

Enabling Cloud and Premise Deployments with CUBE

cisco Live !

Huss**A**in Ali, CCIE#38068

Technical Marketing Engineer

<https://www.linkedin.com/in/hussaincube>

Omer Ilyas, CCIE#42339

Technical Marketing Engineer

<https://www.linkedin.com/in/omerilyas4ccie>

Cisco Webex App

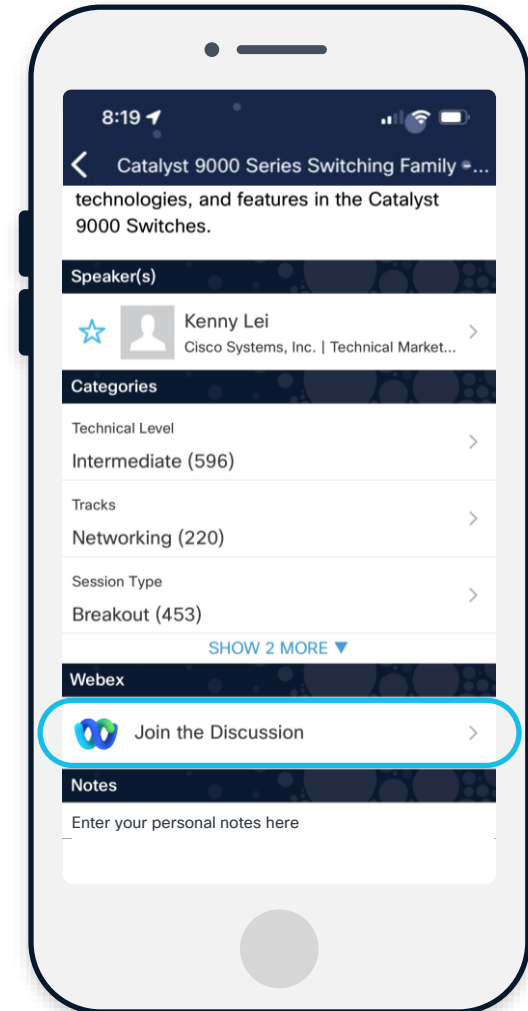
Questions?

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 13, 2025.

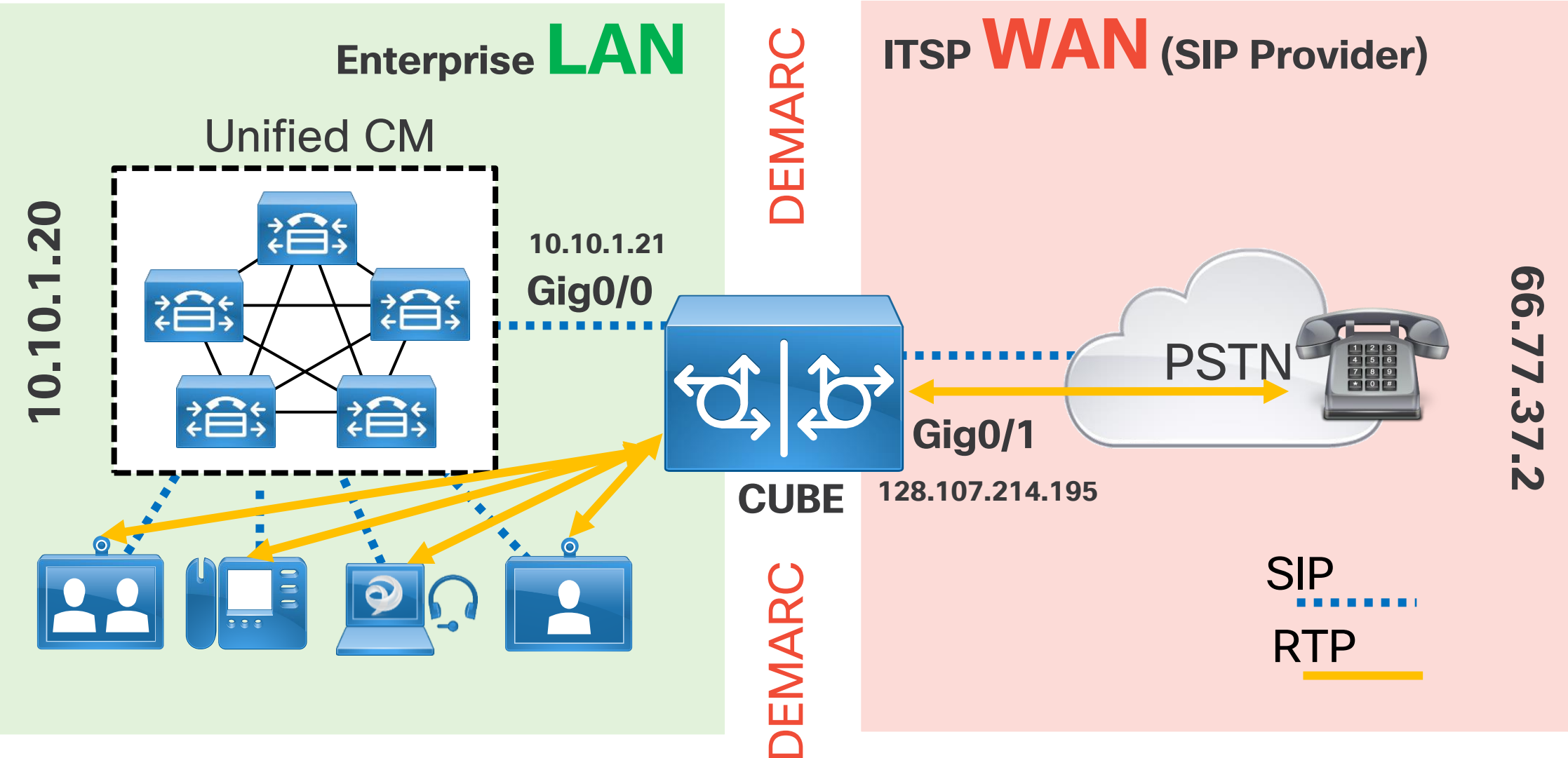


Agenda

- CUBE Recap
 - CUBE Configuration Steps
- Version 14 Updates
- Local Gateway (LGW) for Webex Calling
- Survivability Gateway (SGW) for Webex Calling
- CUBE with ThousandEyes
- References

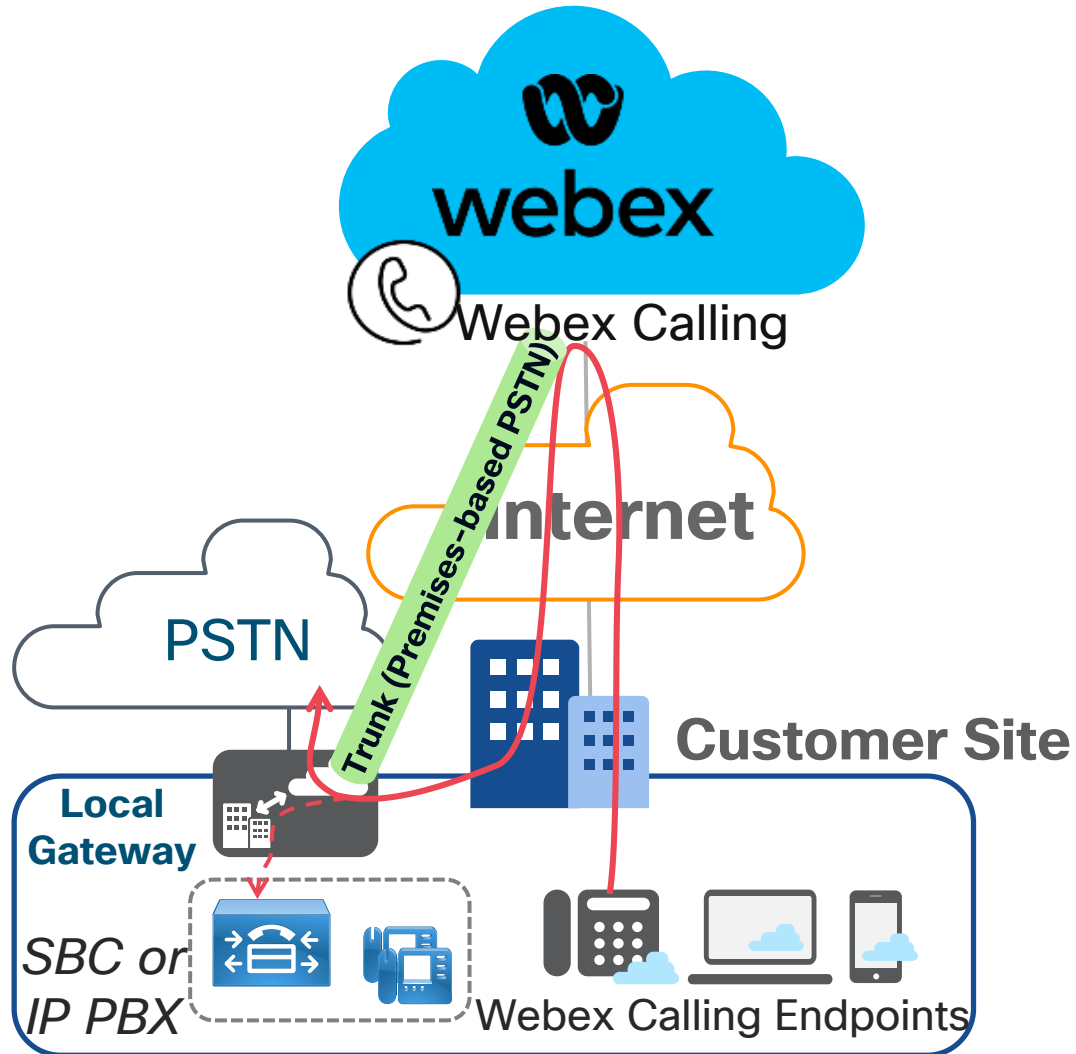
CUBE Recap

CUBE as an SBC for an on-premises Collaboration Deployment



Webex Calling Trunk - Local Gateway

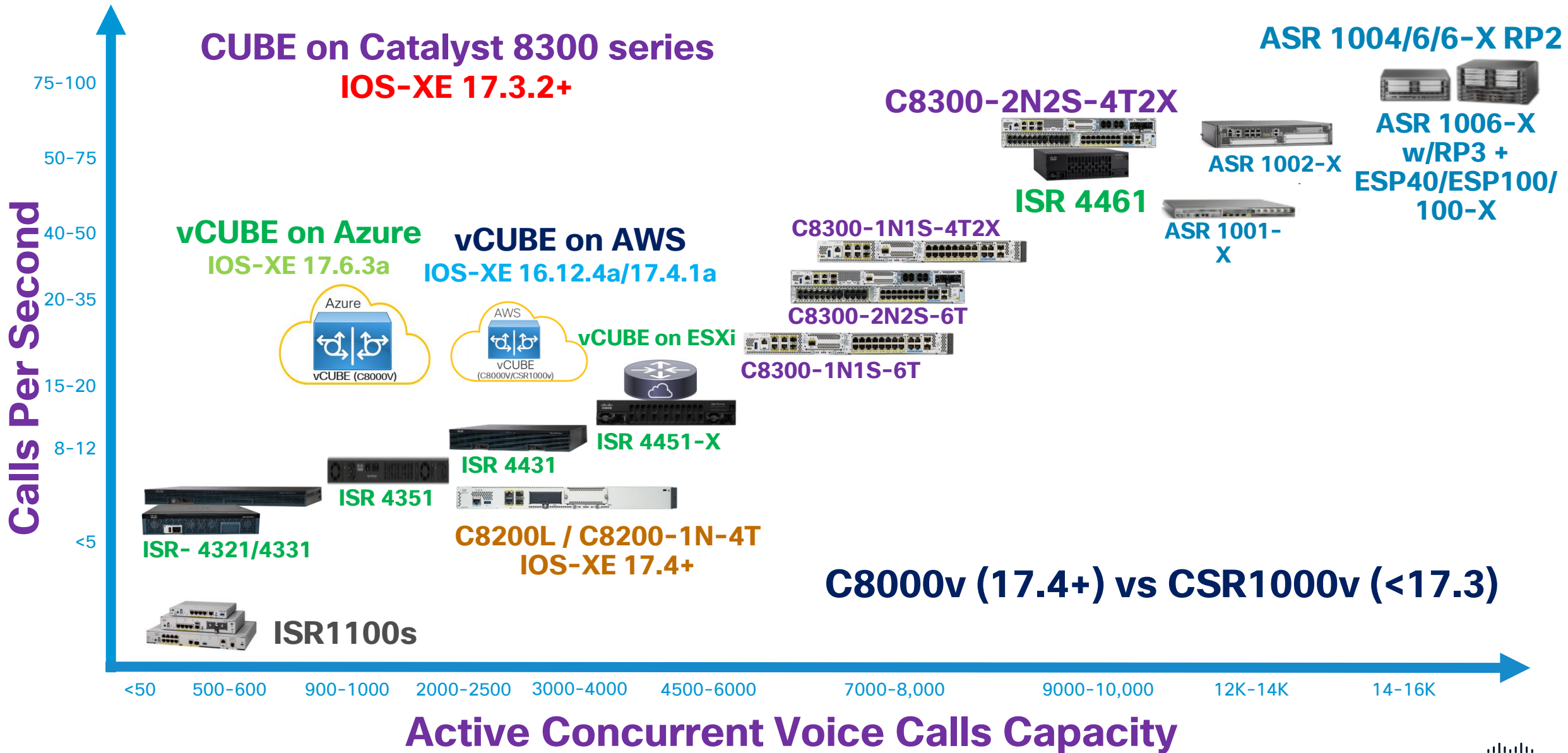
(Premises-based PSTN) Deployment



- 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

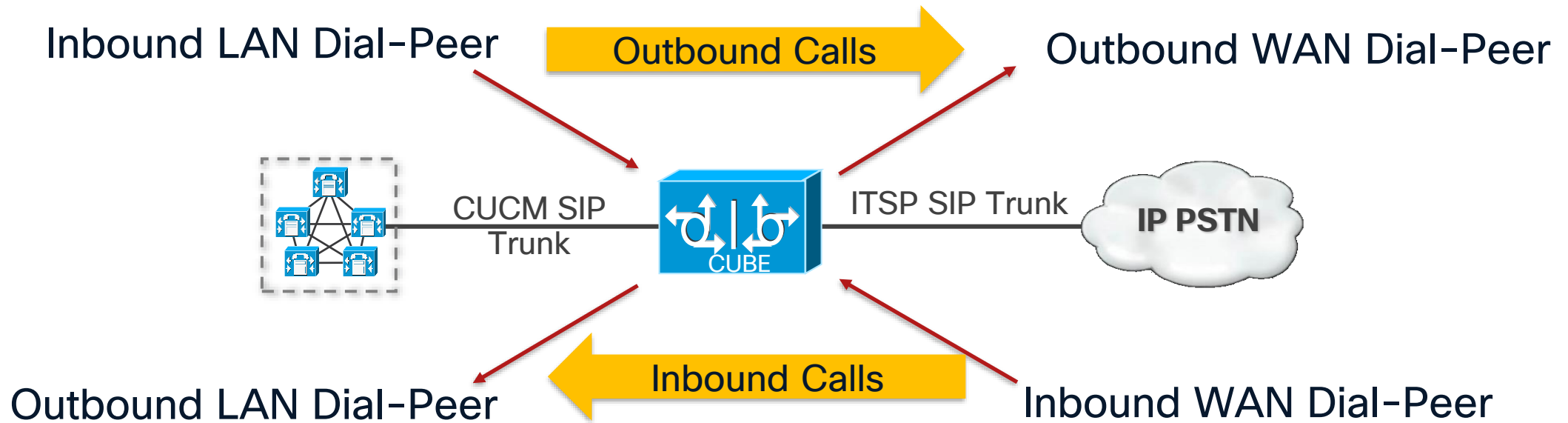
CUBE Version	Initial IOS-XE Release for this CUBE version and Release date		Subsequent IOS-XE Release for this CUBE version
14.4	17.6.1a	July 2021	17.6.8a
14.4	17.7.1a	Nov 2021	17.7.2
14.5	17.8.1a	March 2022	
14.6	17.9.1a	July 2022	17.9.7a
14.6	17.10.1a	Nov 2022	
14.6	17.11.1a	March 2023	
14.7	17.12.1a	July 2023	17.12.5b
14.8	17.13.1a	Nov 2023	
14.9	17.14.1a	March 2024	
14.10	17.15.1a	July 2024	17.15.3a
14.11	17.16.1a	Nov 2024	
TBD	17.18.1a	August 2025	

Last release for
ISR4K except
ISR4461

Dial-Peer Classifications

LAN and 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.



CUBE Configuration

Suggested CUBE Config Steps

Enable CUBE



voice service voip configuration, e.g. IP Trust list, SIP Parameters, Allow connection

Enable CUBE Application on the platform

1. Enable CUBE Application

```
voice service voip
```

```
allow-connections sip to sip
```

→ By default IOS/IOS-XE voice devices do not allow an incoming VoIP leg to go out as VoIP

2. Configure any other global settings

```
voice service voip
```

```
    sip
```

```
        early-offer forced
```

```
        audio forced
```

3. Create a trusted list of IP addresses to prevent toll-fraud

```
voice service voip
```

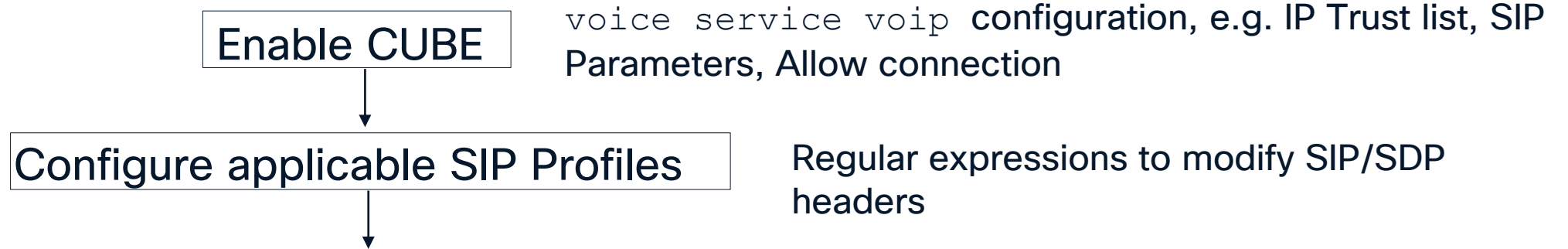
```
    ip address trusted list
```

```
    ipv4 66.77.37.2
```

→ Applications initiating signaling towards CUBE, e.g. CUCM, CVP,

→ Service Provider's SBC. IP Addresses from dial-peers with "session target ip" or session server group need not be added here

Suggested CUBE Config Steps



SIP Normalization

SIP profiles are a mechanism to normalize or customize SIP/SDP headers on CUBE to provide interop between incompatible devices

- SIP Profiles can be applied to both incoming and outgoing SIP messages on CUBE
- SIP Profiles can be applied
 - Globally (`voice service voip`)
 - On a dial-peer (`dial-peer voice <tag> voip`)
 - Tenant (`voice class tenant <tag>`)
- SIP Profiles are also supported on non-standard headers

```
voice class sip-profiles 1
rule 1 request INVITE sip-header Contact Modify "(.*)" "\1;temp=xyz"
rule 2 request INVITE sip-header Supported Add "Supported: "
```

SIP Profile Test Tool available on Collaboration Solutions Analyzer

Home

Tools

P Profile Tester (SPT)

Main page

Collaboration Solutions Analyzer

Report Problem

?

SIP Profile Rules **required**

Load a Prebuilt Rule Set

Please enter the SIP profile rules here. e.g:
rule 1 response 182 sip-header SIP-StatusLine modify "182 Queued" "183 Session In Progress"

Input Help: copystack, voice service voip, dial-peer, tenant, or other voice configurations are not required.
Syntax Help: SIP Profile Config Guide, SIP Copystack Config Guide

SIP Message To Test Rules On **required**

Load a sample SIP Message

Please enter the SIP message to which the add/remove/modify/copy rules should be applied.

Input Help: SIP Request URI or Status Line always required. SIP Headers/SDP Body optional unless testing them.
CSEQ required if "method" used in response rule.
Syntax Help: IANA SIP Parameters, IANA SDP Parameters

Peer SIP Message To Copy From **optional**

Show Peer Copy Input

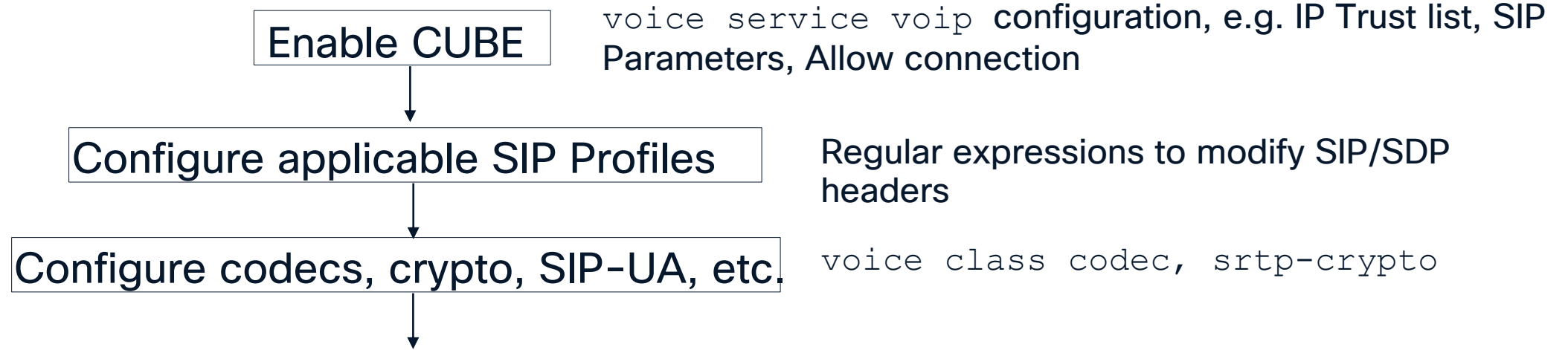
Input Help: Regular "copy" rules will use the other SIP Message; not this input.

Input Help: Regular "copy" rules will use the other SIP Message; not this input.

New Test

Run Test

Suggested CUBE Config Steps



Configure Codecs, Crypto, SIP-UA, etc.

```
voice class codec 1
  codec preference 1 opus
  codec preference 2 g711ulaw
```

- List of codecs to be supported on a call leg

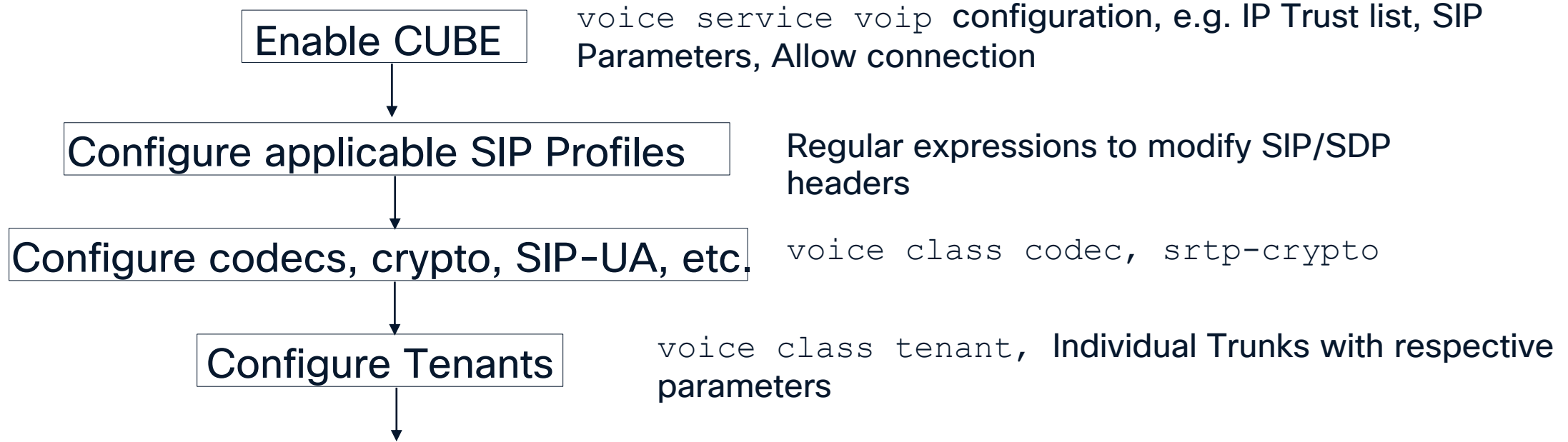
```
sip-ua
  transport tcp tls v1.2
  crypto signaling default trustpoint CUBE_CA_CERT
```

- TLS version, default trustpoint, etc.
- **TLS 1.3 supported from IOS-XE 17.15+**

```
voice class srtp-crypto 100
  crypto 1 AES_CM_128_HMAC_SHA1_80
```

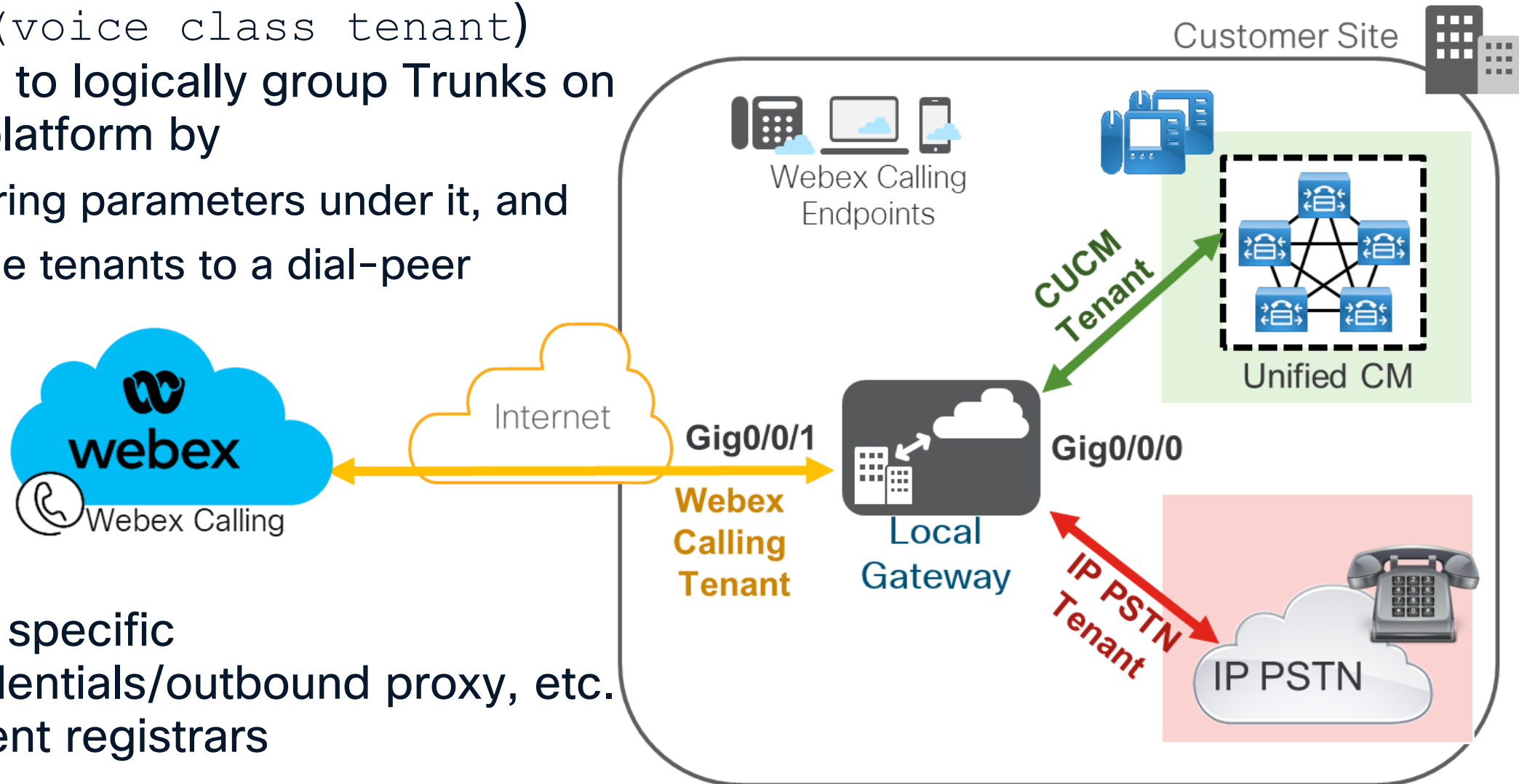
- Used to set the crypto cipher for TLS based SIP Trunks

Suggested CUBE Config Steps



Logical group of Trunks with Tenants

- Tenants (voice class tenant) allow you to logically group Trunks on a CUBE platform by
 - Configuring parameters under it, and
 - Apply the tenants to a dial-peer
- Provision specific bind/credentials/outbound proxy, etc. for different registrars



Configuring Voice Class Tenant

- **Configure voice class tenant**

```
voice class tenant 1
  registrar 1 ipv4:10.64.86.35:9052 expires 3600
  credentials username aaaa password 7 06070E204D realm aaaa.com
  bind control source-interface GigabitEthernet0/0
  bind media source-interface GigabitEthernet0/0
  copy-list 1
  outbound-proxy ipv4:10.64.86.35:9055
  early-offer forced
```



Add new voice class tenant

- **Apply tenant to the desired dial-peer**

```
dial-peer voice 1 voip
  destination-pattern 111
  session protocol sipv2
  session target ipv4:10.64.86.35:9051
  session transport udp
  voice-class sip tenant 1
```

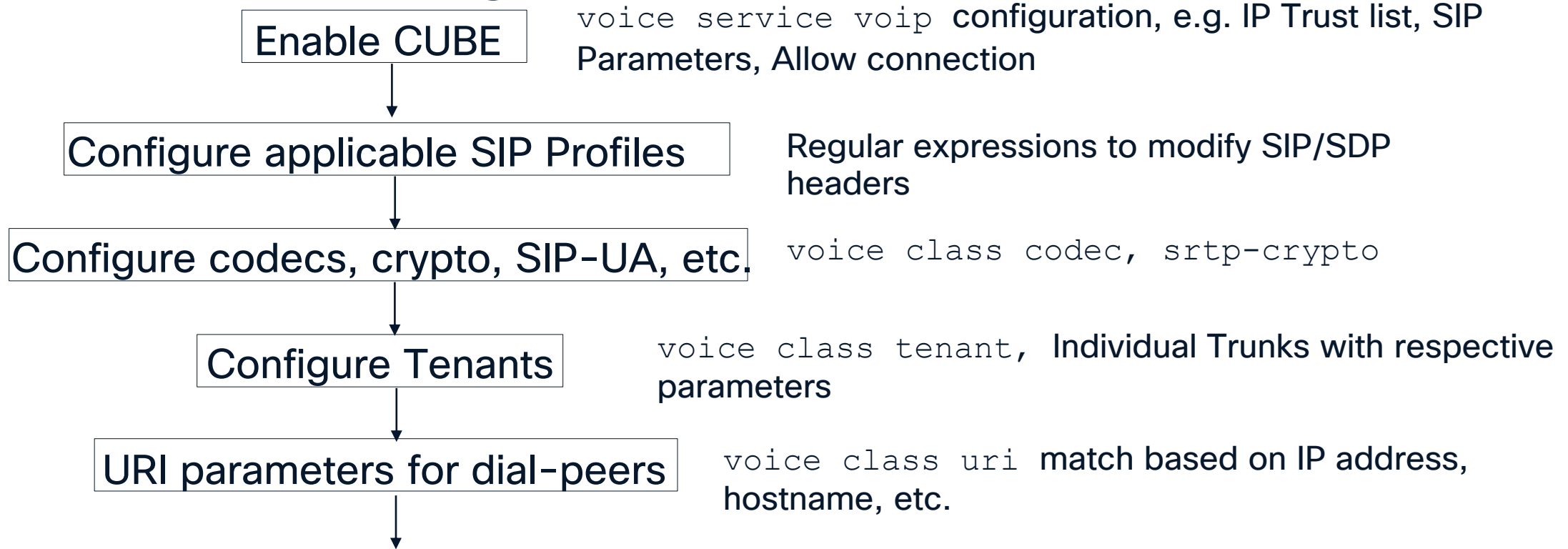


Apply Tenant to a Dial-peer

Configuration Preference Order

1. dial-peer (overrides tenant and global configs)
2. tenant (overrides the global config)
3. global (voice service voip OR sip-ua)

Suggested CUBE Config Steps



Voice class URIs

```
voice class uri 1
 host ipv4:10.1.1.1
 host dns:cisco.com
 pattern 654321@10.2.1.1
 user-id 654321
```

- allows you to configure the selection of inbound dial peers by matching parts of the URI sent by a remote SIP entity
- different parts of the URI like username, IP address, and DNS can be specified

Received:

INVITE sip:654321@10.2.1.1 SIP/2.0

Via: SIP/2.0/UDP 10.1.1.1:5060;x-route-tag="cid:orange@10.1.1.1";;branch=z9hG4bK-23955-1-0

From: "555" <sip:555@10.1.1.1:5060>;tag=1

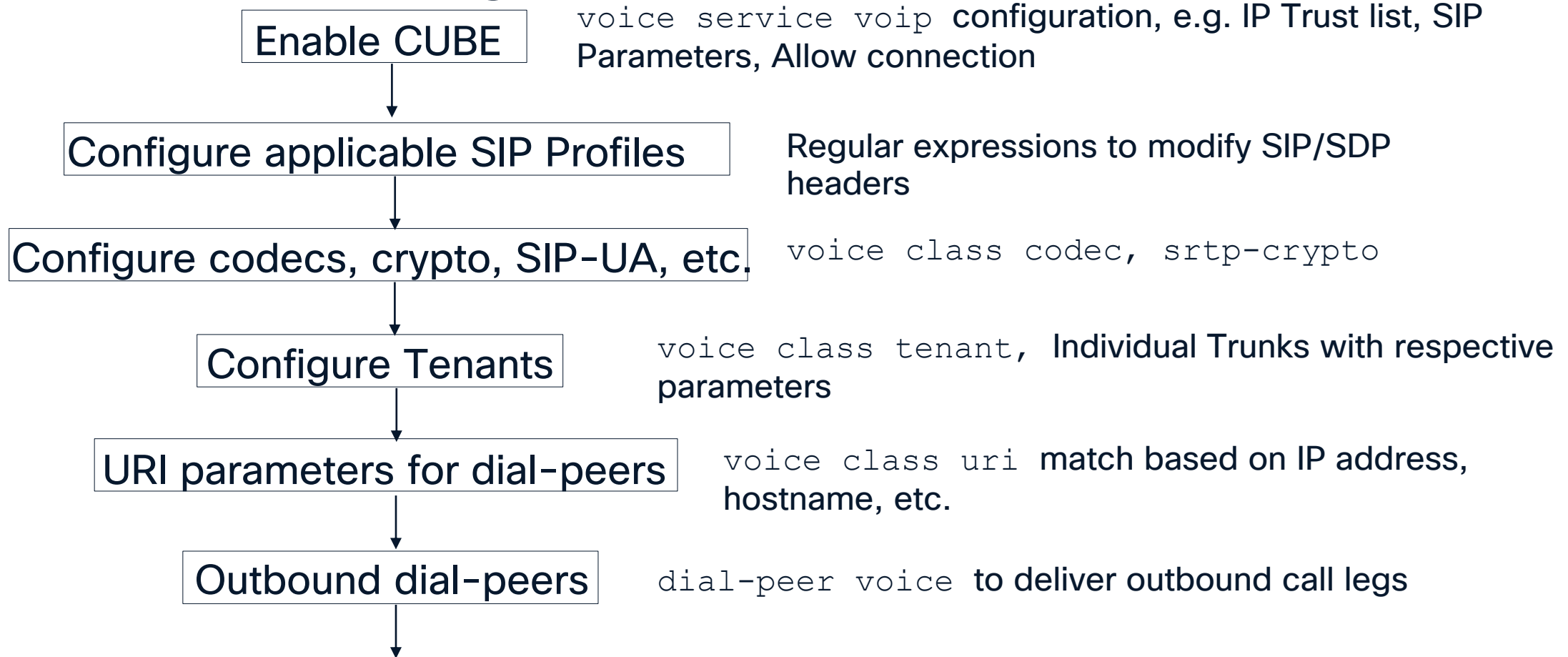
To: ABC <sip:654321@10.2.1.1:5060>

Call-ID: 1-23955@10.1.1.1

CSeq: 1 INVITE

Contact: sip:555@10.1.1.1:5060

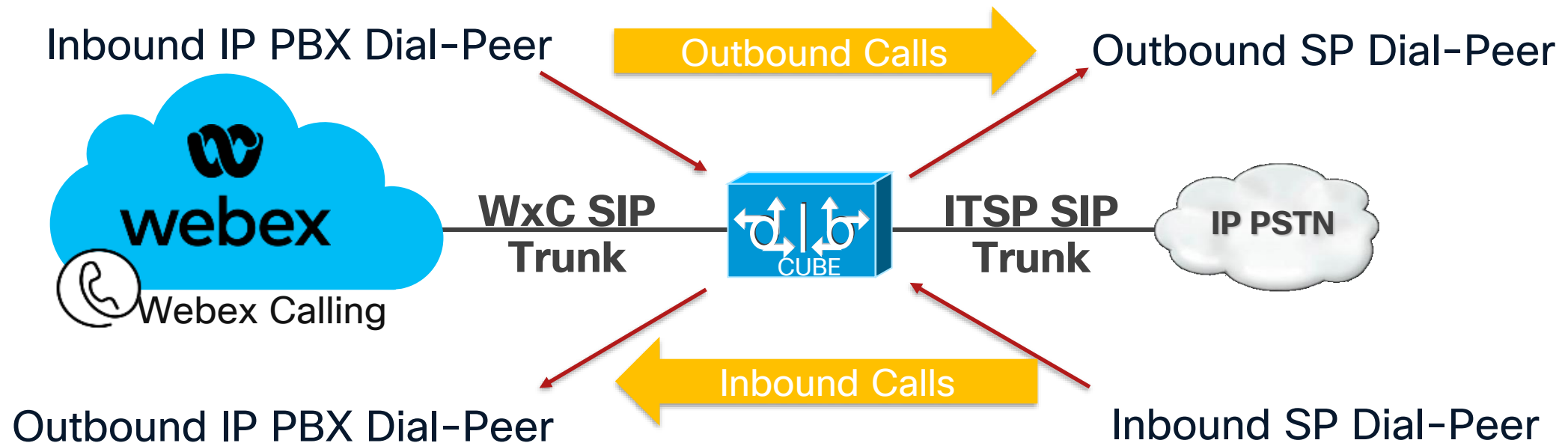
Suggested CUBE Config Steps



Understanding Dial-Peer Matching and Classification

IP PBX and ITSP Dial-Peers

- **IP PBX Dial-Peers** – Dial-peers that are facing towards the IP PBX for sending and receiving calls to and from the PBX (e.g. Webex Calling, CUCM).
- **Service Provider (ITSP) Dial-Peers** – Dial-peers that are facing towards the SIP Trunk provider for sending and receiving calls to and from the provider.



Outbound Dial-Peer Configuration

SIP Service Provider facing OUTBOUND dial-peer

```
dial-peer voice 101 voip
description Outgoing dial-peer to IP PSTN
destination-pattern +1T
session protocol sipv2
session target ipv4:A.B.C.D
voice-class codec 1
voice-class sip tenant 1
dtmf-relay rtp-nte
no vad
```

Meaningful description on the dial-peer

Phone number match criteria

Destination IP Address to deliver the call leg. E.g., SIP service provider

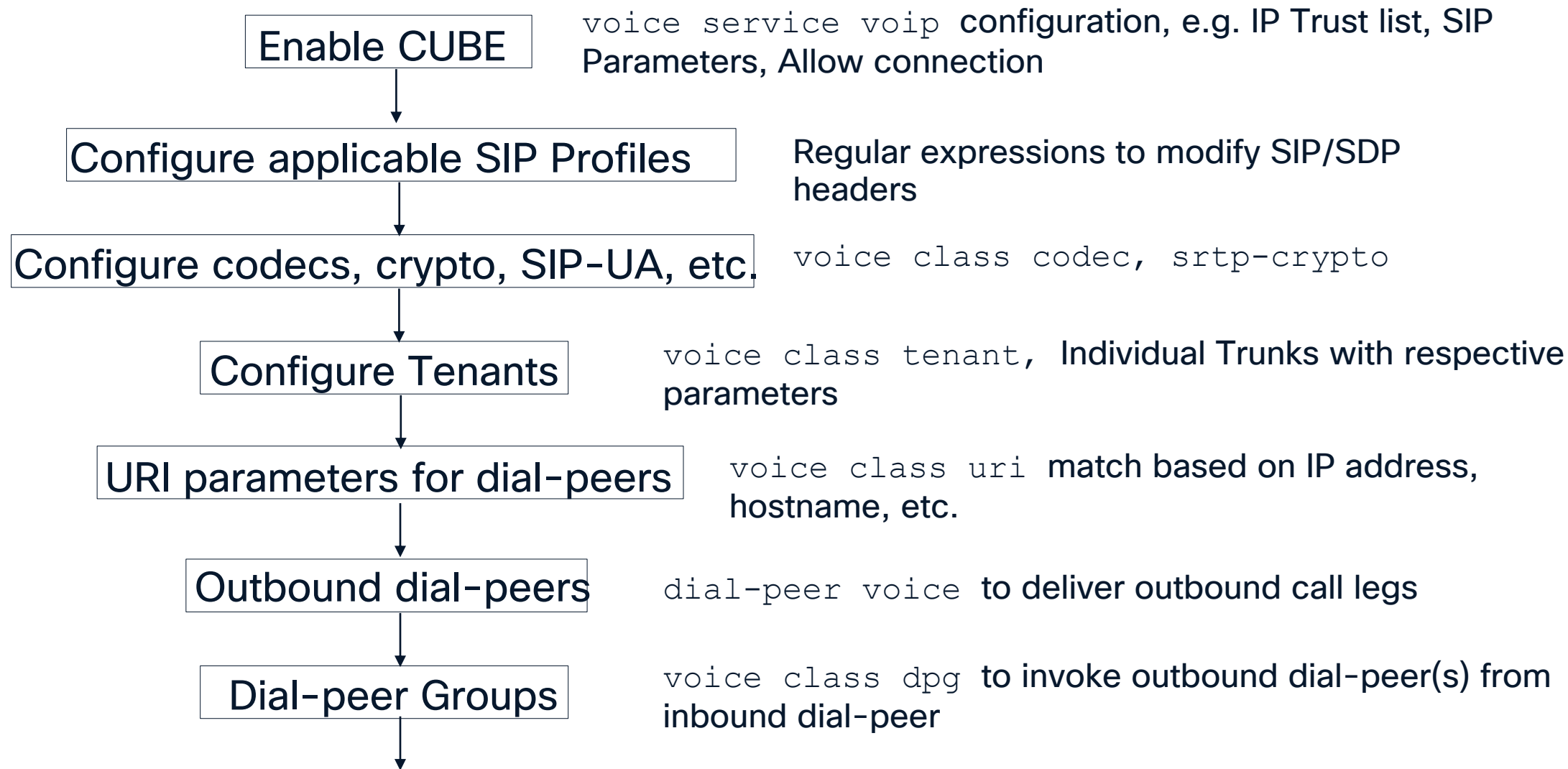
Codec List supported for this call leg

Inherit parameters from the tenant

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>

Suggested CUBE Config Steps



Destination Dial-peer Group

```
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
```

Received:

INVITE sip:1341@<CUBE-IP> SIP/2.0

Sent:

INVITE sip:1341@10.1.1.3 SIP/2.0

3. Outbound
DP is
selected

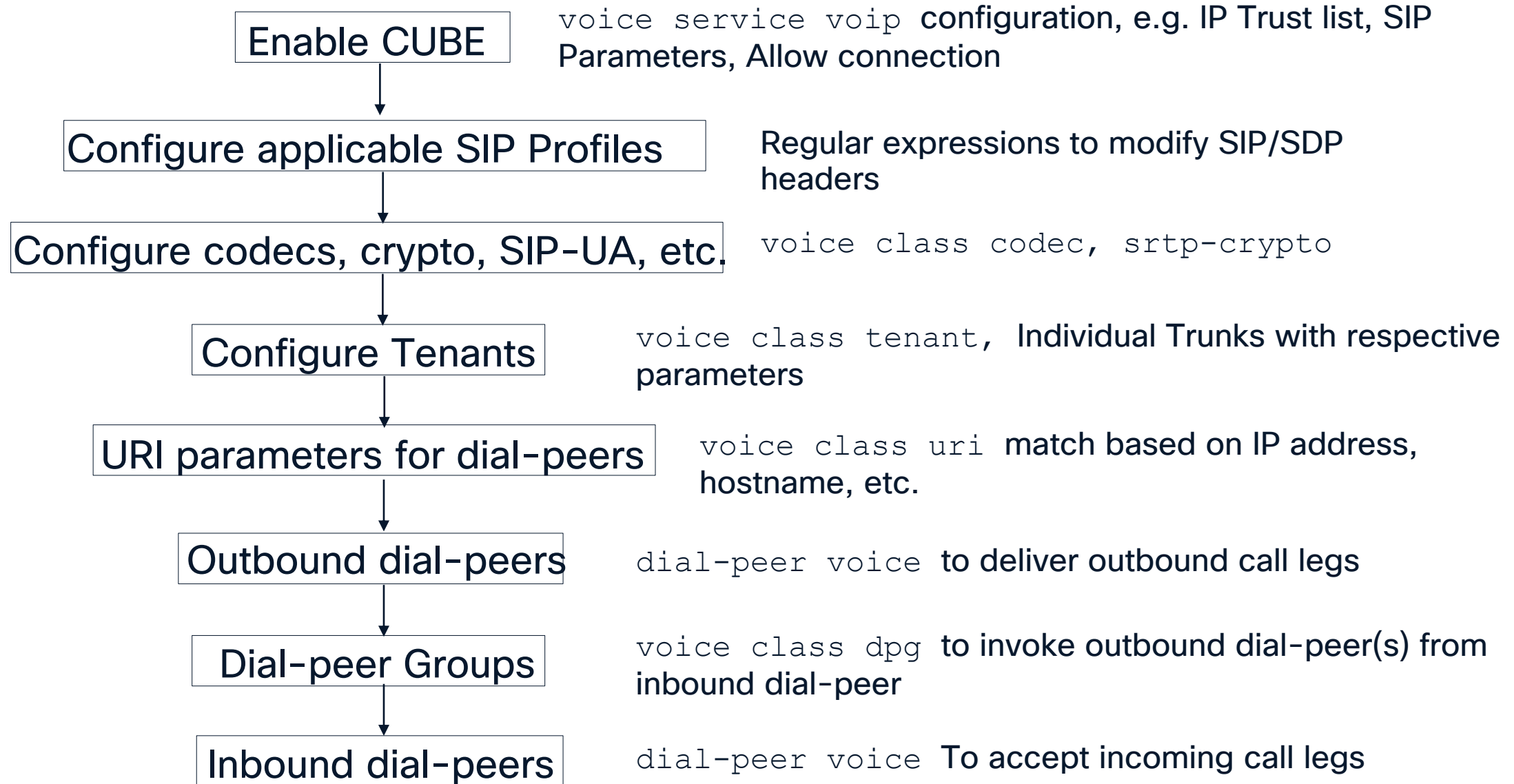
```
dial-peer voice 786 voip
  destination-pattern 1341
  session protocol sipv2
  session target ipv4:10.1.1.1
```

```
!
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
```

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

Suggested CUBE Config Steps



Inbound Dial-Peer Configuration

SIP Service Provider facing INBOUND dial-peer

```
dial-peer voice 786 voip
description Incoming dial-peer from IP PSTN
session protocol sipv2
destination dpd 200
incoming uri via 100
voice-class codec 99
voice-class sip tenant 300
dtmf-relay rtp-nte
no vad
```

Meaningful description on the dial-peer

Bypass default outbound dial-peer matching and invoke outbound dial-peer(s) of this DPG

Inbound match criteria

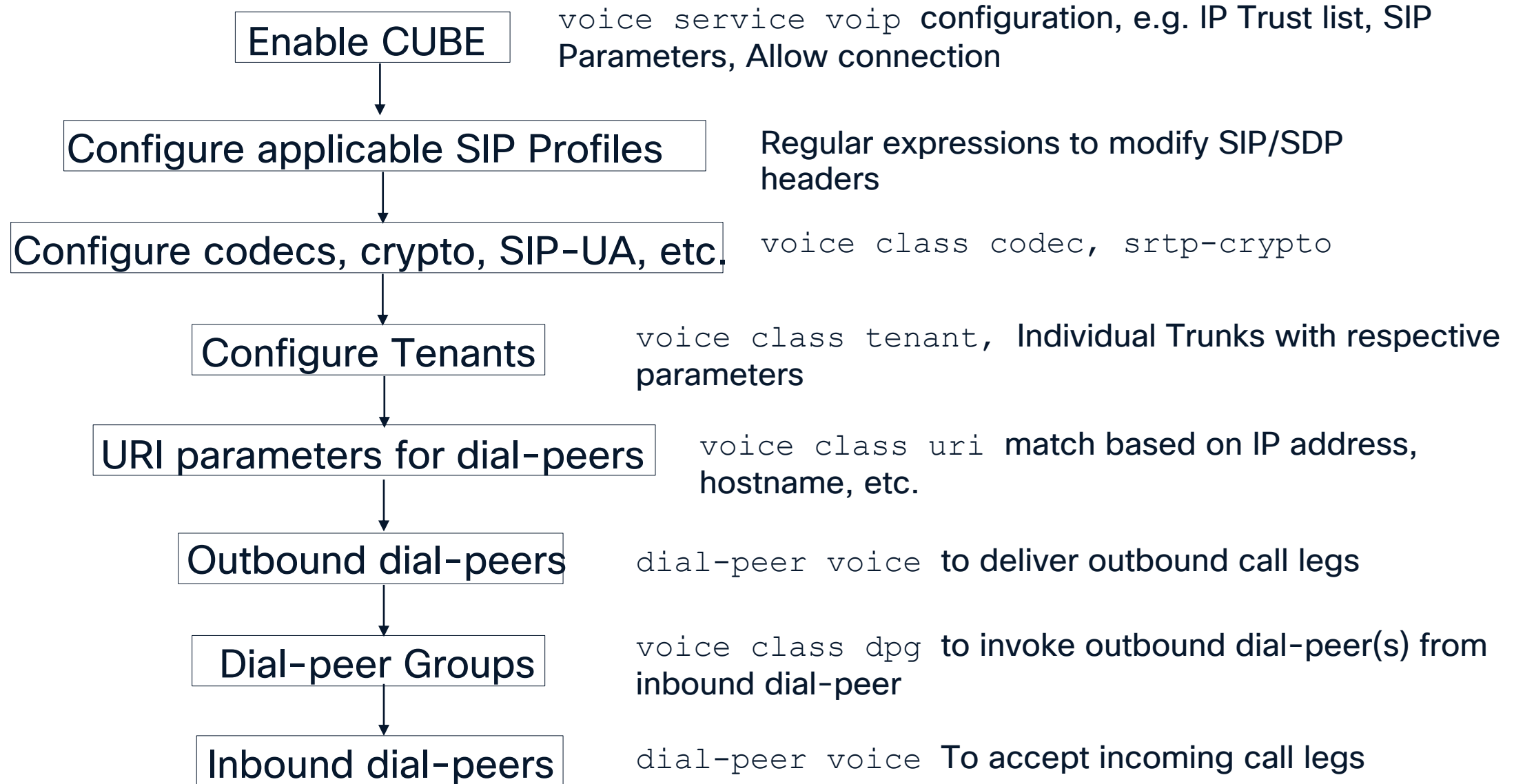
Codec List supported for this call leg

Inherit parameters from the tenant

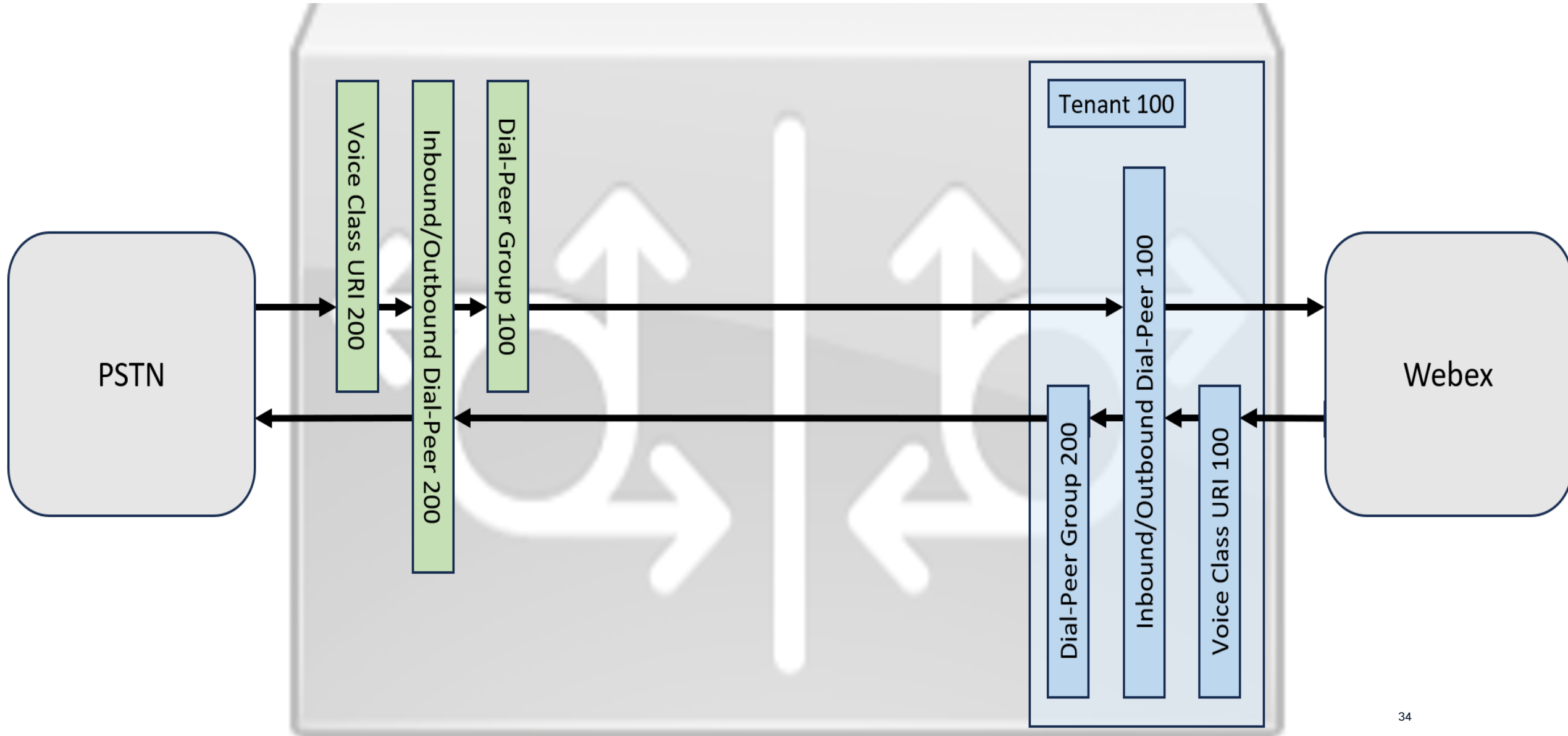
Inbound SIP Dial-Peer Selection Preference

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>

Suggested CUBE Config Steps



Grouping trunks with voice class tenants



Call Admission Control (CAC)

- Call processing capacity for any CUBE instance will be influenced by several considerations, including software version, features configured and the platform itself
- To ensure that calls continue to be processed reliably, configure Call Admission Control as follows to reject calls when use of system resources exceeds 80%¹. Refer to the [CUBE Configuration Guide](#) for further details

```
enable
conf t
  call threshold global cpu-avg low 75 high 80
  call threshold global total-mem low 75 high 80
  call treatment
end
```

¹ For an ISR4461, starting IOS-XE 17.3.2 or later, testing benchmark is at 80% memory utilization. Configure the memory threshold CAC accordingly.

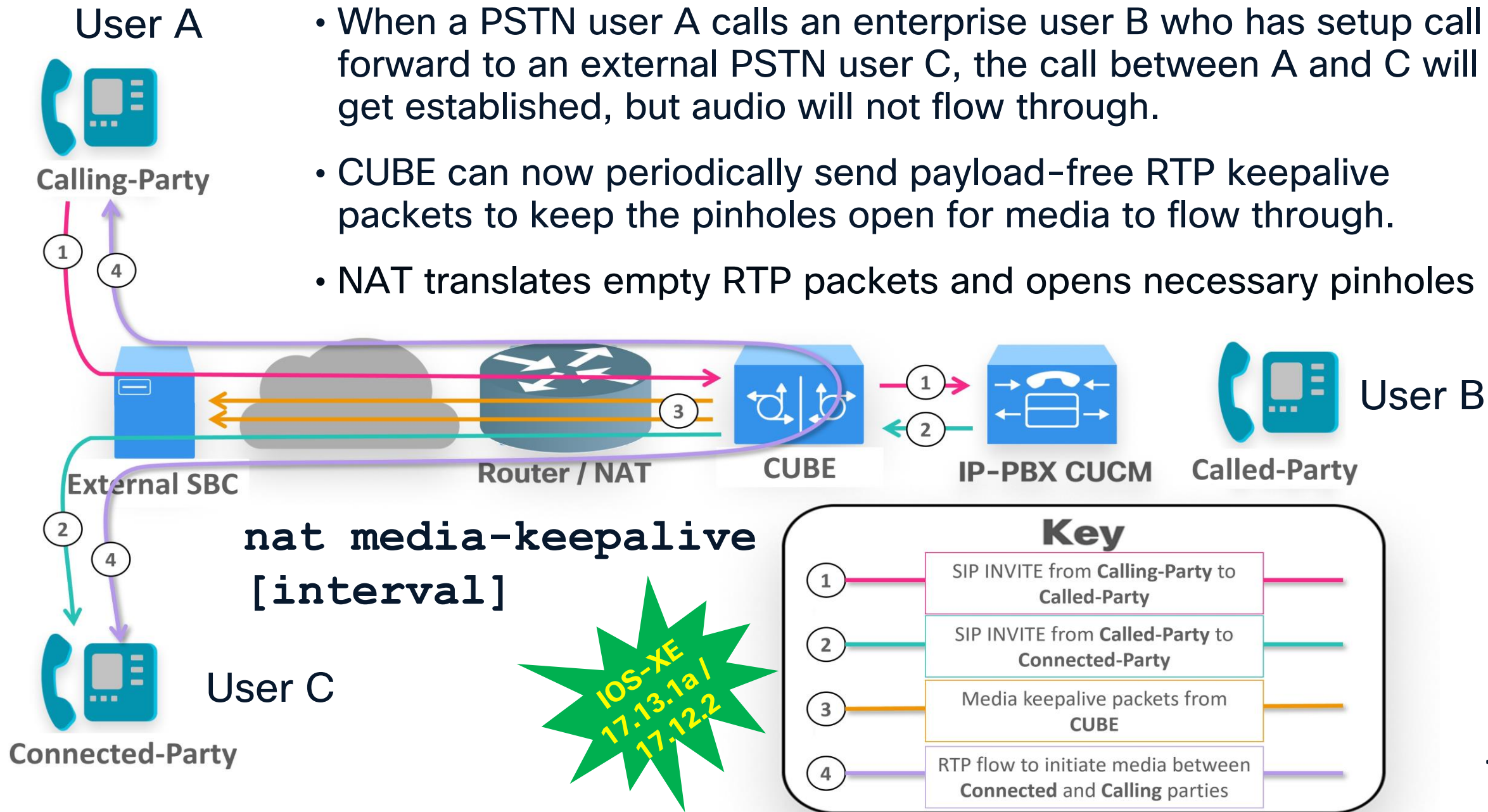
```
call threshold global total-mem low 80 high 85
```

Version 14 Updates

NAT Traversal using RTP keepalives

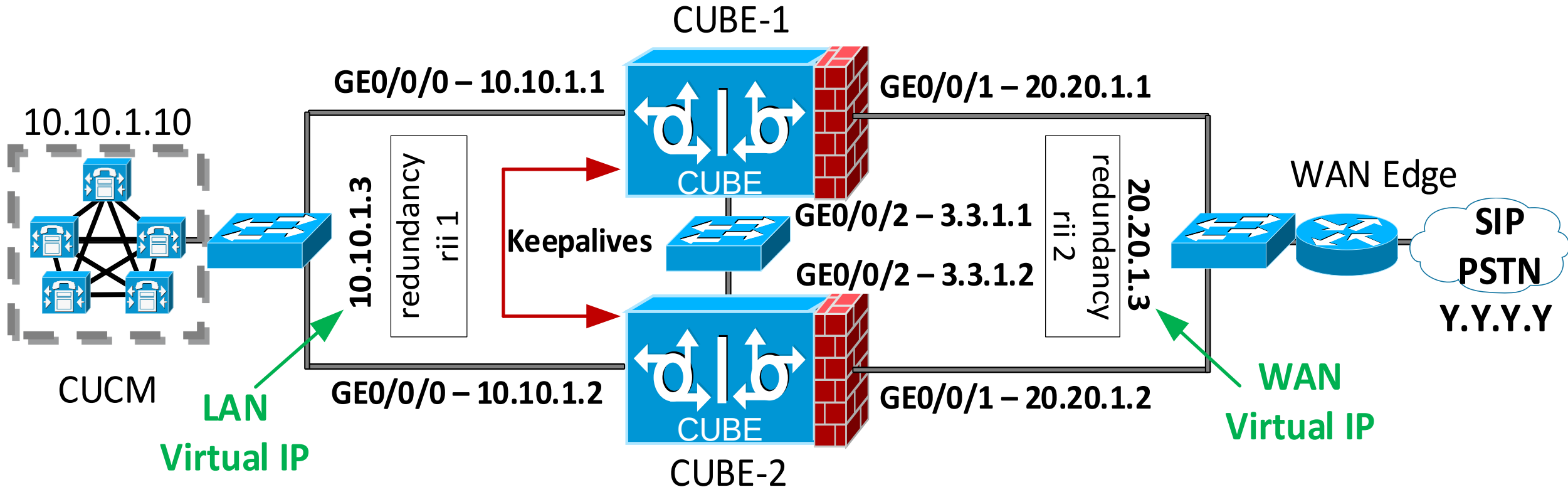
Introducing NAT Traversal using RTP keepalives

- 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.
- CUBE can now periodically send payload-free RTP keepalive packets to keep the pinholes open for media to flow through.
- NAT translates empty RTP packets and opens necessary pinholes



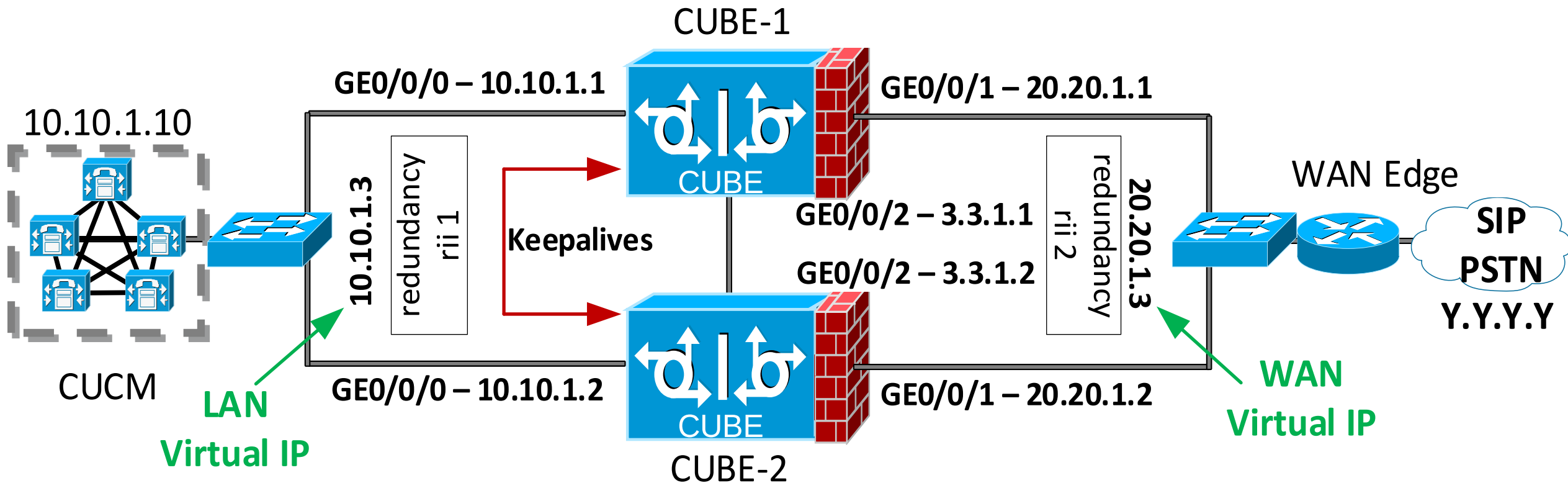
CUBE High Availability (HA) Updates

CUBE HA for Call Preservation



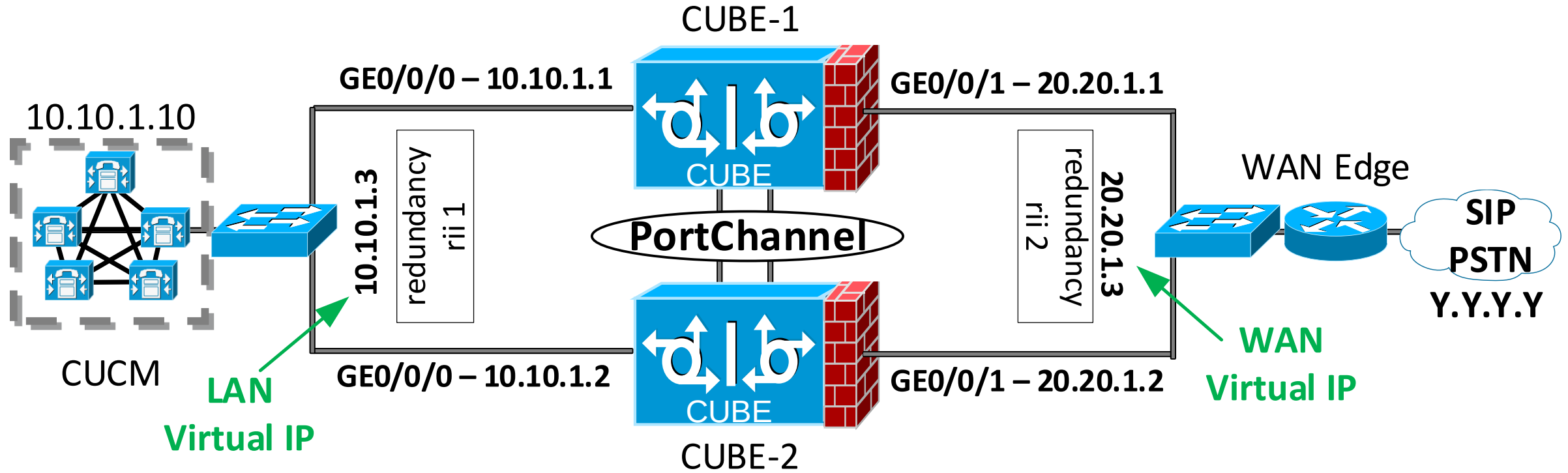
- RG Control/Data interface (G0/0/2) had to be connected via a physical switch
- It can now be connected via a back-to-back cable

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

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 or later**
 - CUBE attempts OPTION keepalives with 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

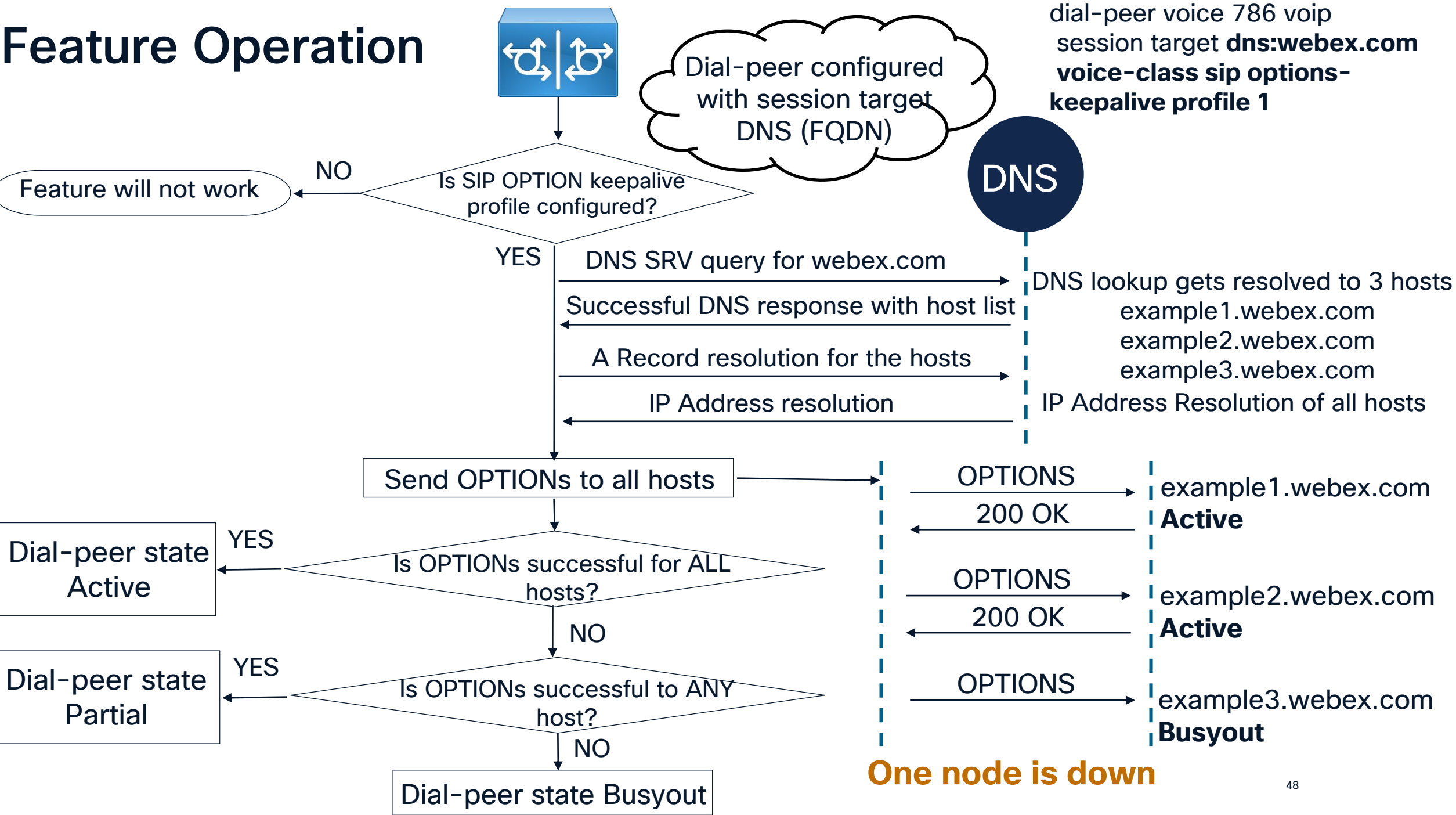
```
CUBE(config)# voice class sip-options-keepalive 1
CUBE(config-class)#description keepalive-webex
CUBE(config-class)#transport tcp
CUBE(config-class)#down-interval 15
CUBE(config-class)#up-interval 5
CUBE(config-class)#retry 1
```

```
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 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 ipv4:10.64.86.70:5880	46	10	50	busyout
		example2.webex.com ipv4:10.65.105.59:5060	45	10	50	active
		example1.webex.com ipv4:10.65.105.58:5060	44	10	50	active

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 ipv4:10.64.86.70:5880	46	10	50	busyout
		example2.webex.com ipv4:10.65.105.59:5060	45	10	50	busyout
		example1.webex.com ipv4:10.65.105.58:5060	44	10	50	busyout

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	syst	ipv4:10.48.53.54			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.

Trunk Info

```
dial-peer voice 2000 voip
description To WxC Edge Proxy SRV Address
session protocol sipv2
session target dns:us18.sipconnect.bcld.webex.com
```

Webex Calling edge proxy address (FQDN)
Currently unavailable

Webex Calling edge proxy address (SRV)
us18.sipconnect.bcld.webex.com

Note: CSCwm08791 Dial-peer never recovers an active state if it goes partial or busyout

Symptom: Dial-peer status is shown as partial/busyout with FQDN, whereas all the nodes in the SRV or IP address are marked as up.

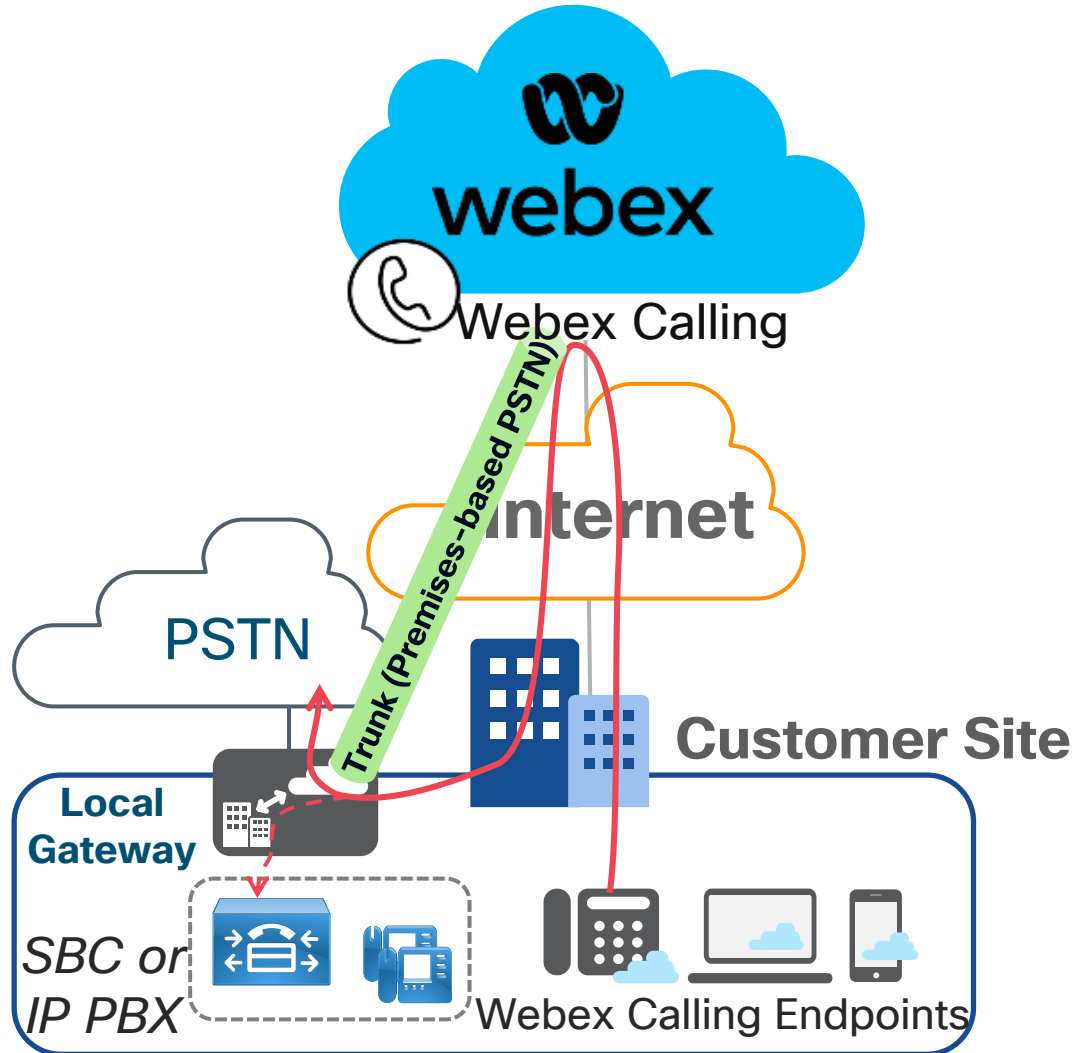
Fixed Release: IOS-XE 17.9.7a, 17.12.5a/5b, 17.15.3a/3b, 17.16.1a

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 3 rd 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 addresses 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 <u>Root Certificate Authorities</u>. • Wild-card certificates are not supported • Certificates must be signed per guidelines as mentioned in <u>Configure Trunks, Route Groups, and Dial Plans for Webex Calling</u>

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

Local Gateway

Platform Support

Only Certificate-based supported



AnyNode



Oracle



Audiocodes



Ribbon



NetMatch-S

Local Gateway (LGW)



CUBE



IOS-XE VGW

Both Registration-based and Certificate-based supported

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

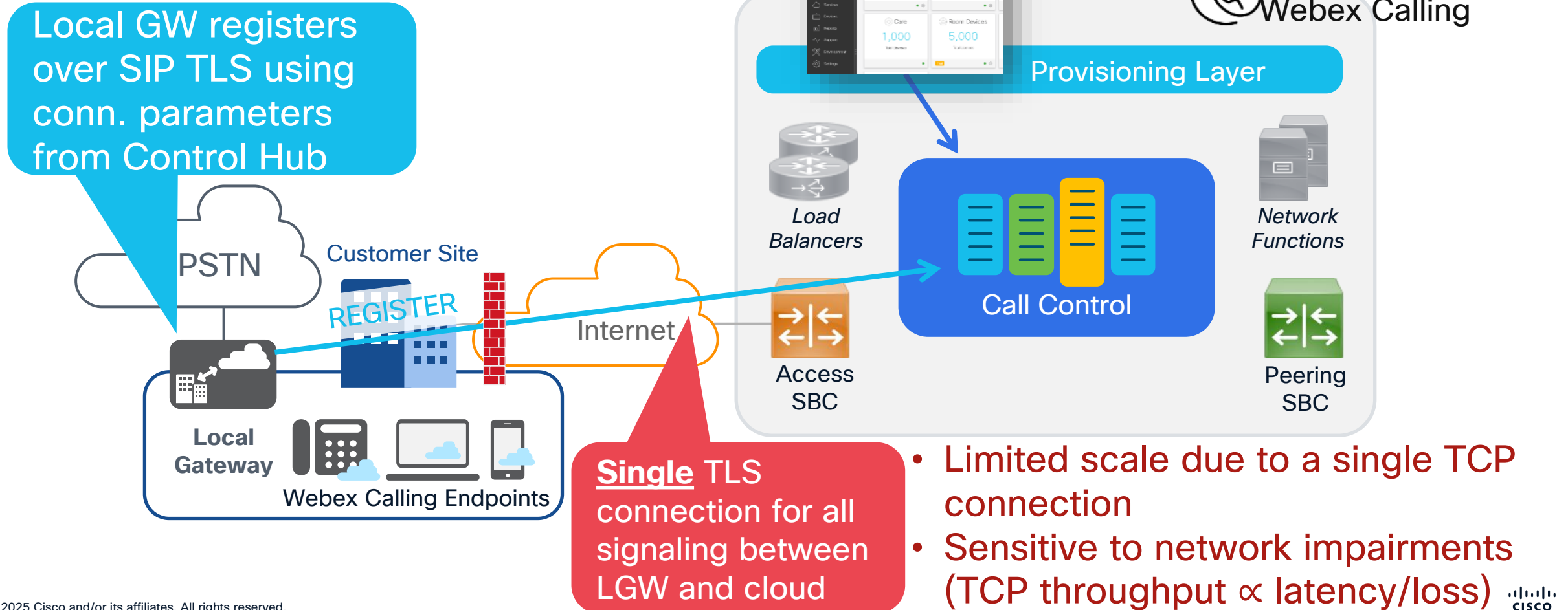
- Over the top (OTT) Internet and interconnect (e.g. Webex Edge Connect) must meet the following link quality conditions

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

Registration-based LGW on a CUBE

Registration-based Local Gateway

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



Log in to Control Hub. Navigate to **Services** – Click **Calling** and then go to the **Call Routing** Tab. Click **Add Trunk**.

webexControl Hub

Search

1

?

✓

HA

Account

Organization Settin...

SERVICES

Updates & Migratio...

Messaging

Meeting

Calling

Customer Experien...

Vidcast

Contact Center

Connected UC

Calling

Numbers

Virtual Lines

Call Routing

Managed Gateways

Features

PSTN

>>

Trunk

Route Group

Dial Plans

Verify Call Routing

Zone

Trusted Network Edge

Trunk

SIP trunks provide connectivity to a customer-owned PSTN service and to an on-premises IP PBX deployment. These were previously accessed via the Local Gateway configuration page.

Add Trunk

Search

Name	Location	Trunk Type	In Use
TokyoLGW	Tokyo	Registration based	No

© 2025 Cisco and/or its affiliates. All rights reserved.

73

cisco

Add a new Trunk for the desired Location

- Trunk name is limited to 24 characters

Add Trunk

Location

This location is where the trunk is physically connected. To create a new location, visit the [Locations](#) page.

Atlanta



Name

Hussain



Trunk Type

Choose the right trunk type for this local gateway. [Learn more](#) on trunk type

Registration based



Device Type

Select Device



Dual Identity Support

Cancel

Save

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

Add Trunk



Control Hub Trunk Info Connection Parameters → LGW CLI Config

Hussain Successfully Created.

Visit [Route Group](#) page to add trunk(s) to a route group

Visit [Locations](#) page to configure PSTN connection to individual

Visit [Dial Plans](#) page to use this trunk as the routing choice for a

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

Authentication Information

Record the username and password

lose this information, you need

username and reset the password

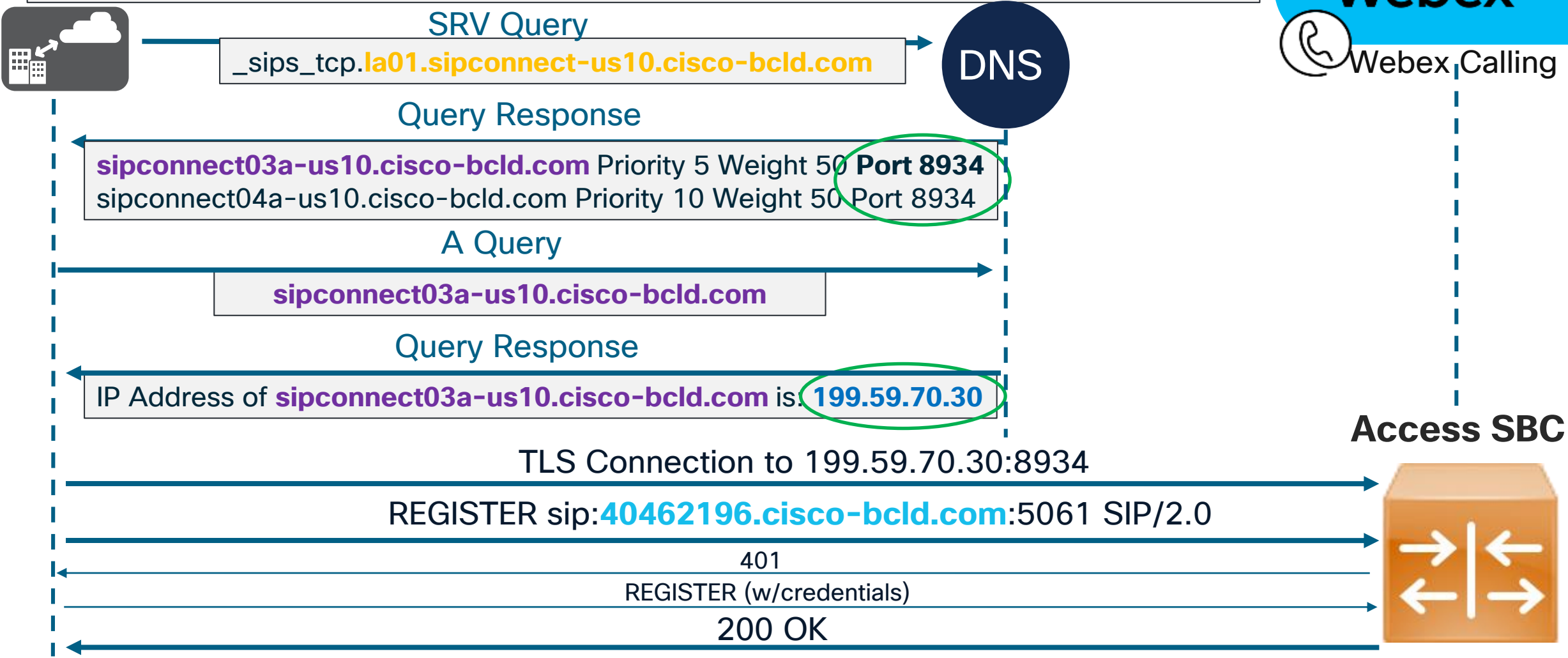
Username: Hussain2572_LGU

Password: meX7]-)VmF

```
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

voice class tenant 200
registrar dns:**40462196.cisco-bcld.com** scheme sips expires 240 refresh-ratio 50 tcp tls
session transport tcp tls
url sips
outbound-proxy dns:**la01.sipconnect-us10.cisco-bcld.com**



Certificate-based Local Gateway

Add a Certificate-based Trunk to a Location

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

Enterprise Session Border Controller (SBC) Address

Select the type and enter an FQDN or SRV address for Webex Calling to reach out to your Enterprise SBC.
You must have the domain for your SBC's FQDN/SRV [claimed or verified](#) before you can use this address. [Manage your domains](#)

☒ FQDN

☐ SRV

Hostname *

sbc2

Domain *

tmedemo.com

Port *

5061

☒ Valid address

FQDN

sbc2.tmedemo.com:5061

Maximum number of concurrent calls *

1000

Adding a Trunk

Add Trunk

Location

This location is where the trunk is physically connected. To create a new location, visit the [Locations](#) page.

Name

Trunk Type

Choose the right trunk type for this local gateway. [Learn more](#) on trunk type

Device Type

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

Enterprise Session Border Controller (SBC) Address

Select the type and enter an FQDN or SRV address for Webex Calling to reach out to your Enterprise SBC.

You must have the domain for your SBC's FQDN/SRV [claimed or verified](#) before you can use this address. [Manage your domains](#)

☒ FQDN

☐ SRV

Hostname *

Domain *

Port *

sbc2

tmedemo.com

5061

☒ Valid address

FQDN

sbc2.tmedemo.com:5061

Maximum number of concurrent calls *

1000

Save the Webex Calling Edge Proxy Address 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)

Currently unavailable

Webex Calling edge proxy address (SRV)

us18.sipconnect.bcld.webex.com

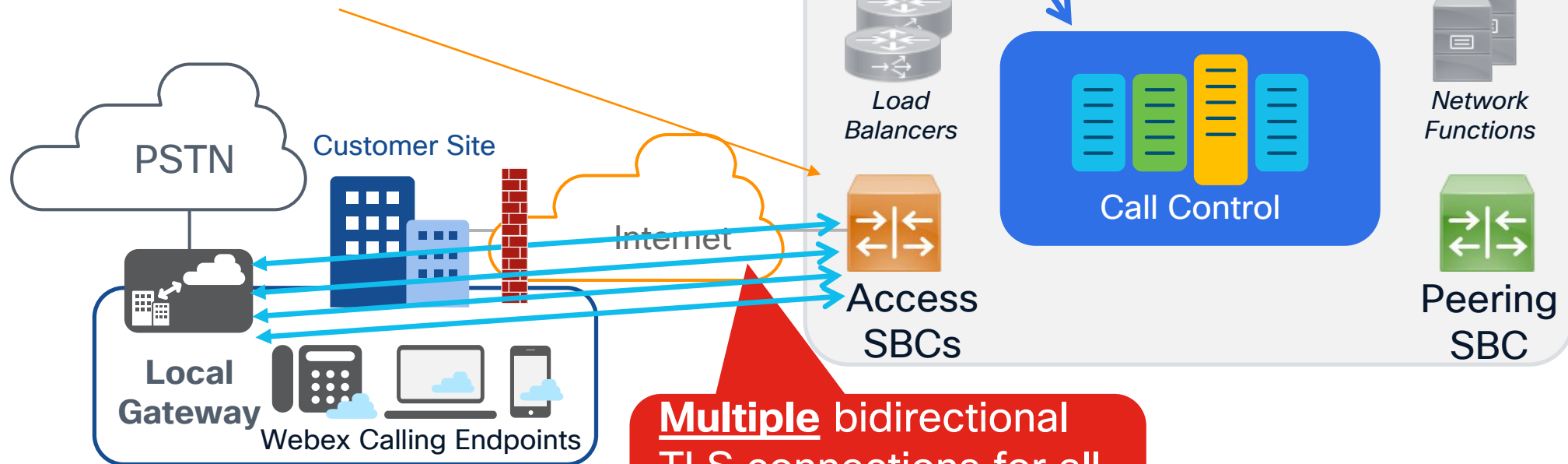
Webex Calling Trunk - Local Gateway (Certificate-based)

Customer DNS/FQDN SRV's configured in CH

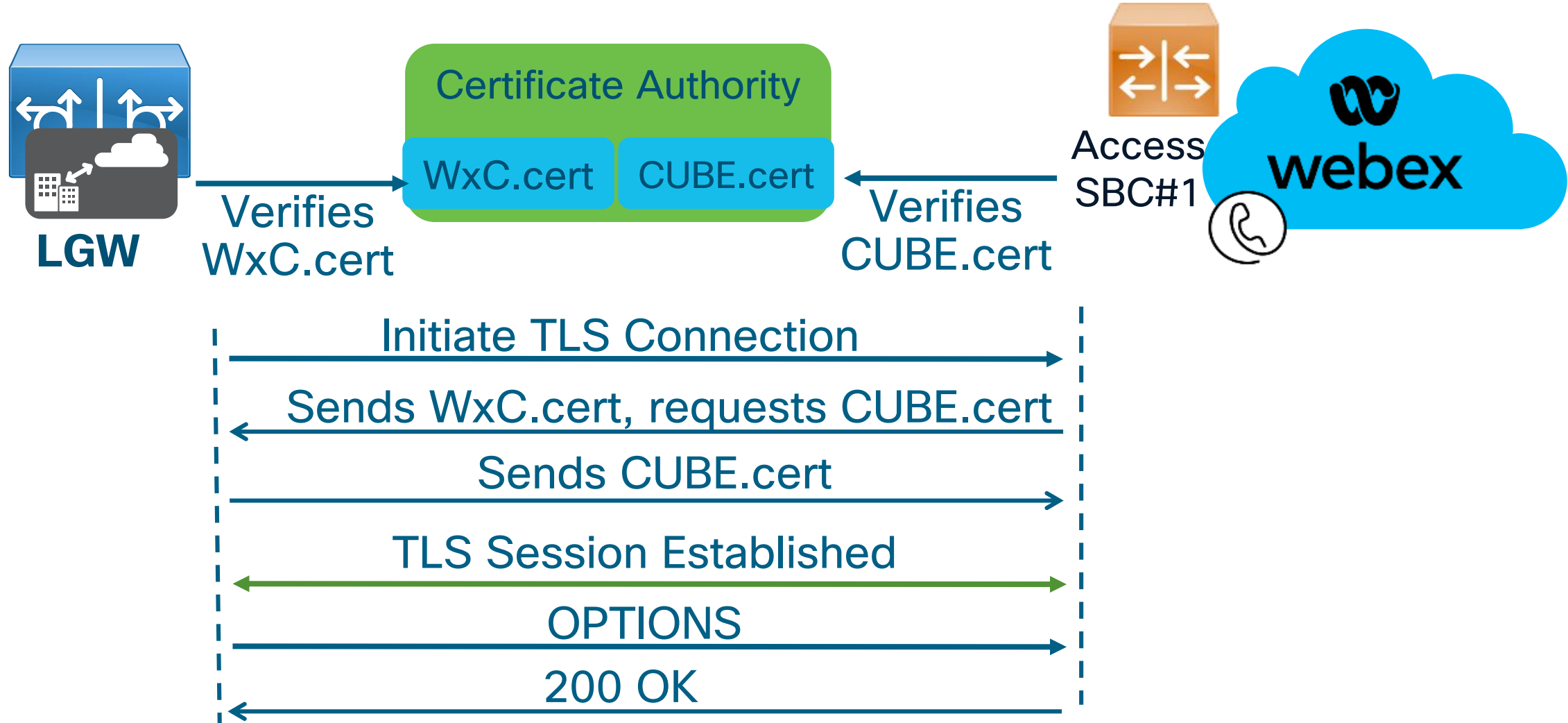


Webex Calling edge proxy address (FQDN)
Currently unavailable

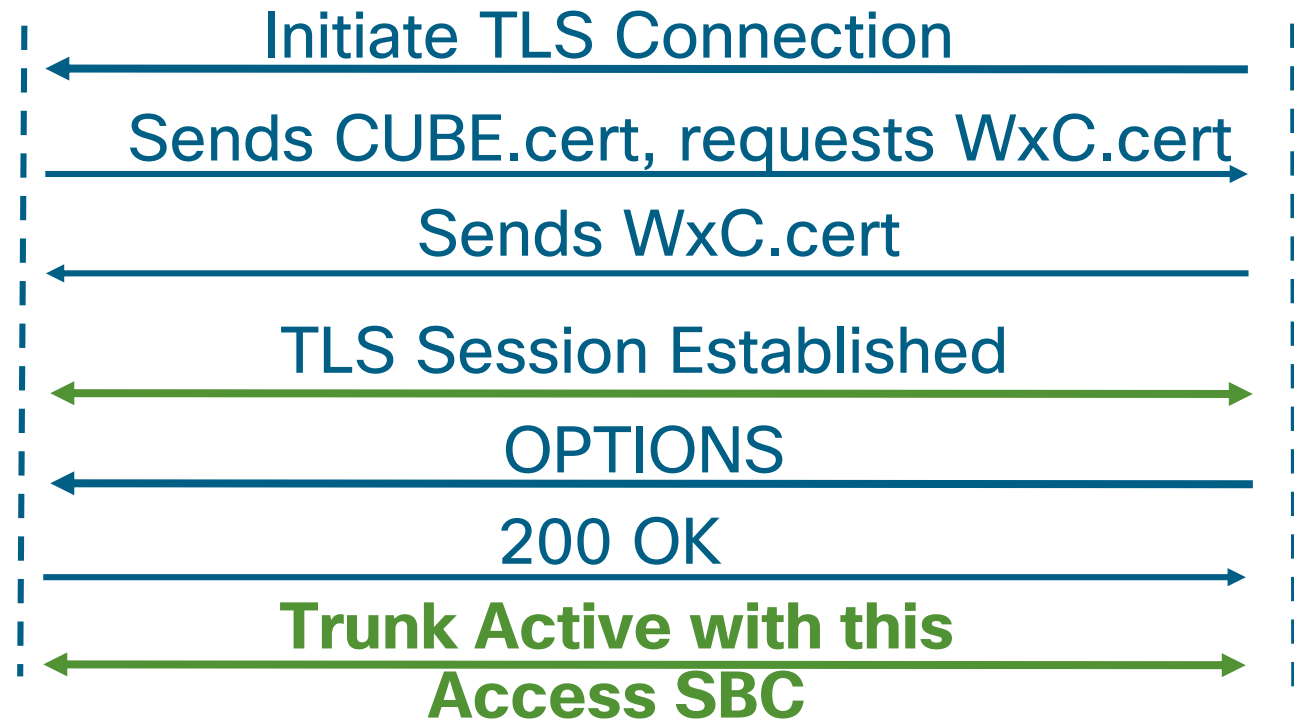
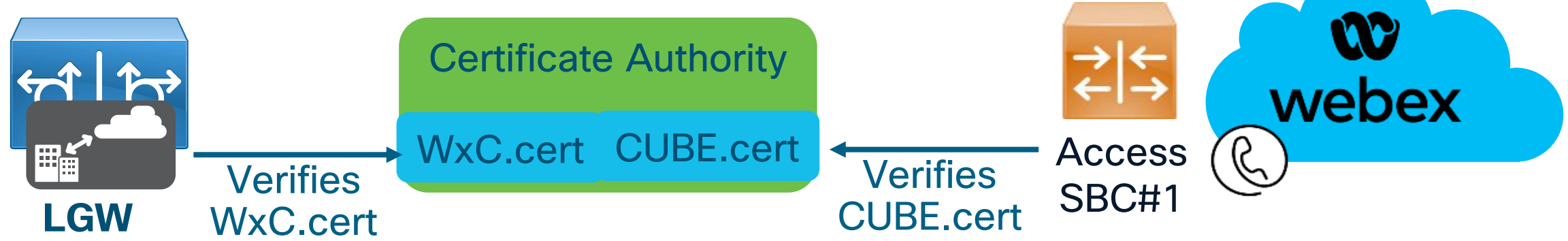
Webex Calling edge proxy address (SRV)
us18.sipconnect.bclid.webex.com



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



Webex Calling edge proxy address (FQDN)

- 1 peering1.jp.sipconnect.bclid.webex.com:5062
- 2 peering2.jp.sipconnect.bclid.webex.com:5062
- 3 peering3.jp.sipconnect.bclid.webex.com:5062
- 4 peering4.jp.sipconnect.bclid.webex.com:5062

Trunk > Details

Status ⓘ

● Online

Trunk Type

Certificate based

Device

Cisco Unified Border Element

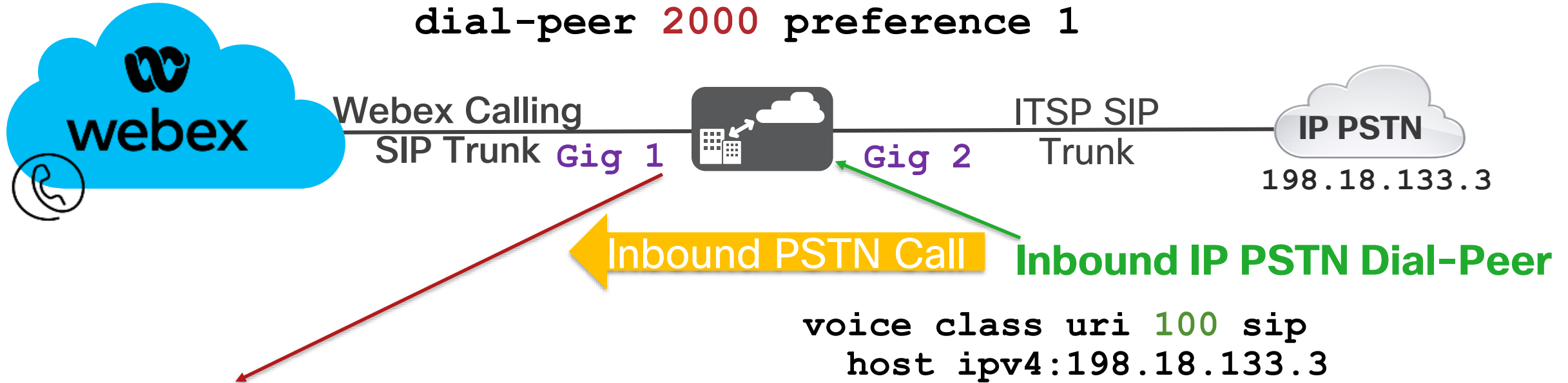
Now repeat the process with the 2nd, the 3rd, and the 4th WxC Access SBC

Inbound LGW PSTN Call

```
voice class dpg 200
```

```
description Incoming IP PSTN(DP100) to WxC(DP2000)
```

```
dial-peer 2000 preference 1
```



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
```

```
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 LGW PSTN Call

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

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

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

FQDN

sbc2.tmedemo.com:5061

**Inbound WxC Dial-
Peer**

Outbound PSTN Call

**Outbound IP PSTN Dial-
Peer**



Webex Calling
SIP Trunk

Gig 1



ITSP SIP Trunk

Gig 2

IP PSTN

198.18.133.3

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

Local Gateway Status Improvements in Control Hub

Peak, current active, and Max calls will be displayed



Calling

NumbersVirtual Lines**Call Routing**Managed GatewaysFeaturesPSTNService SettingsClient Settings

TrunkRoute GroupDial PlansVerify Call RoutingZoneTrusted Network EdgeTranslation Pattern

SIP trunks provide connectivity to a customer-owned PSTN service and to an on-premises IP PBX deployment. These were previously accessed via the Local Gateway configuration page.

All trunks7 trunksLast updated on 09/01/2024 11:32 PM

Name ↓	Location	Trunk type	Peak active calls ⓘ	Current active/Max calls ⓘ	In use ⓘ	Status	Actions
LGW Name1	ACE-test-LGW	Registration based	-	334/500	No	● Offline	
LGW Name2	ACE-emea-LGW	Registration based	243		Yes	● Online	
LGW Name3	ACE-amer-LGW	Registration based	467	334/500	No	● Impaired	
LGW Name4	ACE-emea2-LGW	Registration based	243	119/600	Yes	● Online	
LGW Name5	ACE-tyo-LGW	Registration based	345	223/500	No	○ Unknown	

Color of peak active calls will be changed to red after 80%

- Peak number of calls handled by the trunk in the last 72 hours. Trunks exceeding 80% capacity are shown in red.
- Active concurrent calls handled by the trunk
- Max configured calls

Local Gateway Alerts in Control Hub

Real time Alerts



- Alerts will trigger based on LGW status changes and will include:
 - Trunk status Online/Offline events (Real Time).
 - Ability to choose one or more trunk(s)
 - Certificate expiry (Pre expiry and post expiry alerts)
 - Pre-expiry alert before predefined days at specific days at 60 days, 30 days, 15 days, 7 days.
Post-expiry, an alert just after the certificate has expired. Single alert.
 - Concurrent call limit alerts for trunks (based on sum of both inbound and outbound calls)
 - alerts based on threshold percentages [e.g., alert if 80% of peak active call had reached for Trunk(s)]
 - Assists to identify call concurrency for a busy day, busy hour, etc.

Create a rule – Trunk Status Alert



Create a rule

Summary

Service

Calling

Type

Trunk status

Severity ⓘ

High

Title

Calling trunk status alert

Enabled

☒

Target monitoring

You can monitor trunks for callings.

☐ All in-use trunks ☒ Trunk name(s)

Q

Enter user emails separated by commas

LGW-East-HQ1

×

LGW-East-HQ2

×

LGW-East-HQ3

×

3/30 items

Certificate Expiry Alert



Summary

Service	Calling
Type	Call trunks certificate expiry

Severity ⓘ	High
------------	------

Title	Call trunks certificate expiry alert
-------	--------------------------------------

Enabled	☒
---------	-------------------------------------

Delivery Method

By default, all alerts appear in Control Hub.

☒ Email

reyskywalker@theforce.com ✕

yoda@jedimaster.com ✕

caradune@rebels.com ✕

Enter user emails seperated by commas

☒ Webex app space

☐ Space name ⓘ

☐ Space ID ⓘ

☒ 1 to 1 bot ⓘ

Trunk Concurrent call limit Alert



Summary

Service

Calling

Type

Trunk concurrent call limit

Severity ⓘ

High

Title

Trunk concurrent call limit alert

Enabled

☒

Set the sampling interval to determine how often the system checks the percentage of concurrent calls against the threshold. If the percentage exceeds the specified limit (e.g., 70%) during the selected time range, an alert will be triggered.

Target monitoring

You can monitor trunks for callings.

☐ All in-use trunks

☒ Trunk name(s)

LGW-East-HQ1 ×

LGW-East-HQ2 ×

LGW-East-HQ3 ×

3/30 items

Trunk Concurrent call limit Alert

Summary

This rule triggers an alert when the percentage of failed calls exceeds the specified threshold (e.g., 12%) during the selected sample period (e.g., 5 minutes). The system will continuously check this threshold at the set interval and send alerts if it is met or exceeded.

Service

Calling

Type

Call trunks failure rate

Severity ⓘ

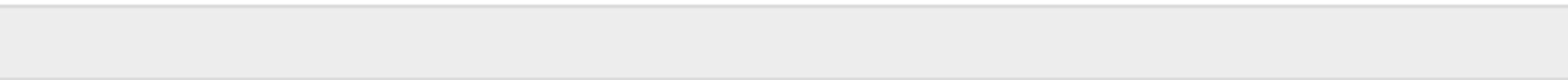
High

Title

Call trunks failure rate alert

Enabled

☒



Target monitoring

You can monitor trunks for callings.

☐ All in-use trunks

☒ Trunk name(s)

Q

Enter user emails separated by commas

LGW-East-HQ1

×

LGW-East-HQ2

×

LGW-East-HQ3

×

3/30 items

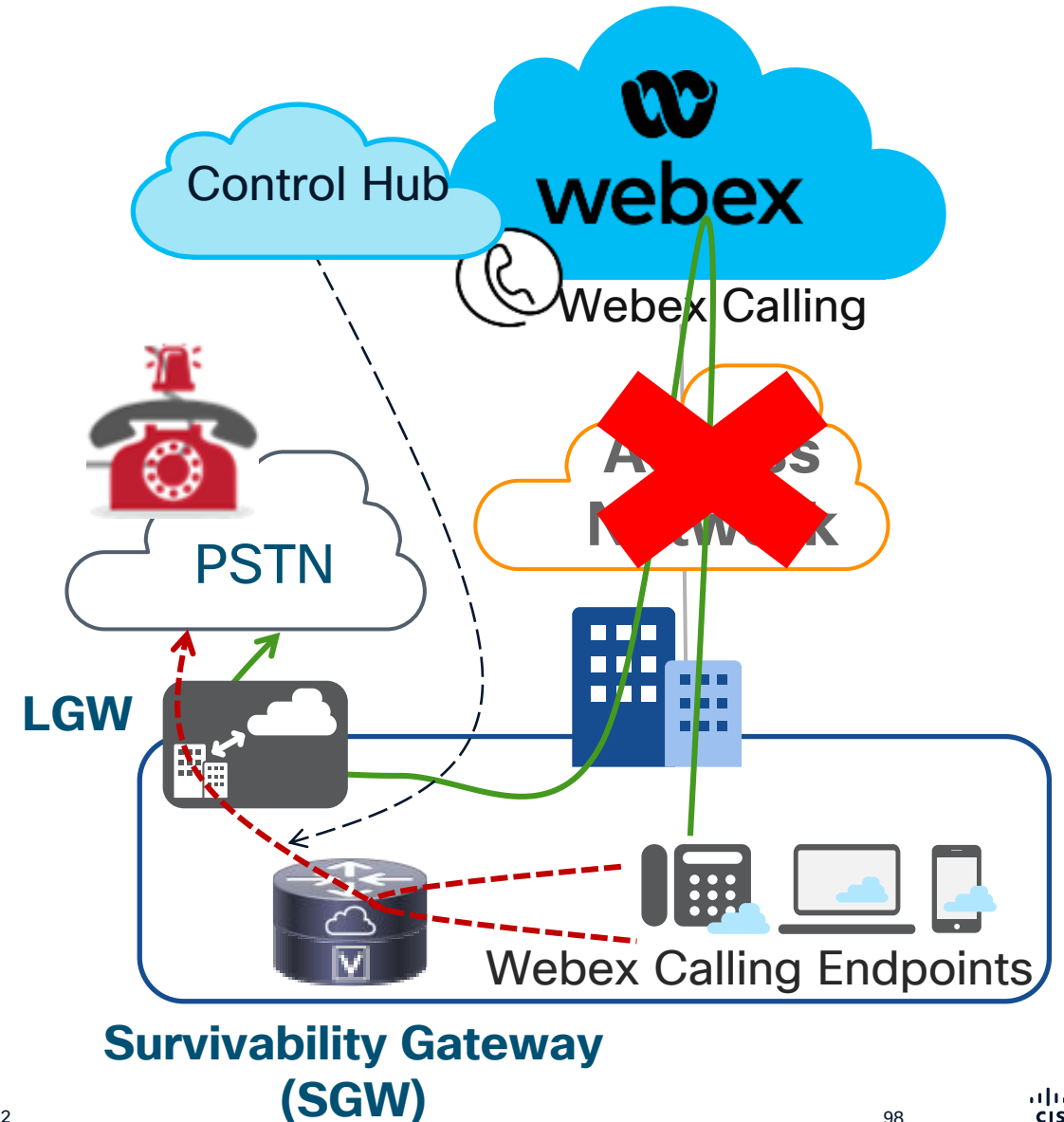
Site Survivability for Webex Calling

Site Survivability Solution Overview

Site Survivability for Webex Calling

- 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, 6841, 6851, 6861, 6861 Wi-Fi, 6871, 7811, 7821, 7841, 7861, 7832, 8832 8811, 8841, 8851, 8861, 8845 (audio only), 8865 (audio only)	12.0(1)
Webex App	Windows, Mac	43.2
Analog Endpoints	VG400, VG410, and VG420	17.16.1a
	ATA191 and ATA192	11.3(1)



Cisco Desk Phone 9800 series,
ATA, VG400 series now
supported



Survivability Gateway (SGW)

Platform Support



Survivability Gateway
(SGW)

- Hardware and software requirements:
 - ISR 4321, 4331, 4351, 4431, 4451 (IOS-XE 17.12.5b)
 - ISR4461 (IOS-XE 17.12.5b)
 - Catalyst 8200/8300 series (IOS-XE 17.12.5b)
 - Catalyst 8000v Edge (vCUBE) (IOS-XE 17.12.5b)



IOS-XE Platform Scale support

Model	Max Registrations
Integrated Services Router 4321	50
Integrated Services Router 4331	100
Integrated Services Router 4351	700
Integrated Services Router 4431	1200
Integrated Services Router 4451-X	2000
Integrated Services Router 4461	2000
Catalyst Edge 8200L-1N-4T	1500
Catalyst Edge 8200-1N-4T	2500
Catalyst Edge 8300-1N1S-6T	2500
Catalyst Edge 8300-2N2S-6T	2500
Catalyst Edge 8300-1N1S-4T2X	2500
Catalyst Edge 8300-2N2S-4T2X	2500
Catalyst Edge 8000V Software – Small/Medium/Large	500 / 1000 / 2000

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
14.7	17.12.1a	July 2023	17.12.5b
14.8	17.13.1a	Nov 2023	
14.9	17.14.1a	March 2024	
14.10	17.15.1a	July 2024	17.15.3a
14.11	17.16.1a	Nov 2024	
TBD	17.18.1a	August 2025	

Last release for
ISR4K except
ISR4461

Note: CSCwk44855 Cannot dial to/from phone after it reboots in survivability mode

Symptom: When phones register to the Survivability Gateway (SGW), phones are successfully registered and can make and receive calls. If a phone gets rebooted, it will register back to the SGW but after 5mins the SGW deletes the AOR entry for the phone. This affects the call routing as the virtual dial-peer is deleted, causing a 404 Not Found SIP Error message since there is no route to the destination extension. Phone cannot dial-out indicating "no line" status.

Fixed Release: IOS-XE 17.12.5a/5b, 17.15.3a/3b, 17.16.1a

Port Reference Information for SGW

Connection Purpose	Source Addresses	Source Ports	Protocol	Destination Addresses	Destination Ports
Call signaling to SGW (SIP TLS)	Devices	5060-5080	TLS	SGW	8933
Call media to SGW (SRTP)	Devices	19560-19660	UDP	SGW	8000-14198 (SRTP over UDP)
Call signaling to PSTN gateway (SIP)	SGW	Ephemeral	TCP or UDP	Your ITSP PSTN gateway	5060
Call media to PSTN gateway (SRTP)	SGW	8000-48198	UDP	Your ITSP PSTN gateway	Ephemeral
Time synchronization (NTP)	SGW	Ephemeral	UDP	NTP server	123
Name resolution (DNS)	SGW	Ephemeral	UDP	DNS server	53
Cloud Management	Connector	Ephemeral	HTTPS	Webex services	443, 8433

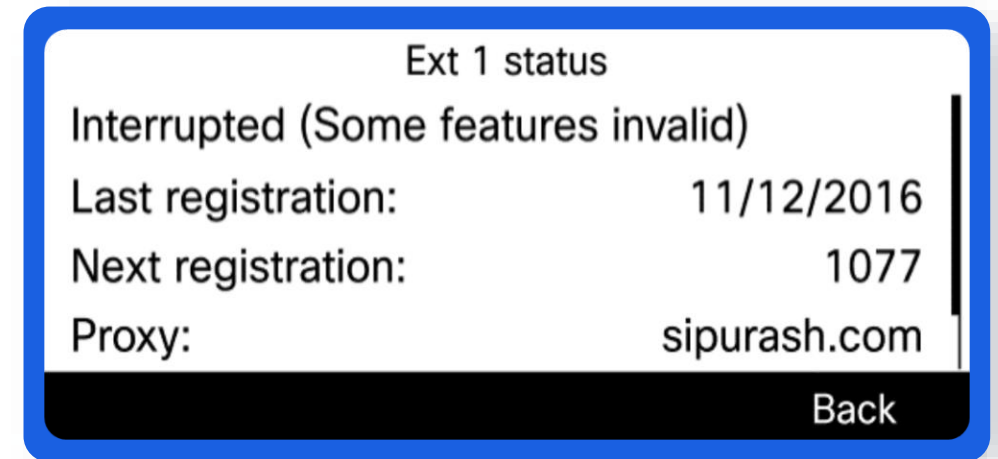
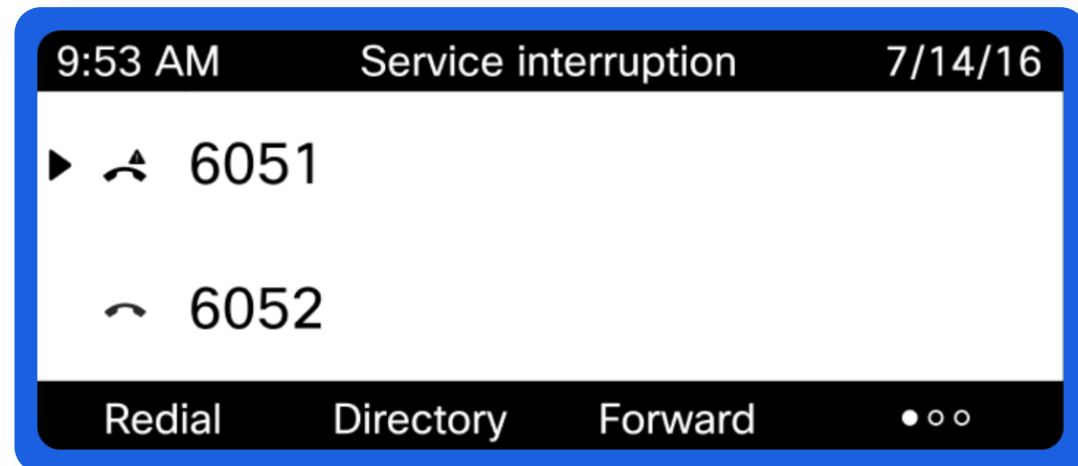
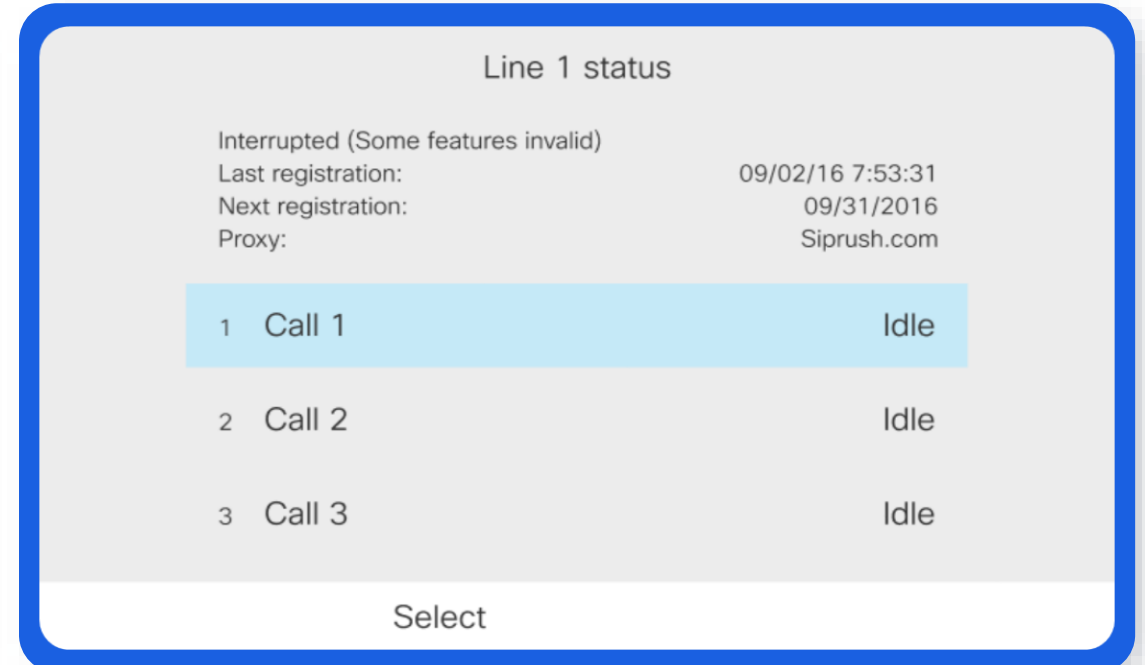
Survivability zones

- Currently, survivability sites are aligned with “locations” in Webex Calling
- Each Survivability Gateway is associated to a specific location (1:1)
- All supported devices added to that location are configured to use that gateway, in the event of an outage
- The SGW is automatically provisioned with registration details for users/devices for its location
- No manual assignment of users to survivability zone is required
- **Multiple Locations per SGW coming soon**

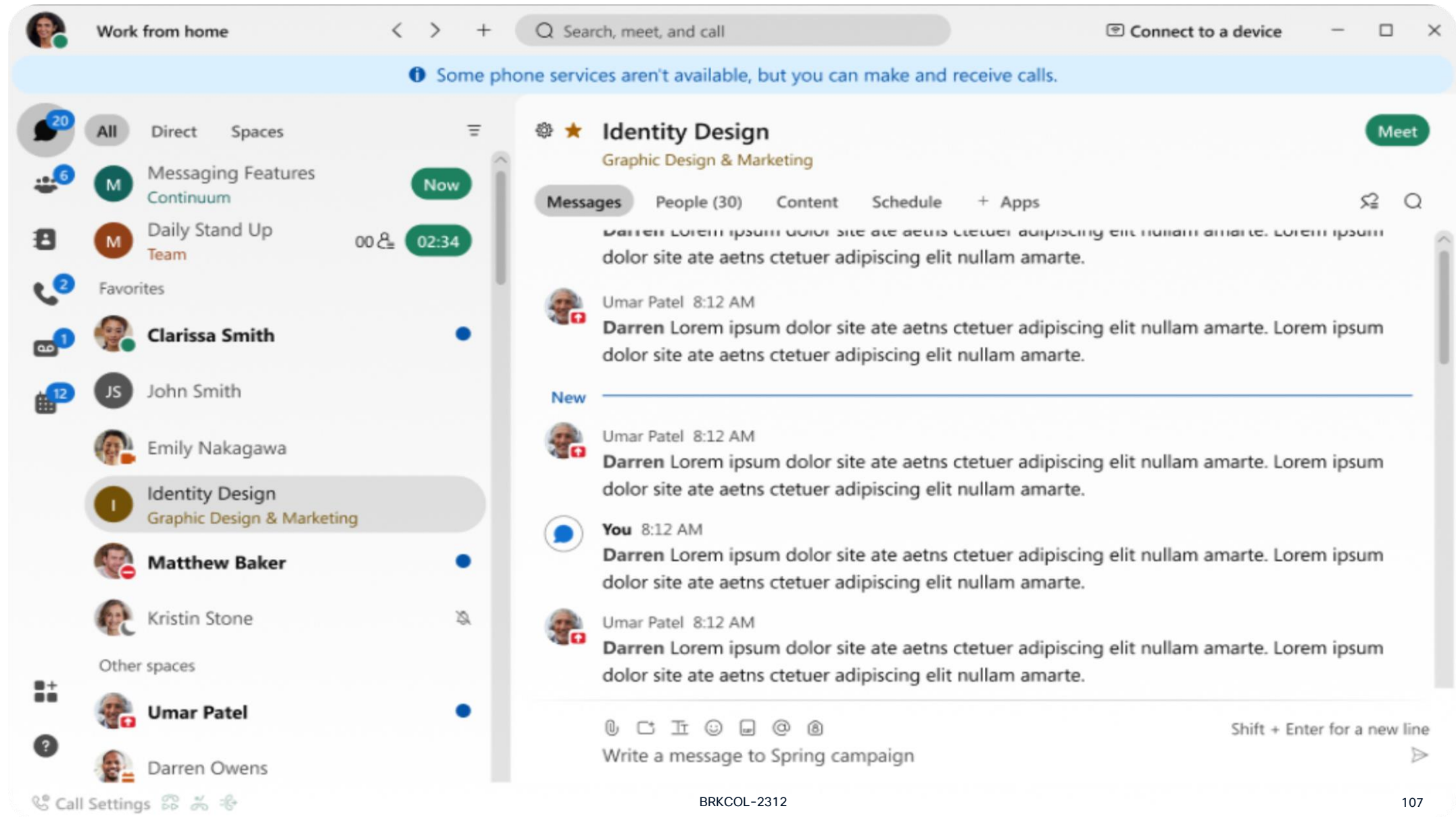


Webex App and endpoint changes

Interface Design – IP Phones



Interface Design – Webex Desktop App



Test mode in the Webex App

Health Checker

You're connected to the internet.

☒ Turn on Survivability Test Mode

 Server connection Test	 All services are accessible	Services impacted Everything looks good here!
 Cloud Refresh	 Operational	Information taken from status.webex.com
 Phone services Test	 Softphone connected	

Call Forward Unreachable Setting

Updated Call Forward Unreachable option

Hussain Ali



- Active • hussain@wxcsa.wbx.ai • Member of Cisco Atlanta Office
- Member of Cisco Atlanta Office

Action ▾

Profile General Meetings **Calling** Messaging Hybrid Services Devices Vidcast

< Calling

Call forwarding

Transfer or forward outgoing calls to another phone number or directly to voicemail. Note that custom user settings override these settings.

- ☐ Forward all calls
- ☐ Forward calls during busy lines
- ☐ Forward calls when unanswered
- ☐ Forward calls if the network is disconnected ⓘ

Updated Call Forward Unreachable option

Call forwarding

Transfer or forward outgoing calls to another phone number

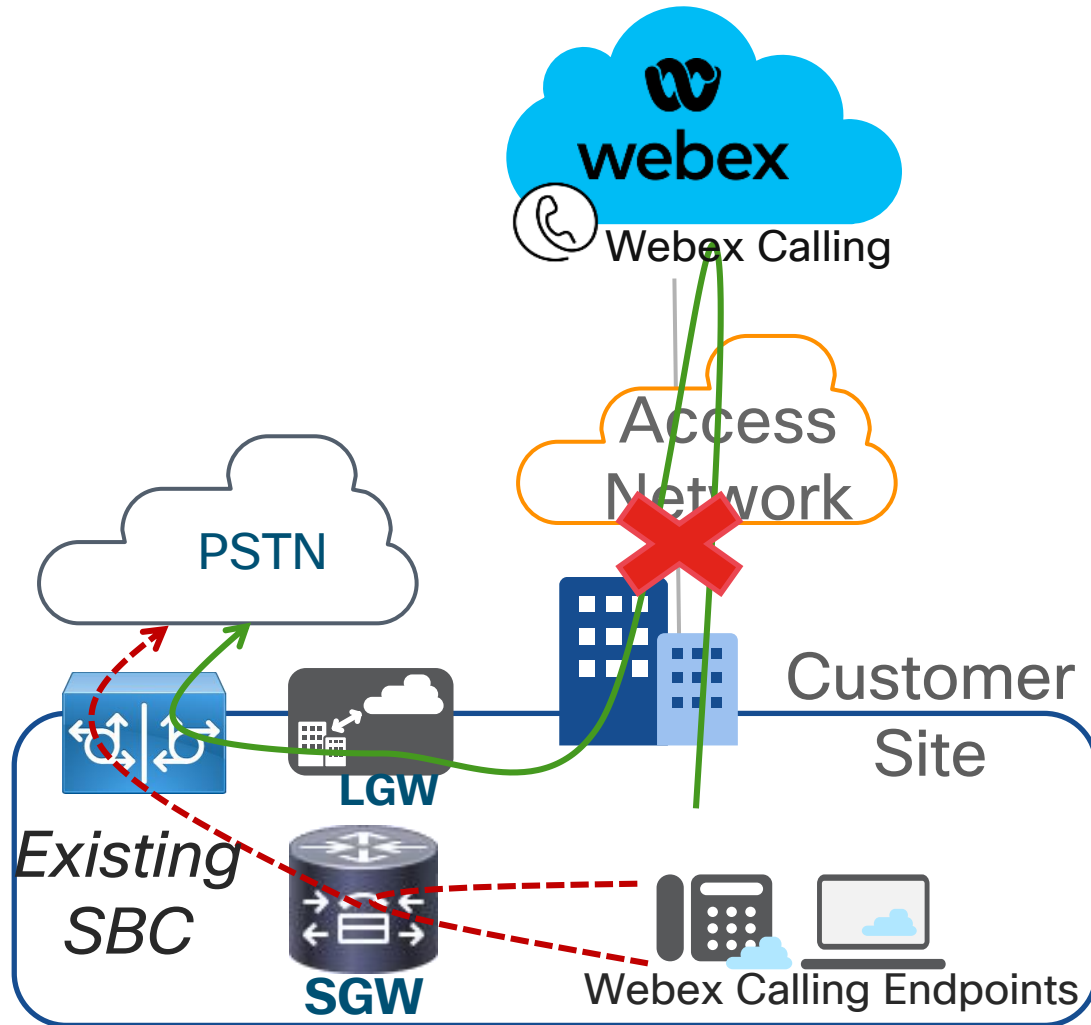
- ☐ Forward all calls
- ☐ Forward calls during busy lines
- ☐ Forward calls when unanswered
- ☒ Forward calls if the network is disconnected ⓘ

Forward calls to this phone number

- ☐ Allow forwarded calls to leave voicemail ⓘ

Survivability Call Flows

Site Survivability for Webex Calling – Single Site

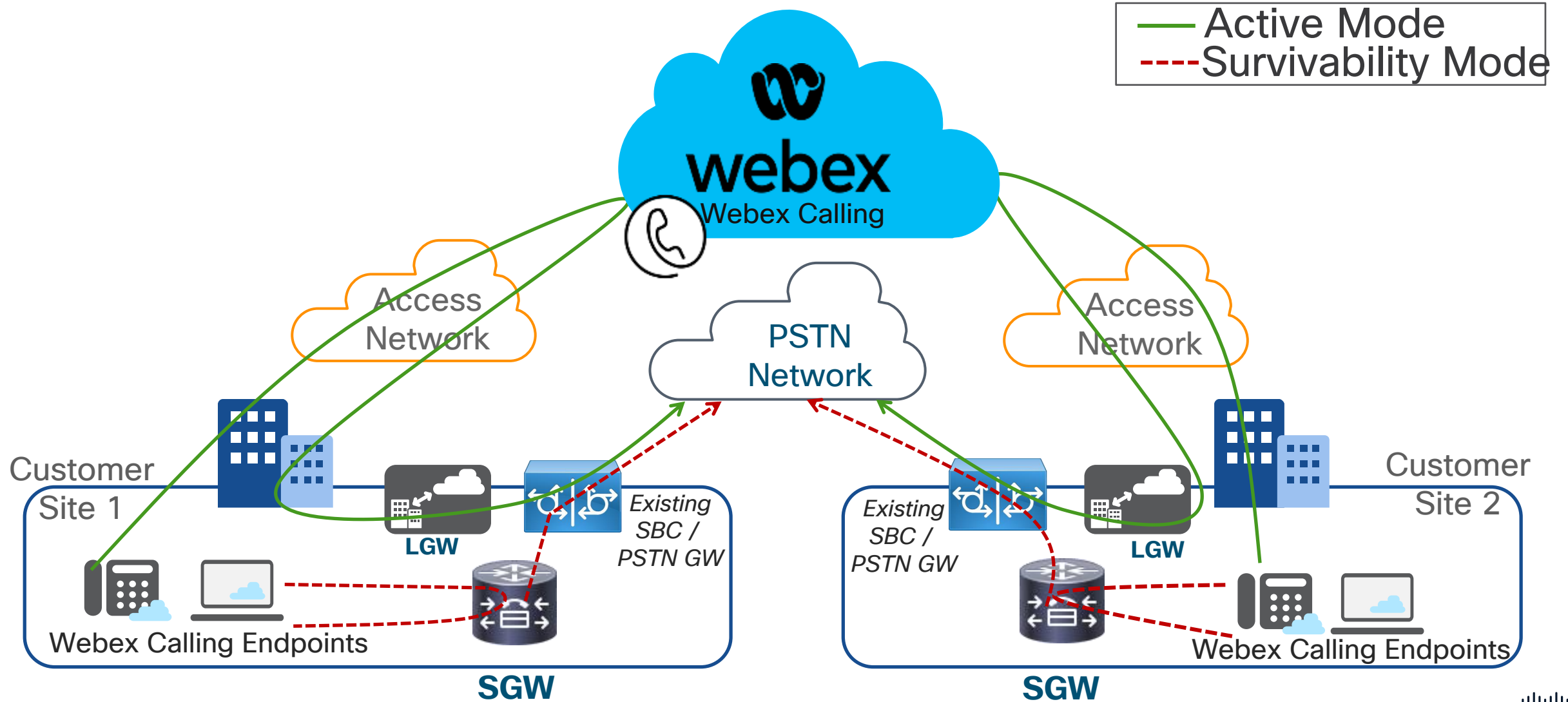


Survivability Mode

- Extension basic dialing
- Outbound/Inbound calls via local PSTN Gateway
- Config default trunk towards PSTN gateway



Site Survivability for Webex Calling - Multi Site

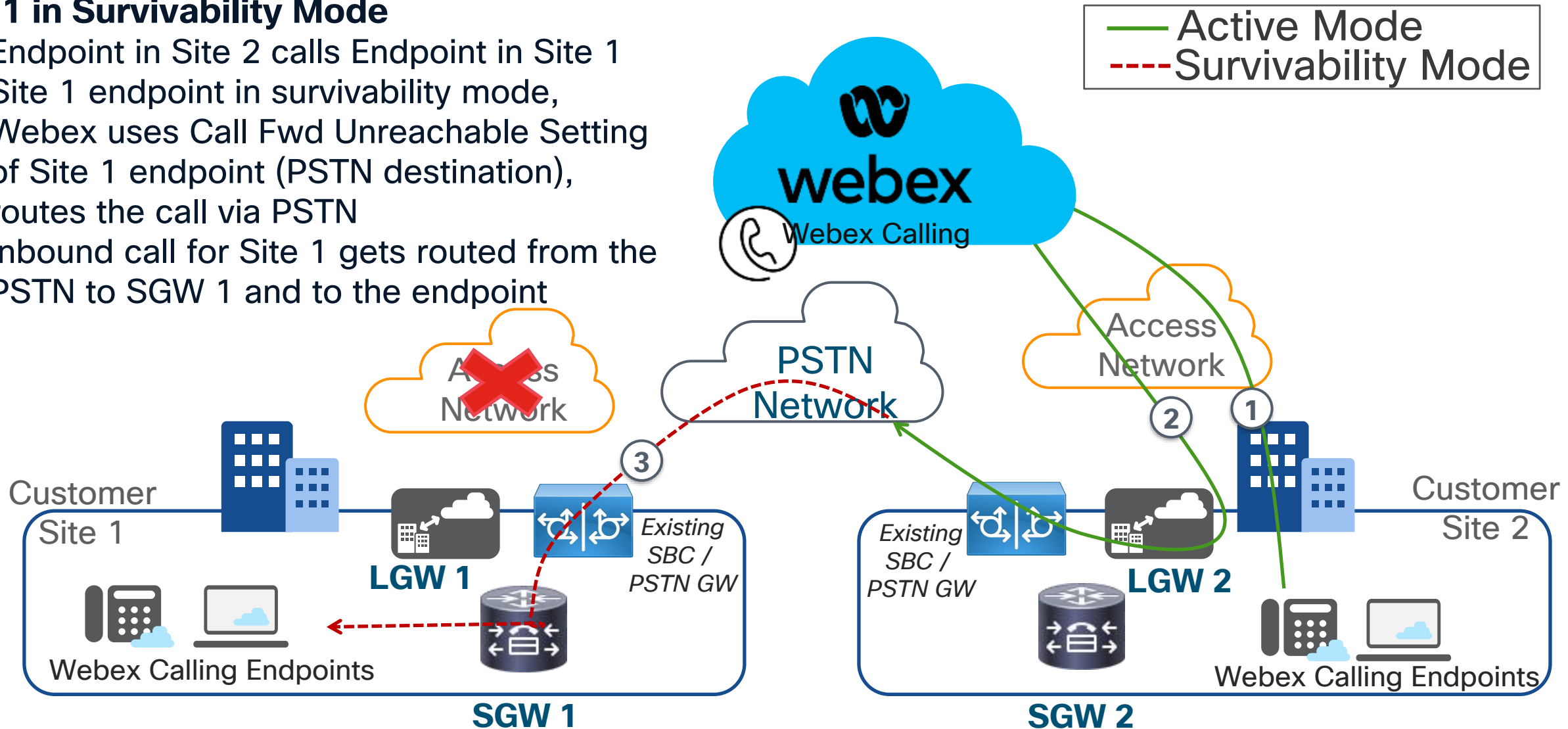


Site Survivability for Webex Calling

Inter site call routing Active Mode Site to Survivability Mode Site

Site 1 in Survivability Mode

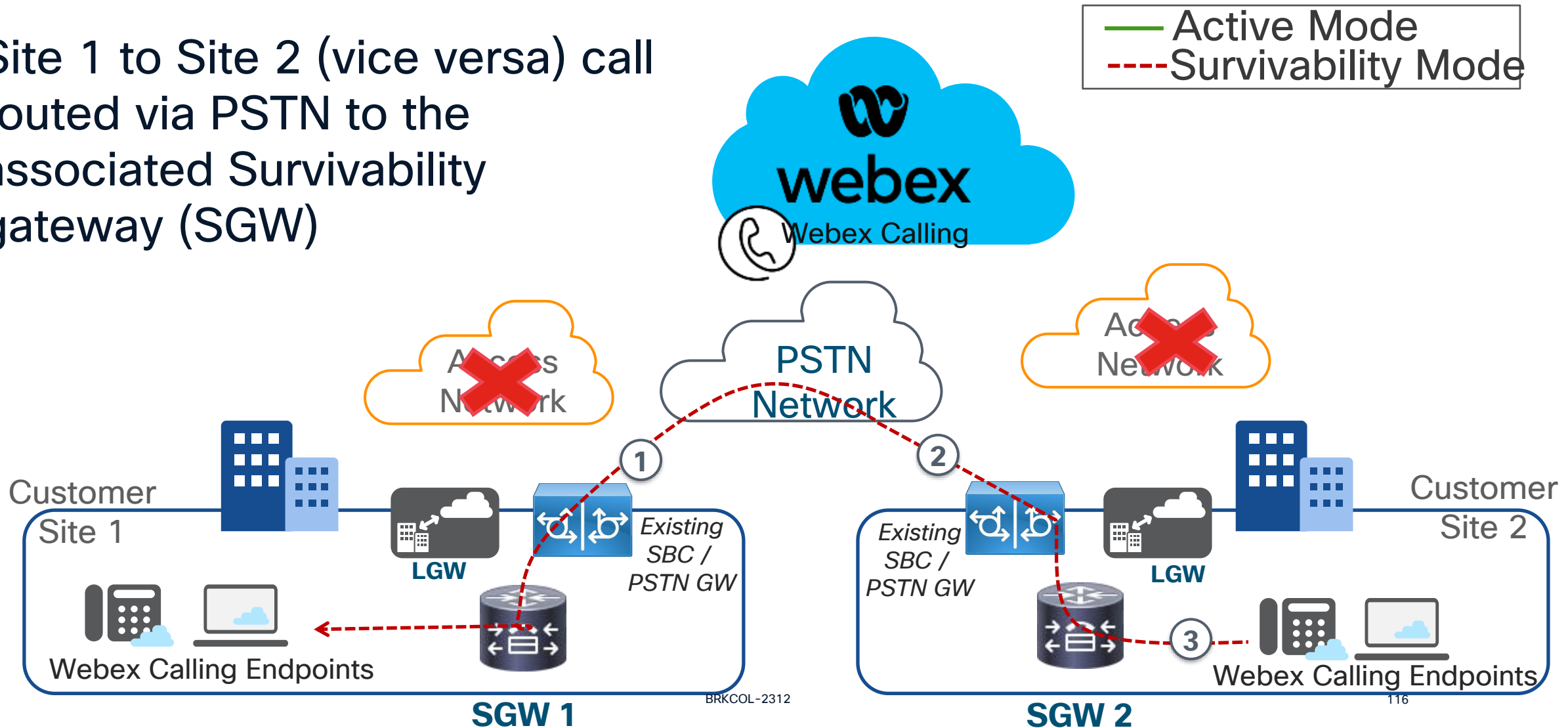
1. Endpoint in Site 2 calls Endpoint in Site 1
2. Site 1 endpoint in survivability mode, Webex uses Call Fwd Unreachable Setting of Site 1 endpoint (PSTN destination), routes the call via PSTN
3. Inbound call for Site 1 gets routed from the PSTN to SGW 1 and to the endpoint



Site Survivability for Webex Calling

Inter site call routing Active Mode Site to Survivability Mode Site

Site 1 to Site 2 (vice versa) call routed via PSTN to the associated Survivability gateway (SGW)



Site Survivability Deployment Workflow

Site Survivability Prerequisite

- IOS-XE Gateway, that is, SGW should be connected to Cisco Webex Control Hub as mentioned in the below onboarding connector document
- <https://help.webex.com/en-us/article/xftgfc/Enroll-Cisco-IOS-Managed-Gateways-to-Webex-Cloud>

Managed Gateway is a must for deploying an SGW

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 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

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

< Managed Gateways

Hussain-Cat8kv

Actions ▾

● Connector Online • Version 17.9.20221213



Assign Service

Assign the Webex Calling service that you will be using your gateway for.

Assign Service

Service Type: LGW or SGW

Assign Service to Hussain-Cat8kv

Select the Webex Calling service that you will be using your gateway for.

Select service type

Local Gateway

Survivability Gateway

Cancel

Assign

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

Assign Service to Hussain-Cat8kv

Select the Webex Calling service that you will be using your gateway for.

Survivability Gateway

Each gateway provides survivability services for one Webex Calling location. Select the location at which this gateway is installed and provide the hostname used in the trustpoint certificate and the IP address to which clients will register.

Note: Clients will not be able to failover until they receive these Survivability Gateway details with their next provisioning event.

Location

Cisco Atlanta Office

Host Name ⓘ

sbc2.tmedemo.com

IP Address ⓘ

10.52.12.203

Cancel

Assign

Endpoint Config update

Assign Service to Hi

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 ti
provisioning event.

Location

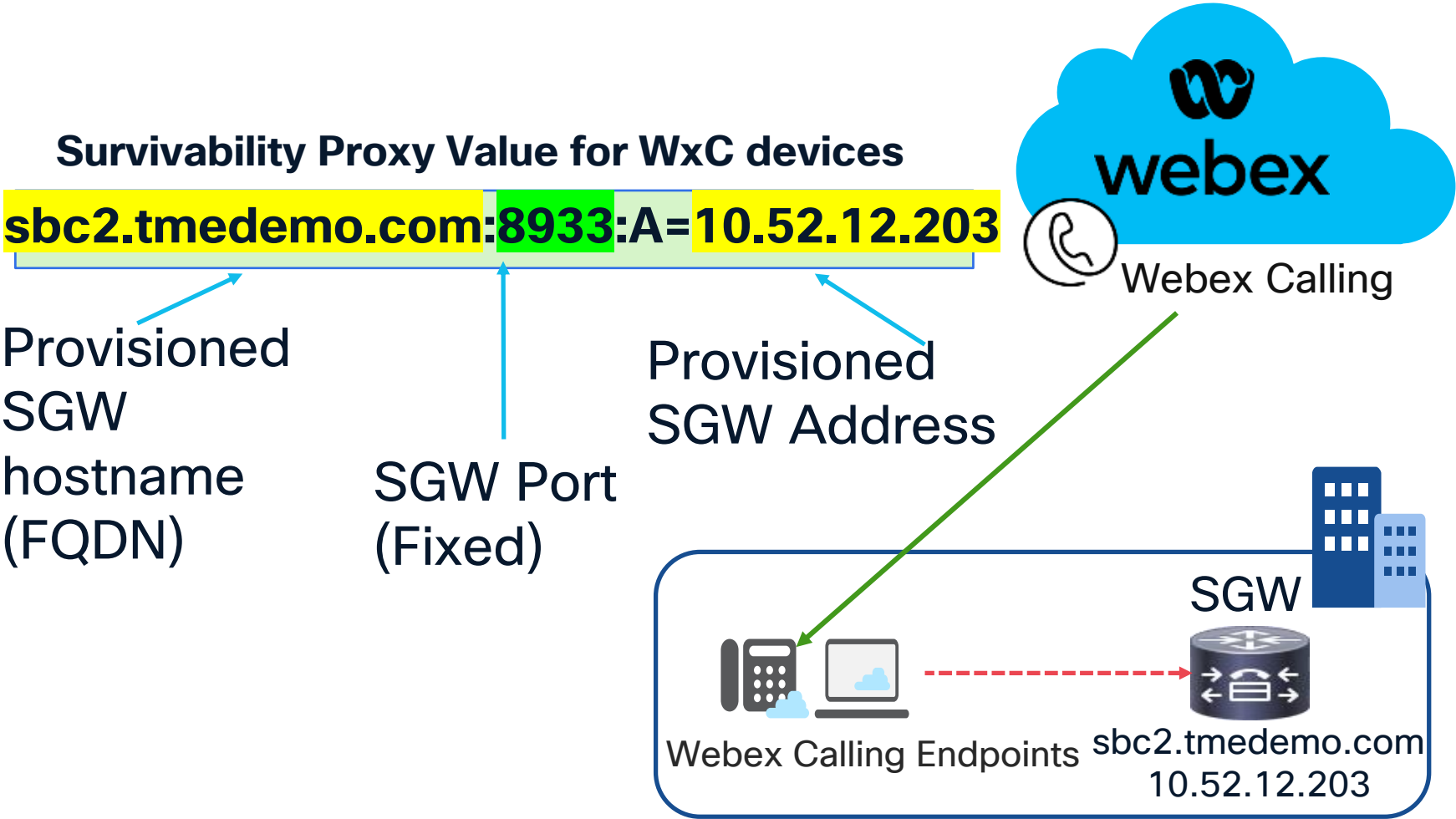
Cisco Atlanta Office

Host Name ⓘ

sbc2.tmedemo.com

IP Address ⓘ

10.52.12.203



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.

< Managed Gateways

Hussain-Cat8kv

Actions ▾

● Connector Online • Version 17.9.20221213:174319

Survivability Service

Location	Cisco Atlanta Office
Host Name	sbc2.tmedemo.com
IP Address	10.52.12.203
Last Data Sync ⓘ	-
Last Successful Data Sync ⓘ	-

Edit

Sync

Download config template

Dial-peer voice summary

SGW#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
100	voip	up	up				0	syst		
101	voip	up	up		+1408944....\$		0	syst	ipv4:198.18.133.3	
201	voip	up	up		81[2-9]..[2-9]..-		0	syst	ipv4:10.1.40.11	
1050	voip	up	up		999		0	syst	ipv4:198.18.133.186	
40001	voip	up	up		+14085551074\$		0	syst	ipv4:198.18.133.39:5	
40002	voip	up	up		+14085557700\$		0	syst	ipv4:198.18.133.38:5	

Dynamic (Virtual) dial-peers are setup for SIP SRST/SGW endpoints when they register to the SRST/SGW platform

```
dial-peer voice 40001 voip
destination-pattern pjkj1ffadg$
redirect ip2ip
session target ipv4:198.18.133.39:5074
session protocol sipv2
dtmf-relay rtp-nte
digit collect kpml
voice-class codec 1
after-hours-exempt FALSE
```

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
```

Received:

INVITE sip:1341@<CUBE-IP> SIP/2.0

Sent:

INVITE sip:1341@10.1.1.3 SIP/2.0

Outbound DP is
selected based on
preference listed
in DPG only

```
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
!
```

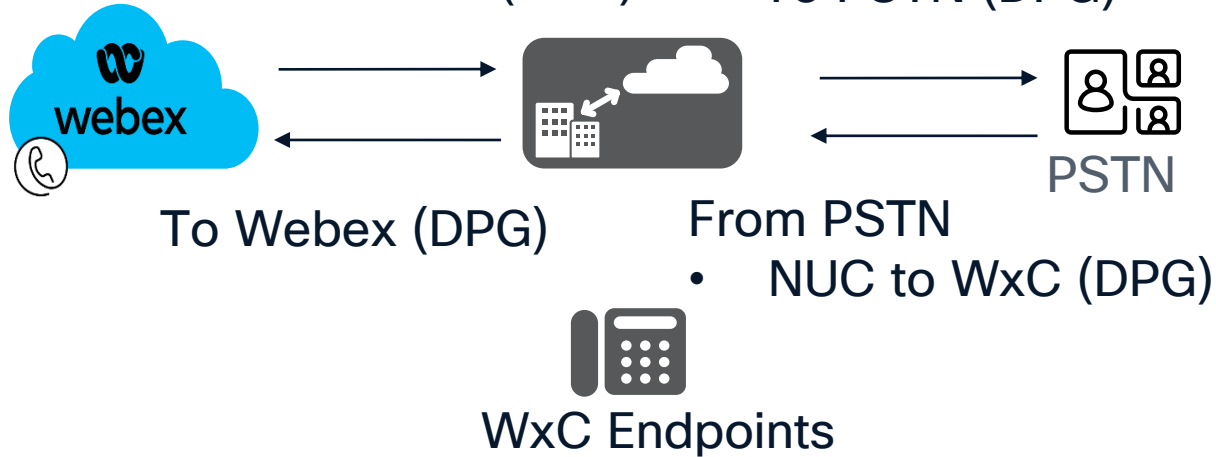
```
dial-peer voice 1003 voip
destination-pattern 4444
session protocol sipv2
session target ipv4:10.1.1.3
```

Call Routing Overview – Existing LGW and SGW Operation

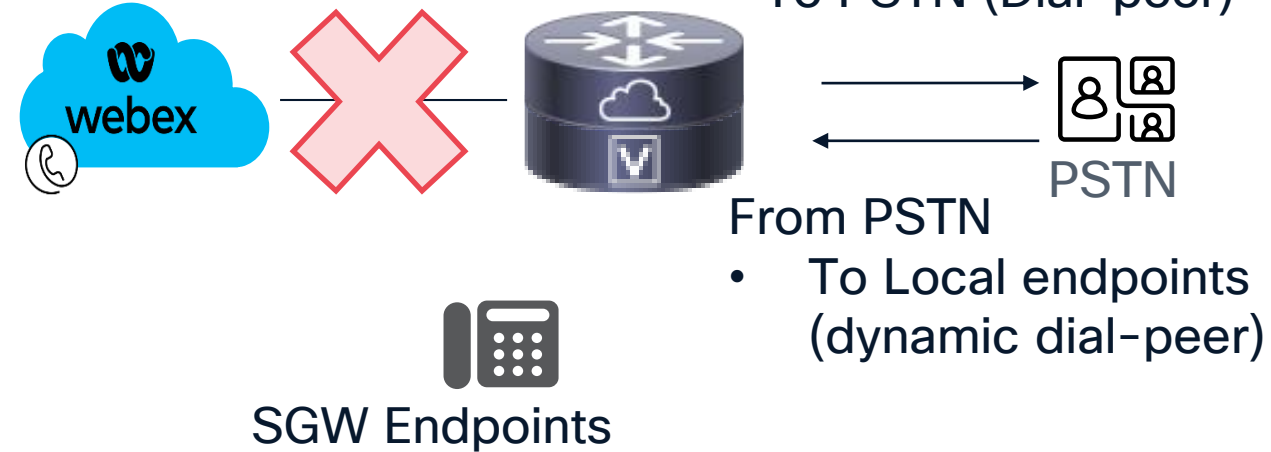
From Webex

- NUC to PSTN (DPG)

To PSTN (DPG)



To PSTN (Dial-peer)



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

Co-located LGW and SGW config summary

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

```
dial-peer voice 101 voip
  description Outgoing to IP PSTN
  destination-pattern .T
  preference 3
```

→ Replace BAD.BAD with .T
→ Add preference 3



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

→ Replace BAD.BAD with .T
→ Add preference 2

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

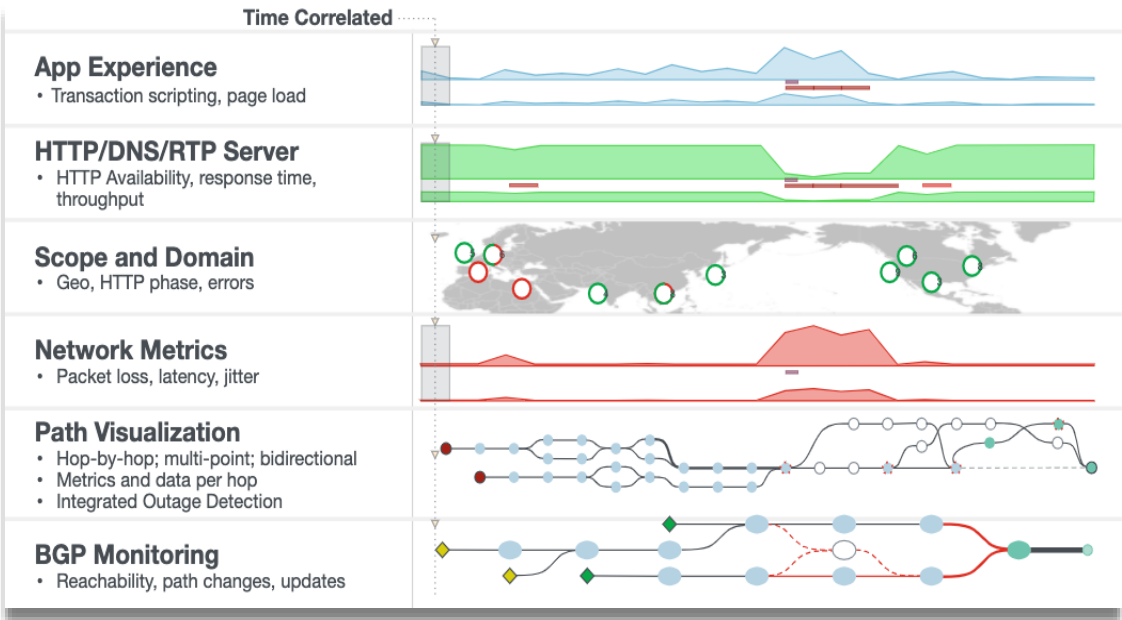
```
dial-peer voice 100 voip
  description Incoming from IP PSTN
  incoming uri via 100
  destination dpg 200
```

→ Remove destination dpg 200 from inbound ITSP dial-peer to allow operation in SGW mode

Thousand Eyes

ThousandEyes – Delivering Network Intelligence

A SaaS based I/internet and cloud intelligence solution



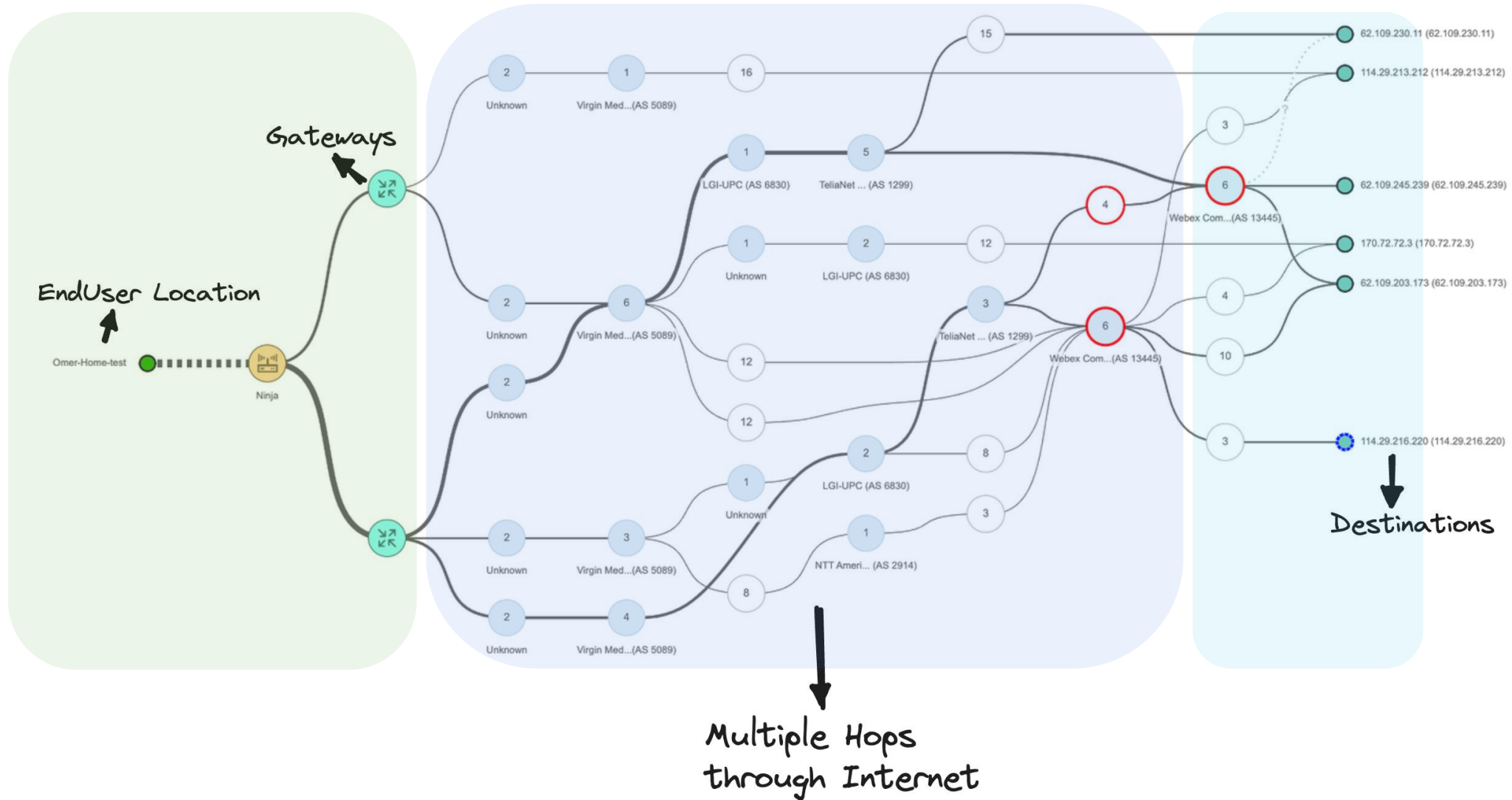
Superior Network Experience

Collective Intelligence

Interactive Collaboration

ThousandEyes - Delivering Network Intelligence

A SaaS based I/internet and cloud intelligence solution



ThousandEyes - Agent Types

ThousandEyes Agents



 Cloud Agents

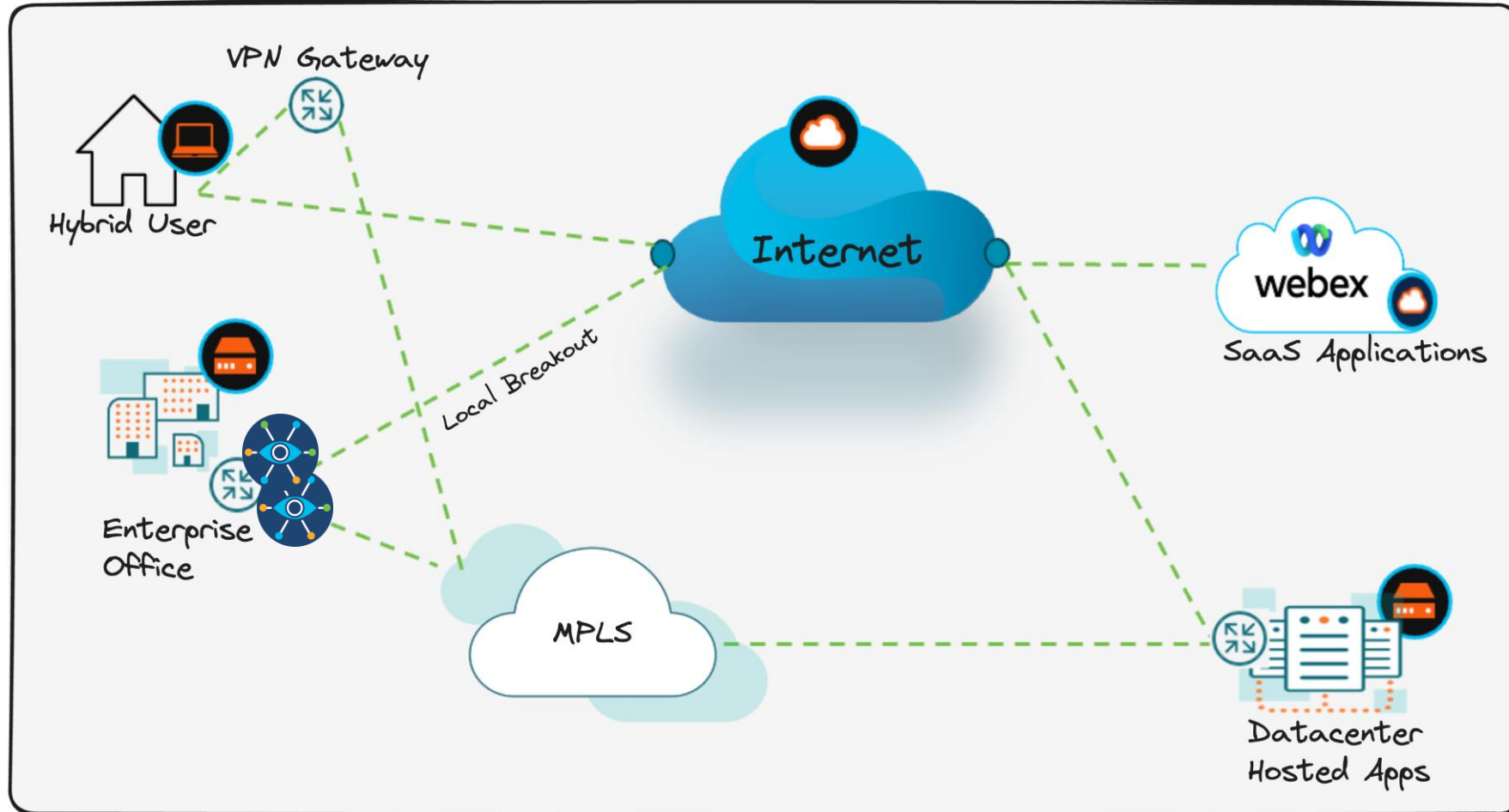
 Enterprise Agents

 Endpoint Agents

Agents / Vantage Points

Enterprise Agents

Enterprise Agents – Monitoring Internal and External Networks



Enterprise Agents + Cube

Pre-Requisites

- Enterprise Agent can be installed on the Cisco router, using one of three available methods
 1. SDWAN Manager Feature Template
 2. SDWAN Manager TE workflow
 3. Using Docker
- Both SD-WAN and Autonomous mode are supported.
- Min IOS version IOS-XE 17.6.1 or later
- The filename structure for ThousandEyes agent images is:

`thousandeyes-enterprise-agent-aarch64-5.0.1.cisco.tar`

↑
Architecture
Version

[Catalyst Switching](#) [Nexus Switching](#) [Catalyst Routing](#) [NFV Infrastructure Software](#)

Catalyst Routing

[View Supported Platforms](#)

Device Architecture

x86_64

aarch64

Hardware

aarch64 Configuration Parameters

App ID

Enter application name

Agent Hostname (Optional)

Enter name

Network Configuration

Static

DHCP

VLAN ID

Number between 0 - 4095

Name Server IP

e.g. 192.168.55.161

IP Address

e.g. 192.168.55.161

Gateway IP (Optional)

e.g. 192.168.55.161 (Optional)

Netmask

Enter Netmask number

Gateway IP

e.g. 192.168.4.1

Copy, adapt, and run the following commands:

```
Device> enable
Device# app-hosting install appid DESIRED_APP_ID package https://downloads.thousandeyes.com/enterprise-agent-aarch64-5.0.1.cisco.tar
Device# configure terminal
Device(config)# app-hosting appid DESIRED_APP_ID
Device(config-app-hosting)# app-vnic gateway1 virtualportgroup 0 guest-interface 0
Device(config-app-hosting-gateway0)# guest-ipaddress DESIRED_IP netmask DESIRED_NETMASK
Device(config-app-hosting-gateway0)# exit
Device(config-app-hosting)# app-default-gateway GATEWAY_IP guest-interface 0
Device(config-app-hosting)# name-server0 NAMESERVER1_IP
```

Verification of Agents Installation

```
router# sh app-hosting list ←
App id                               State
thousandeyes_enterprise_agent       RUNNING ←
```

```
router#sh app-hosting detail appid thousandeyes_enterprise_agent
App id : thousandeyes-enterprise-agent
Owner : iox
State : RUNNING
Application
  Type : docker
  Name : ThousandEyes Enterprise Agent
  Version : 5.0.1
  Description : Perform active synthetic measurements to your business-critical
  Author : ThousandEyes support@thousandeyes.com
  Path : https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enter
  URL Path : bootflash:./thousandeyes-enterprise-agent-x86_64-5.0.1.cisco.tar
  Activated profile name : custom

Resource reservation
  Memory : 500 MB
  Disk : 1 MB
  CPU : 1850 units
  CPU-percent : 9 %
  VCPU : 1

Platform resource profiles
  Profile Name          CPU(unit) CPU(percent)  Memory(MB)  Disk(MB)
  -----
Attached devices
  Type          Name          Alias
  -----
  serial/shell  iox_console_shell  serial0
  serial/aux    iox_console_aux    serial1
  serial/syslog iox_syslog         serial2
  serial/trace  iox_trace         serial3

Network interfaces
  -----
eth0:
  MAC address      : 52:54:dd:e9:9e:9f
  IPv4 address     : 172.29.1.11
  IPv6 address     : ::
  Network name     : VPG0
```

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

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 2026.



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

Thank you

CISCO Live !

