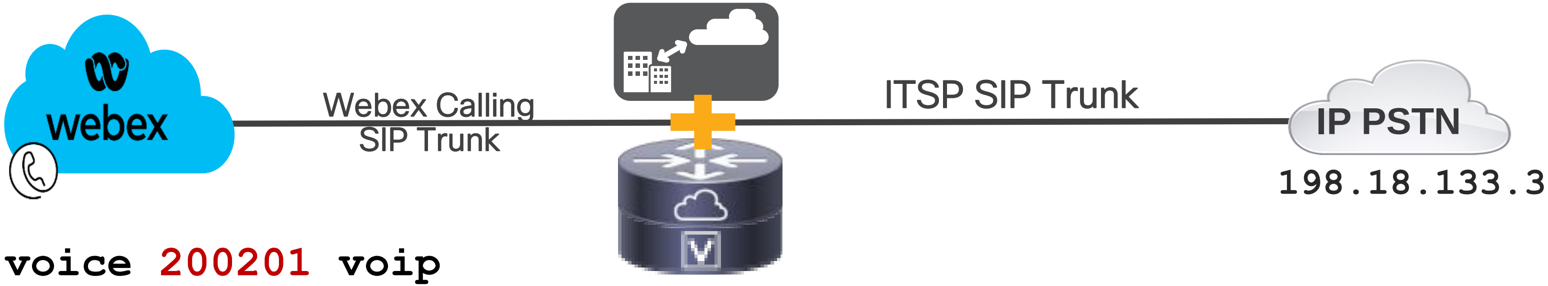



```
voice class uri 100 sip
  host ipv4:198.18.133.3

dial-peer voice 100 voip
  description Incoming dial-peer from IP PSTN
  incoming uri via 100
```

LGW - Inbound from PSTN to WxC

```
voice class uri 200 sip
  pattern dtg=hussain2572_lgu

voice class dpg 100
 description Incoming WxC(DP200201) to IP PSTN(DP101)
 dial-peer 101 preference 1
```

```
dial-peer voice 101 voip
 description Outgoing to IP PSTN
 destination-pattern .T
 preference 3
 session target ipv4:198.18.133.3
```




```
dial-peer voice 200201 voip
  description Inbound/Outbound WxC
  max-conn 250
  destination dpg 100
  destination-pattern .T
  preference 2
  incoming uri request 200
  voice-class sip tenant 200
```

```
voice class uri 100 sip
  host ipv4:198.18.133.3

dial-peer voice 100 voip
 description Incoming from IP PSTN
 incoming uri via 100
```

LGW/SGW Co-location considerations

- IOS-XE 17.12.1a or later is required
- CUBE High Availability is not supported for LGW
- Registration-based LGW Config validation is not supported
- In Control Hub, the gateway must be provisioned as a Survivability Gateway service.
    - If the customer has provisioned the gateway as a Local Gateway, they need to unassign, and then reassign the service as Survivability Gateway.
- Colocation is specific to Cisco IOS-XE Gateway. Customers using third-party Local Gateway must deploy Survivability Gateway separately.
- Colocation for partner-deployed Local Gateway shared across multiple customers is not applicable.

References

CUBE Resources

- CUBE Configuration Guide Through IOS-XE 17.5
- CUBE Configuration Guide – IOS-XE 17.6 Onwards
- vCUBE support on Azure
- vCUBE on AWS
- CUBE Interop Portal including Direct Routing Application Note
- CUBE Box – https://cisco.box.com/CUBE-Enterprise (request access via email)
- Webex Calling – https://cisco.box.com/WebexCalling (request access via email)
  - Email ASK-CUBE@EXTERNAL.CISCO.COM with your Box.com account id (email) for access to the Box.com links above. Free Box.com account is fine as well

LGW Resources

For more information take a look at the following resources:

- What's new in Webex Calling: https://help.webex.com/en-us/article/rdmb0/What's-new-in-Webex-Calling
- Trunk configuration guide: Webex Calling Trunks
- Configure Local Gateway on Cisco IOS XE for Webex Calling https://help.webex.com/en-us/article/jr1i3r/Configure-Local-Gateway-on-Cisco-IOS-XE-for-Webex-Calling
- https://help.webex.com/en-us/article/n0xb944/Configure-Trunks,-Route-Groups,-and-Dial-Plans-for-Webex-Calling

SGW and LGW Resources

For more information take a look at the following resources:

- Webex Calling Trunks
- Local Gateway Configuration Guide
- Enroll Cisco IOS Managed Gateways to Webex Cloud
- Assign Services to Managed Gateways
- Site Survivability for Webex Calling
- Colocation of LGW and SGW

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: ask-cube@external.cisco.com or the space for this session

The bridge to possible

Thank you

#CiscoLive