Voice Media for Webex CC

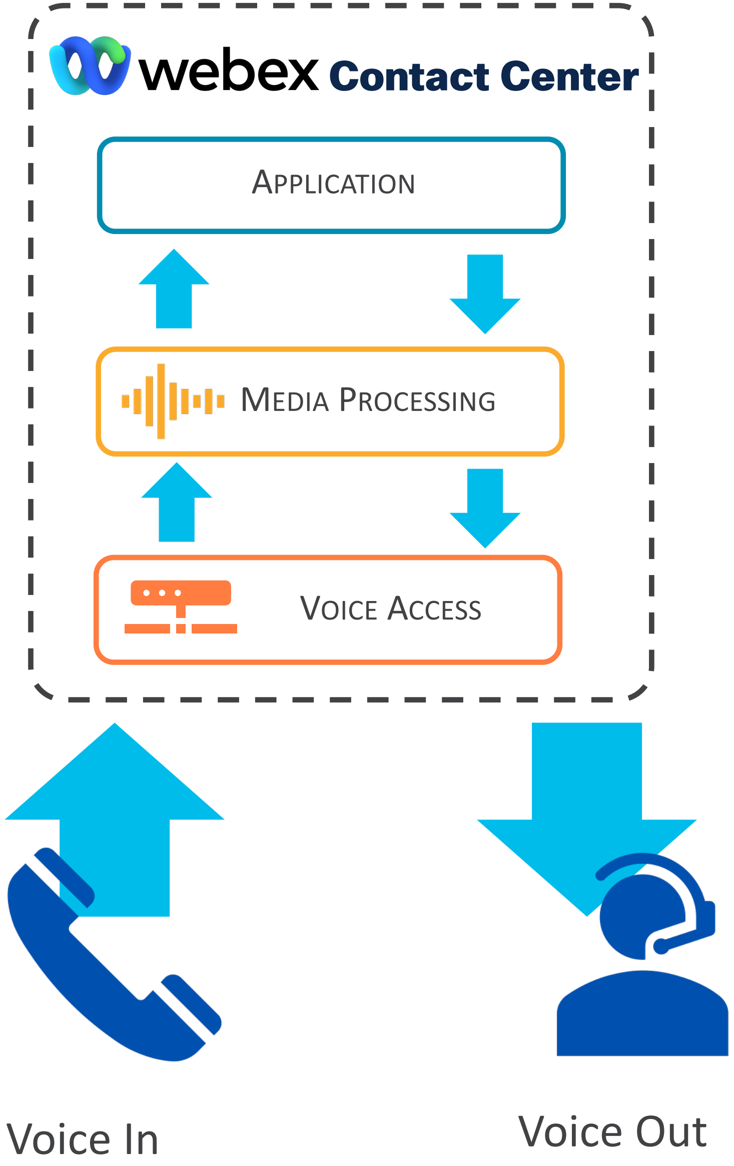
Advanced (US)

Kal Gouda
Rohit Harsh

March 2024

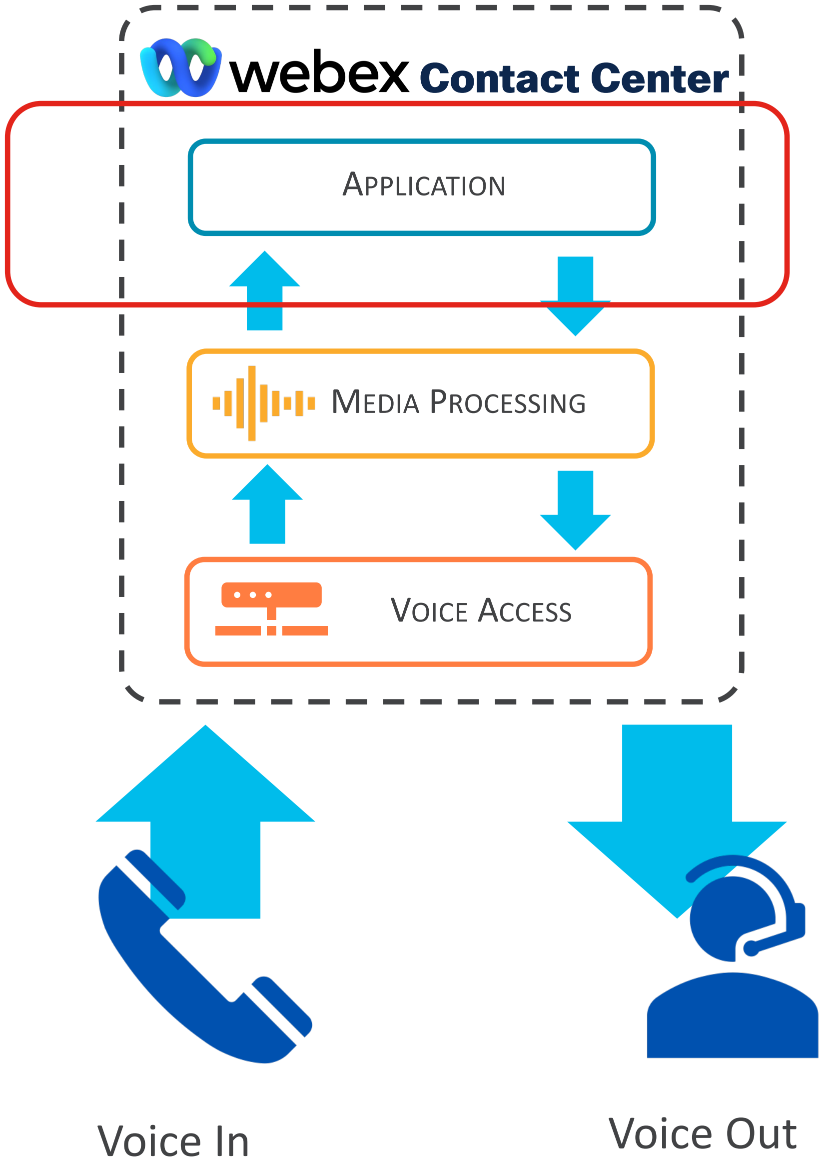
Foundation (Recap)

High level Architecture



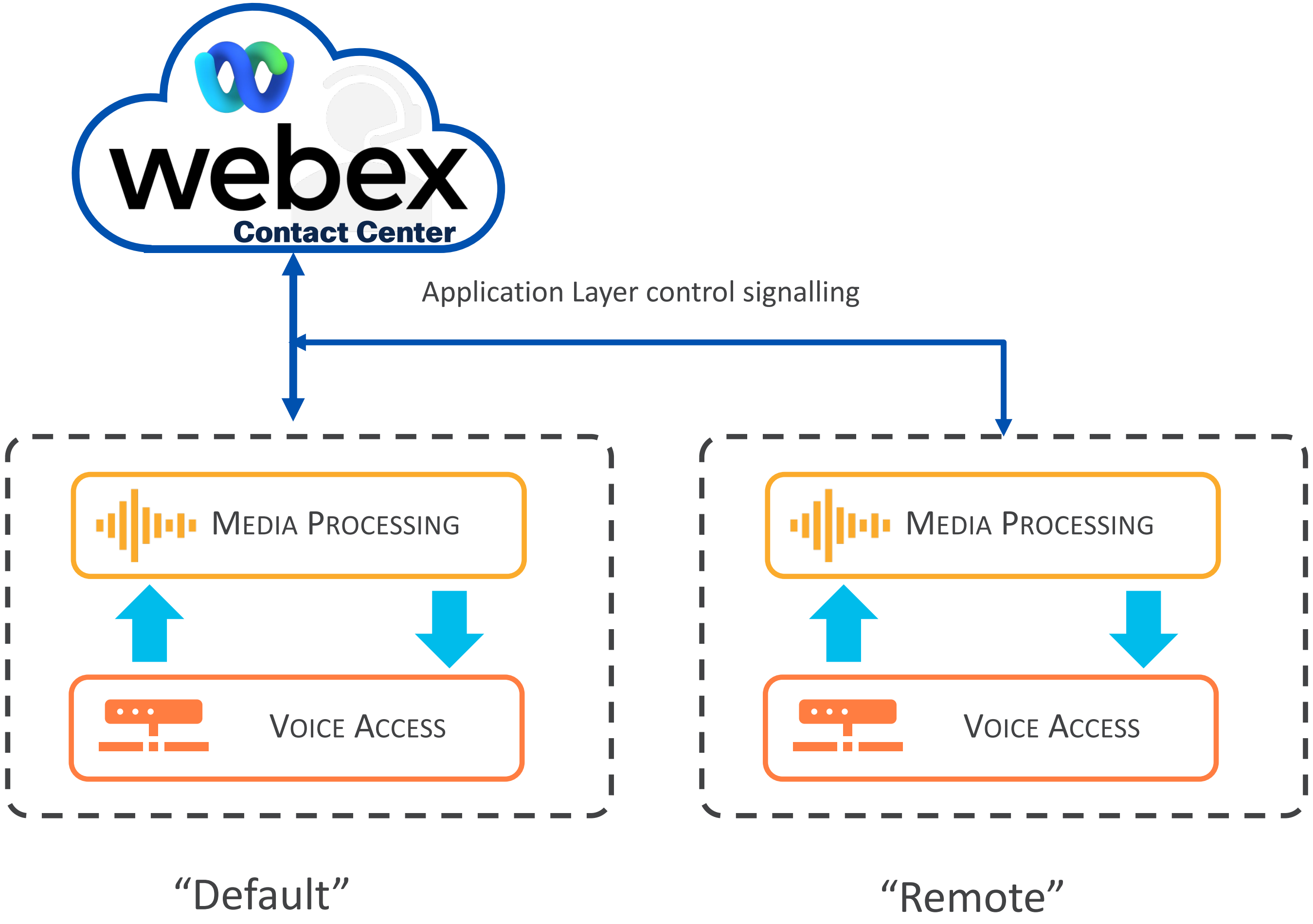
- Application Layer
  - Business Logic, Routing, Queuing, Flows and Agents management
- Media Processing Layer
  - Voice termination, Signalling Media playout, capture input, AI Harness, BNR, agent connection and call recording
- Voice Access Layer
  - Customer Premise AND SP Voice connections
  - VPOP (Direct SIP Trunk) OR Webex Calling

Application Data Center Home Region



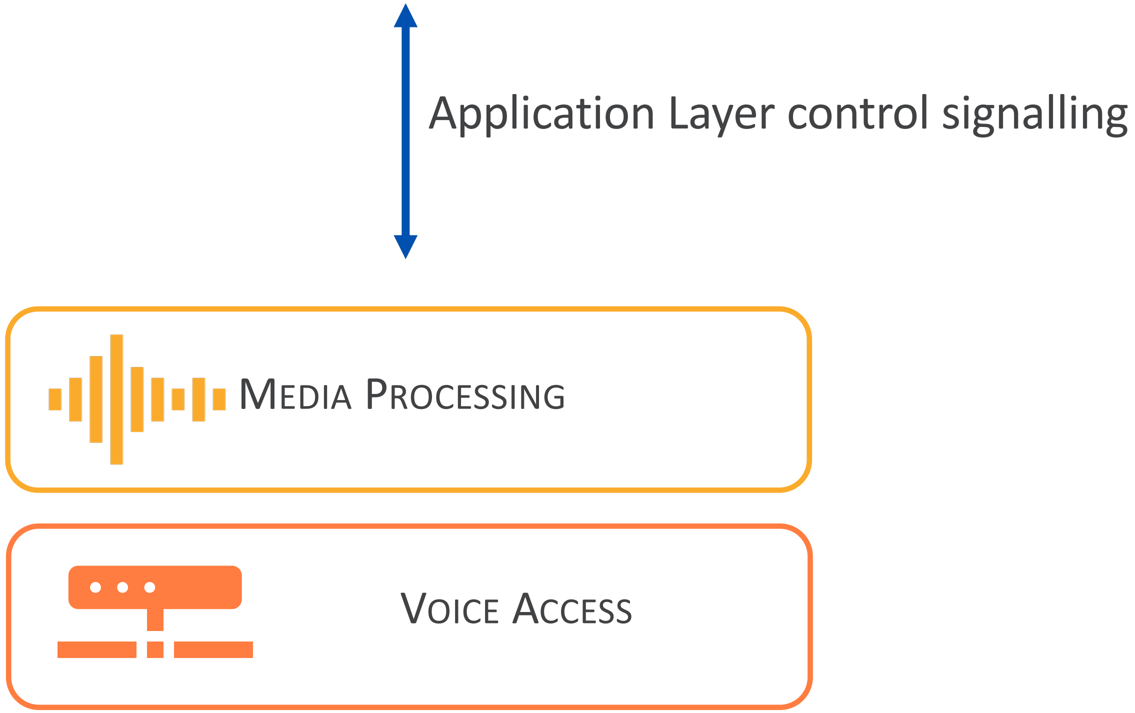
- Also known as **Tenant location** or **Tenant Region**
- Region where the **Application Layer** is deployed
- Each Home Region has a **Default Media Processing Layer** and **Voice Access Layer**
- **Customer Data** is stored in the Home Region
- **Voice Access Layer (VPOP or WxCalling/Media POP)** is selected at deployment time

PSTN Region



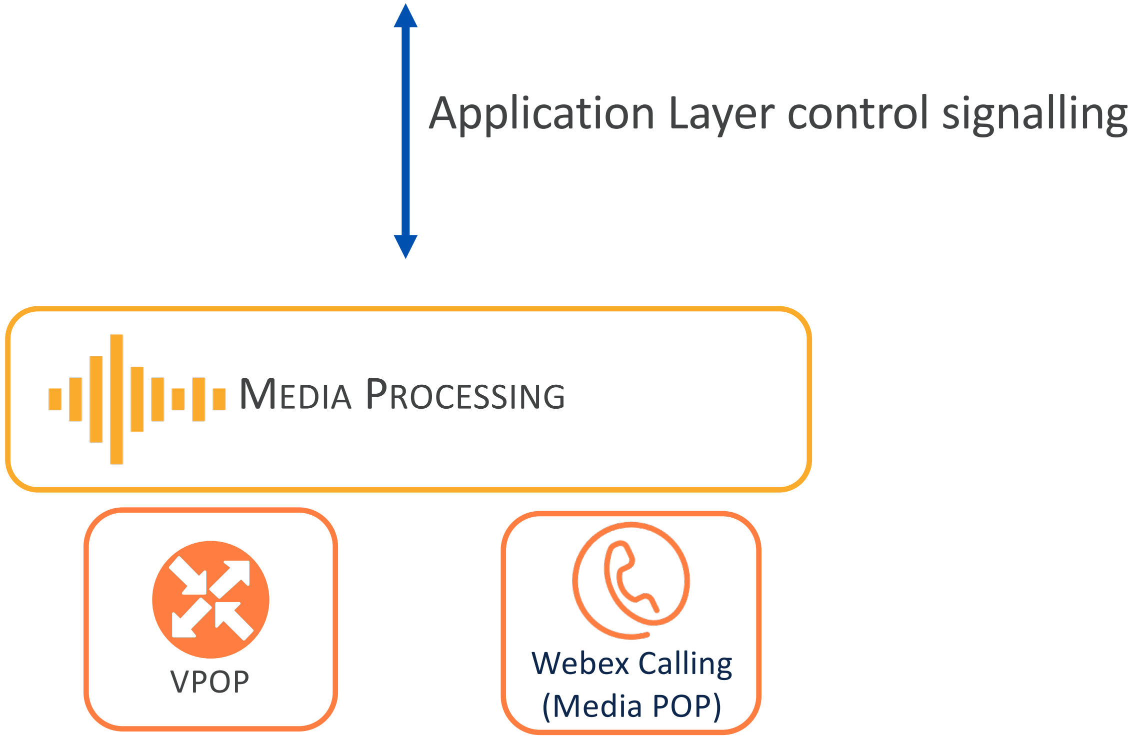
- Also known as **Remote Region** or **Remote PSTN Region**
- **Archors media in-region** during **IVR** and **agent** call legs
- Records calls in-region
- Communicates with Home region for **call routing decisions**
- Only has **Media Processing Layer** and **Voice Access Layer**

Voice Access Layer

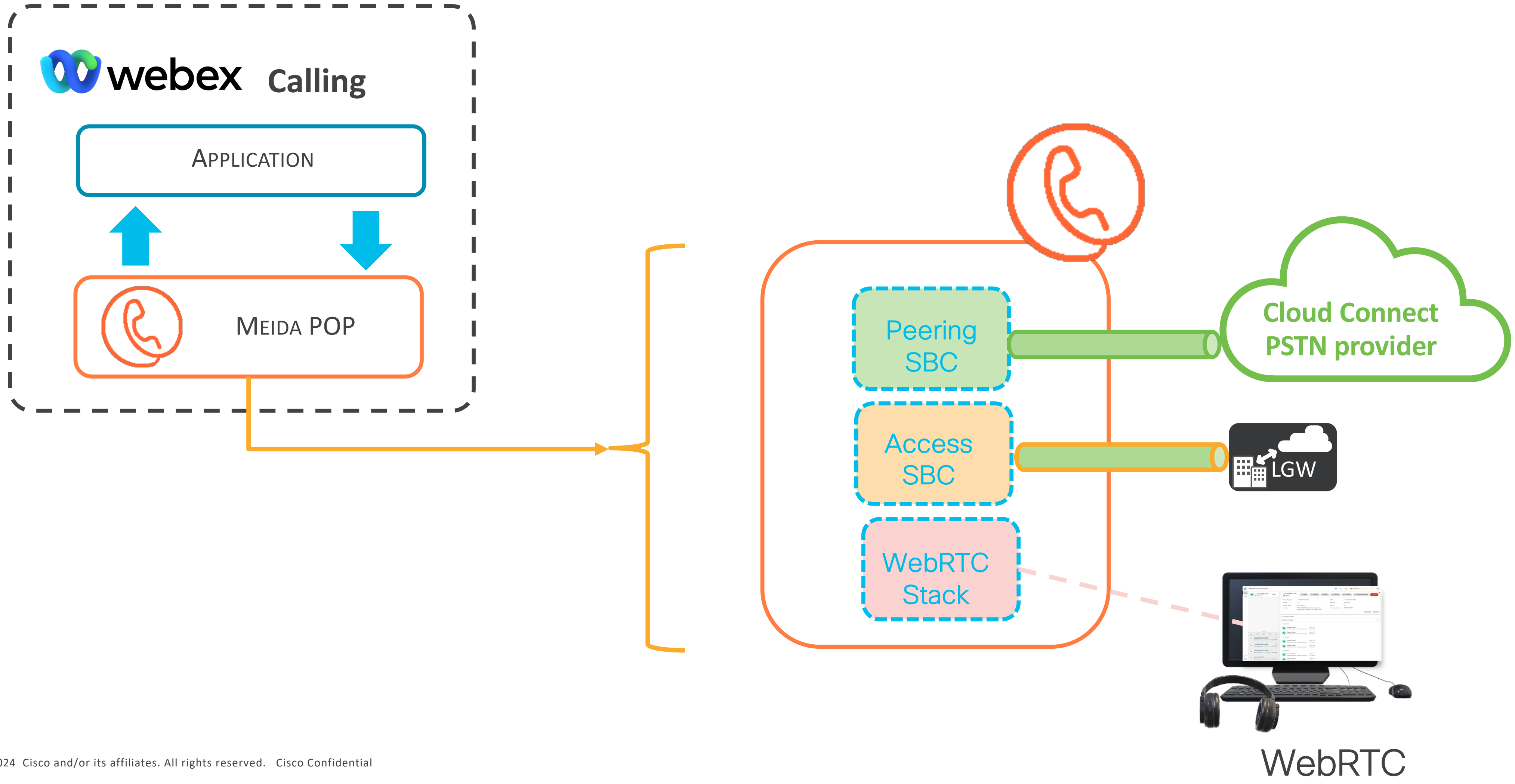


2 **mutually exclusive** options

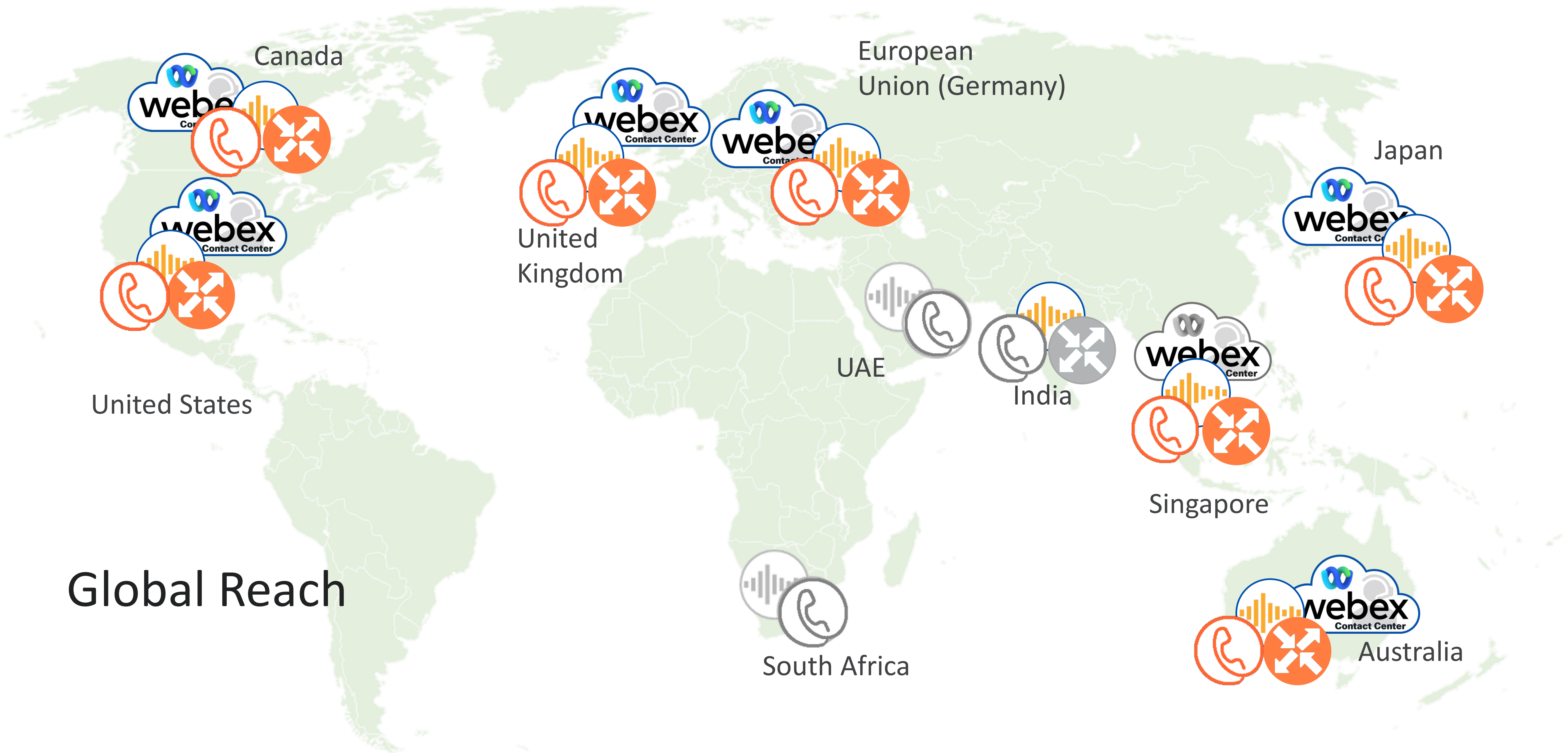
Voice Access Layer



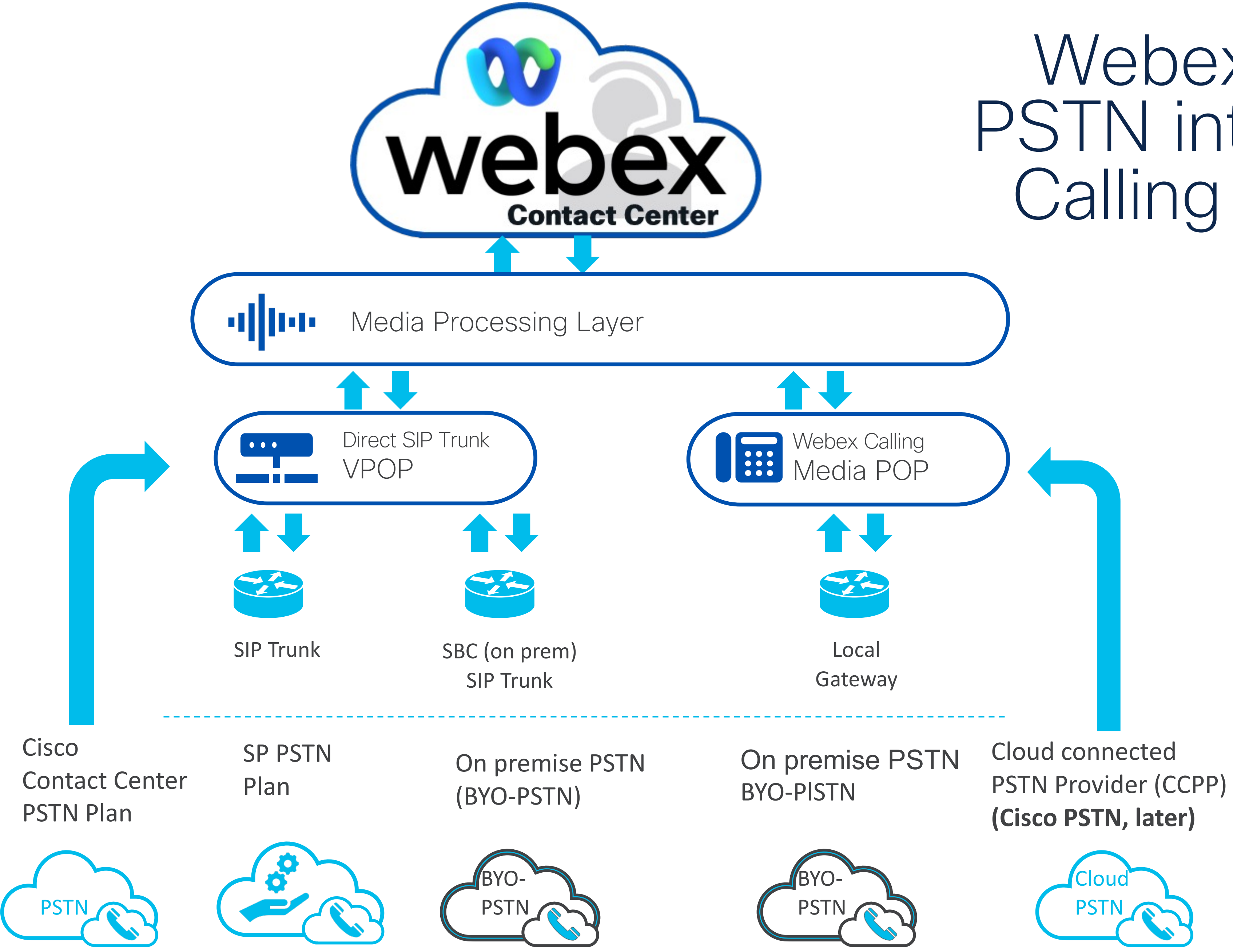
Webex Calling
- Kal's view, what do I mean by Media POP??



Global Reach



Webex Contact Center PSTN integration options & Calling Plans (Summary)



Partner selects an option when initially provisioning tenant

VPOP

- Cisco Contact Center PSTN plan
- Support Customer/SP connection
- Provide SIP Trunk Integration
- No access to Cloud PSTN plans

Webex Calling (Media POP)

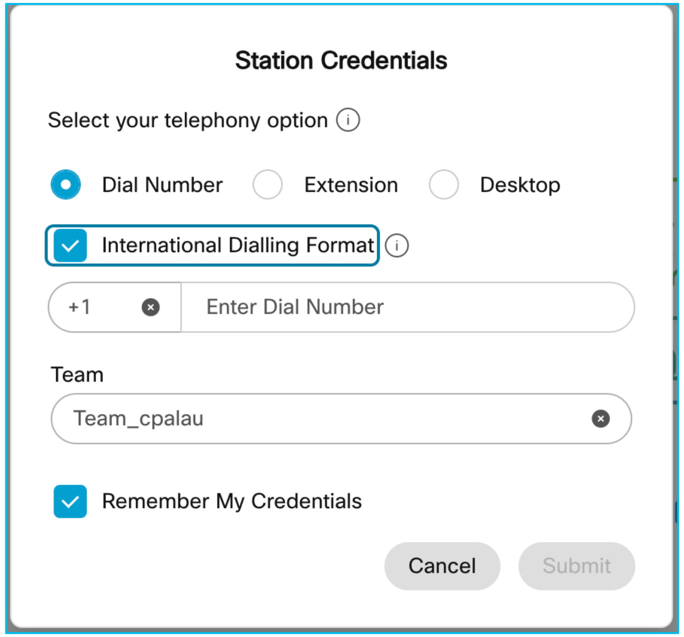
- Requires WxC subscription
- Provide access to Cloud PSTN (CCPP) and local gateway (SIP Trunk)

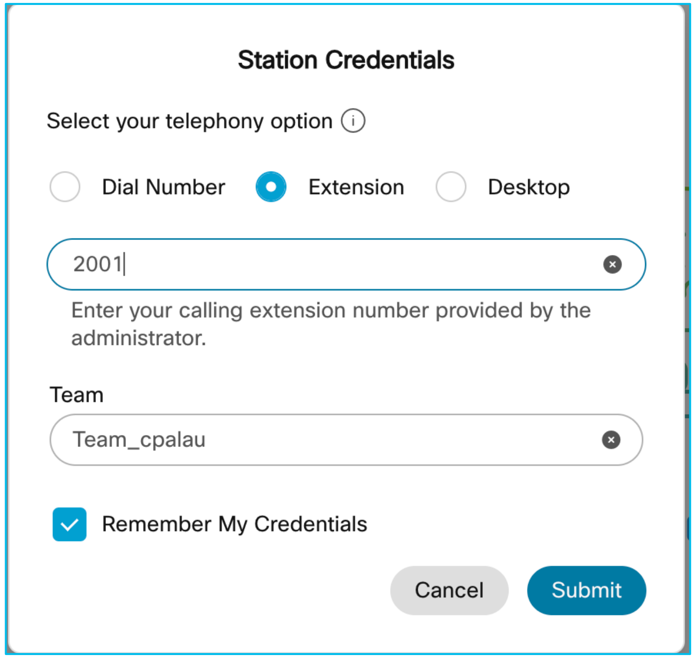
Note: Cisco Contact Center PSTN Plan

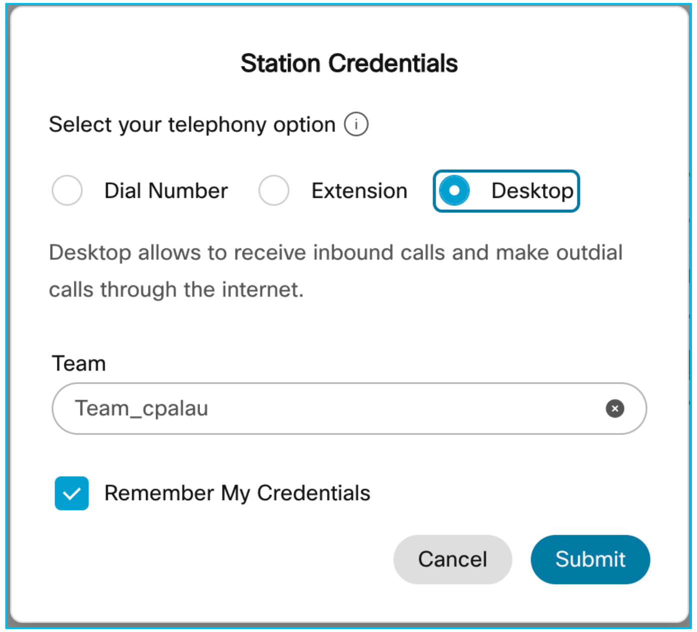
- PSTN Plan for US/Canada only
- VPOP only today (WxC Media POP planned)

Agent Call Delivery

Agent Call Delivery selection





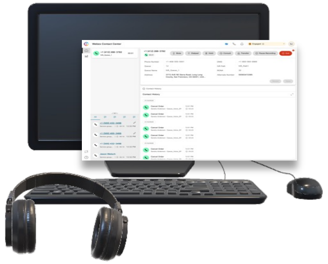


PSTN based Agent

On Premise Telephony

Webex Telephony

Webex App



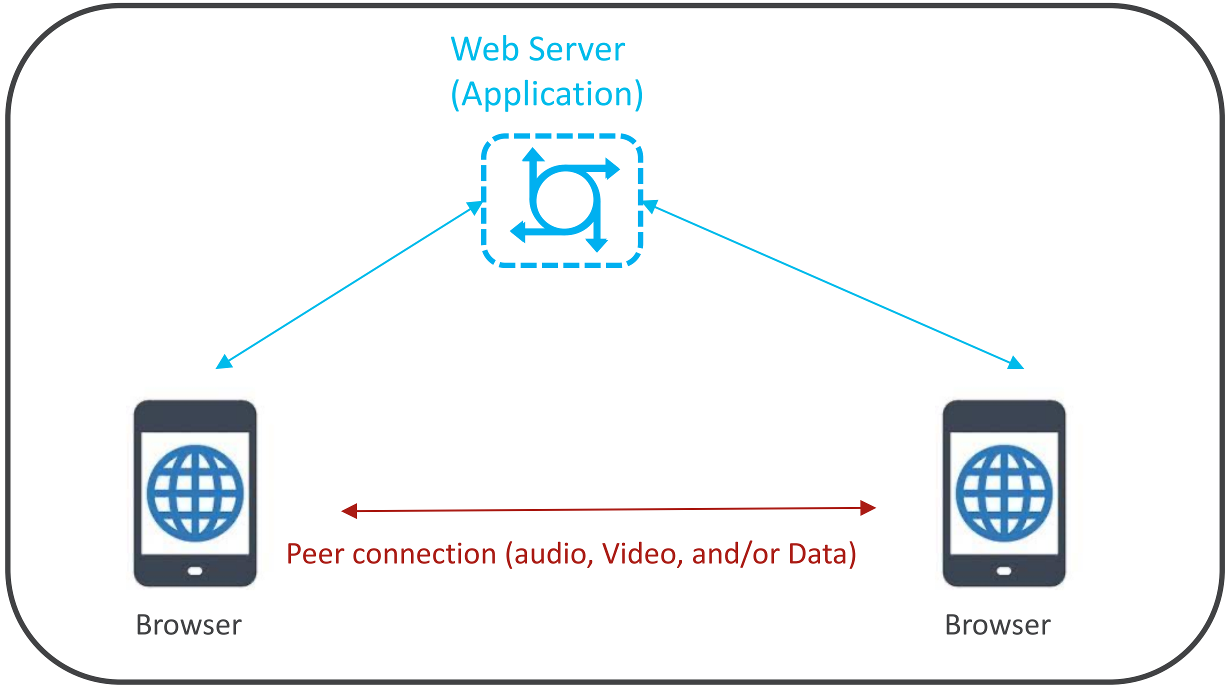
NEW

WebRTC

WebRTC

What is WebRTC?

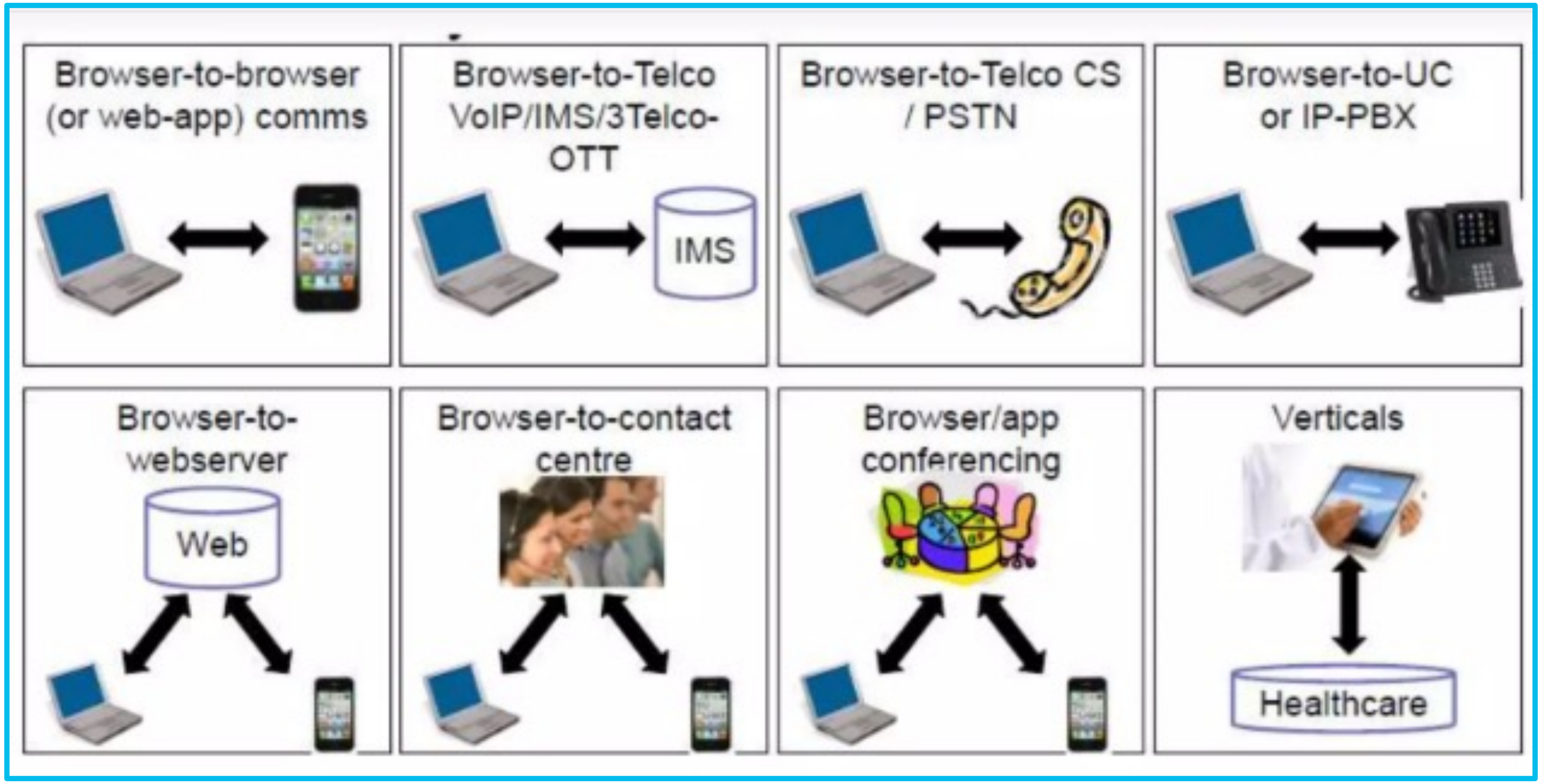
WebRTC (Web Real-Time Communication) is a technology that enables Web applications and sites to capture and optionally stream audio and/or video media, as well as to exchange arbitrary data between browsers without requiring an intermediary



There are many other deployment models....

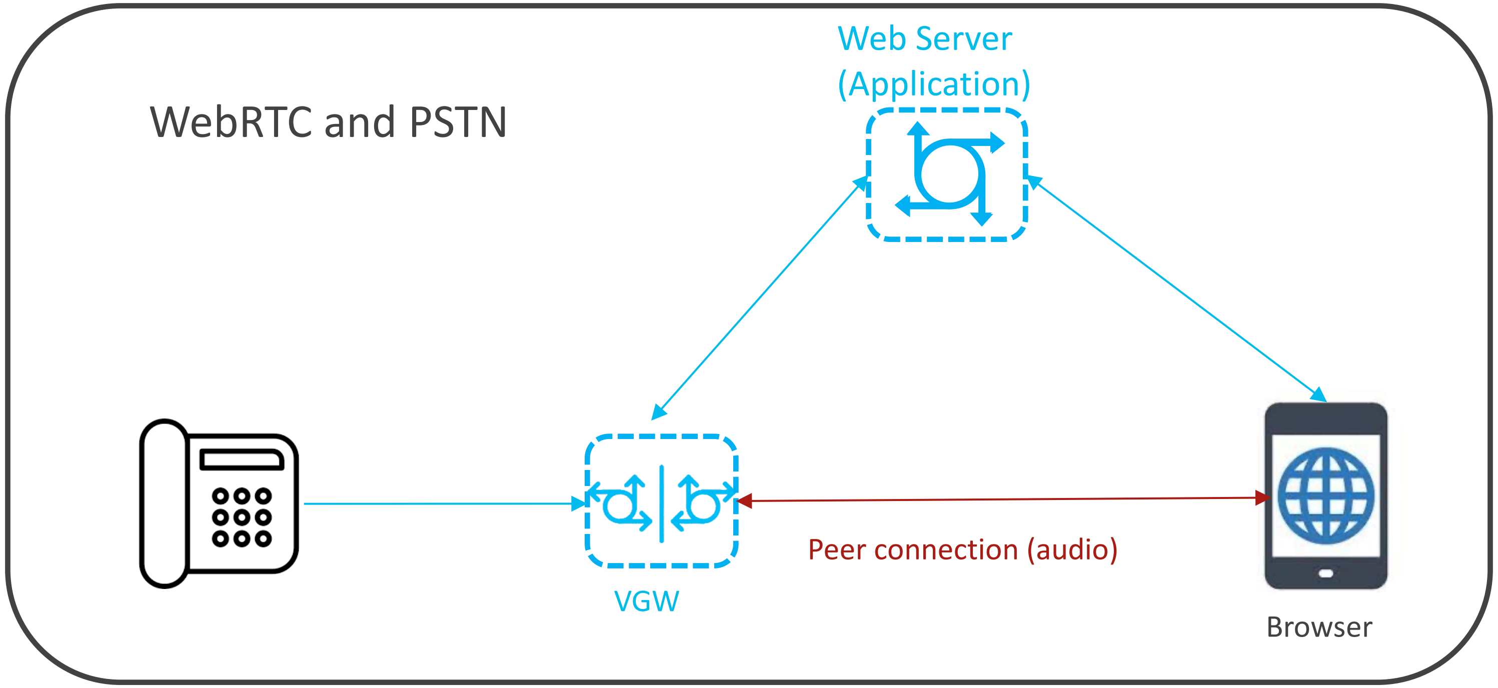
Details: https://webrtc.org/

WebRTC use cases



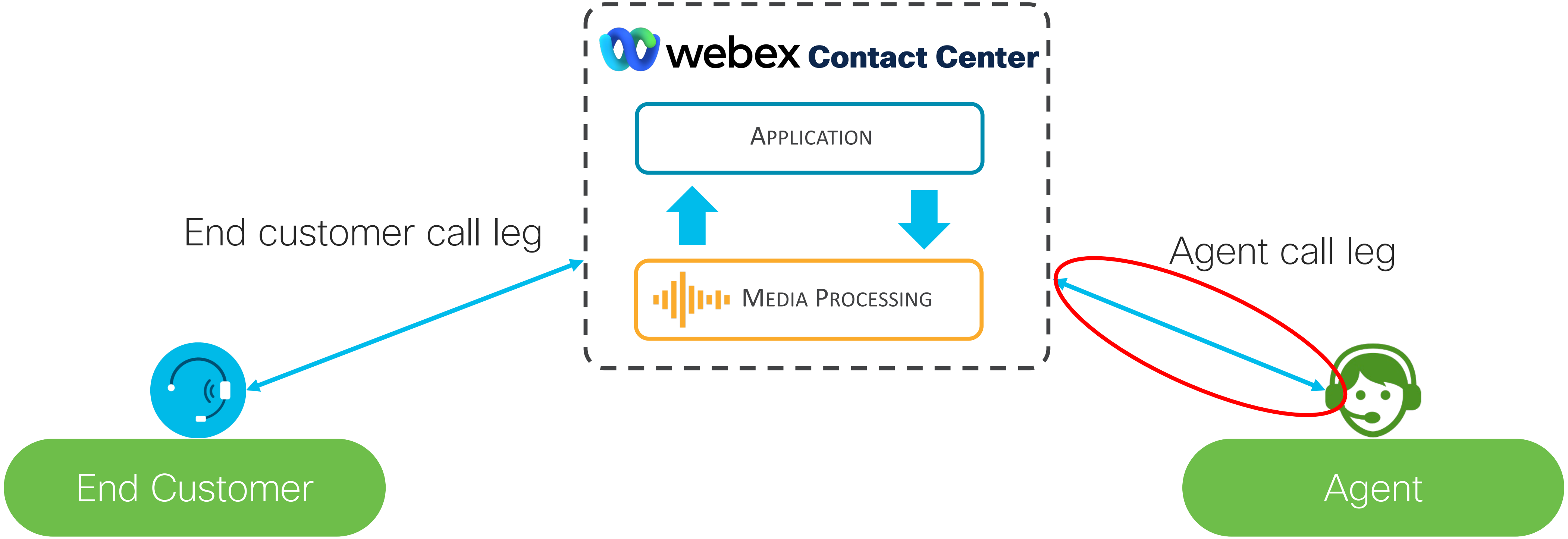
+ various other …

WebRTC & PSTN



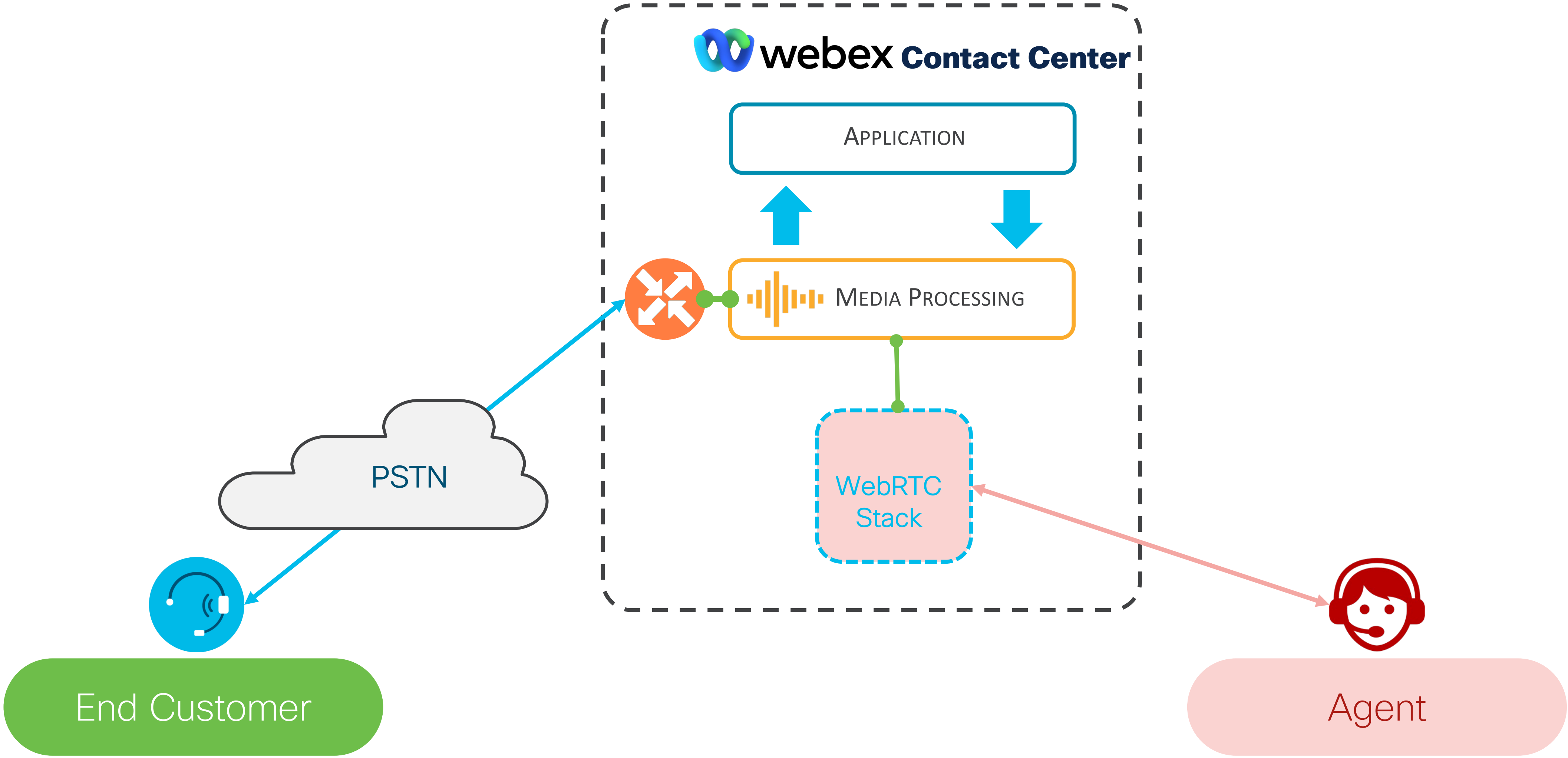
WebRTC and PSTN
Web Server
(Application)
VGW
Peer connection (audio)
Browser

Recall …

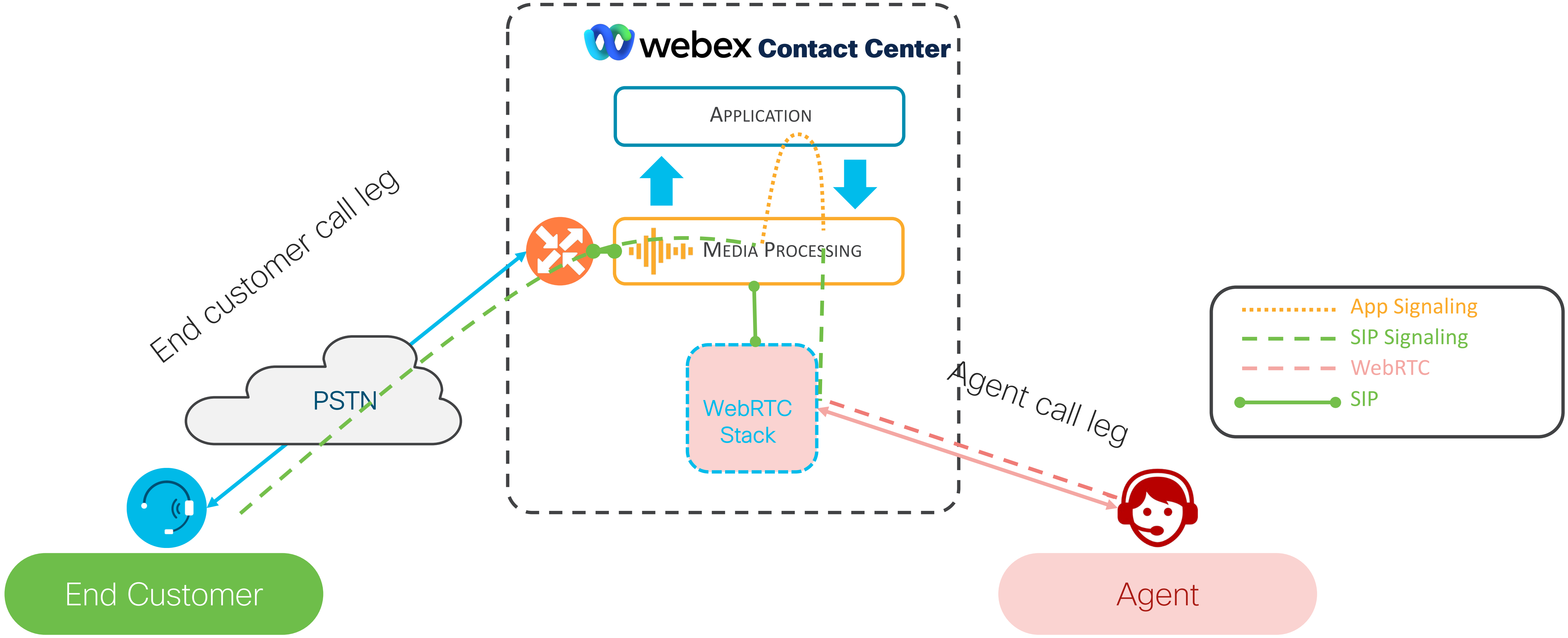


Regardless of PSTN integration, each answered call by an agent has two call legs as shown above

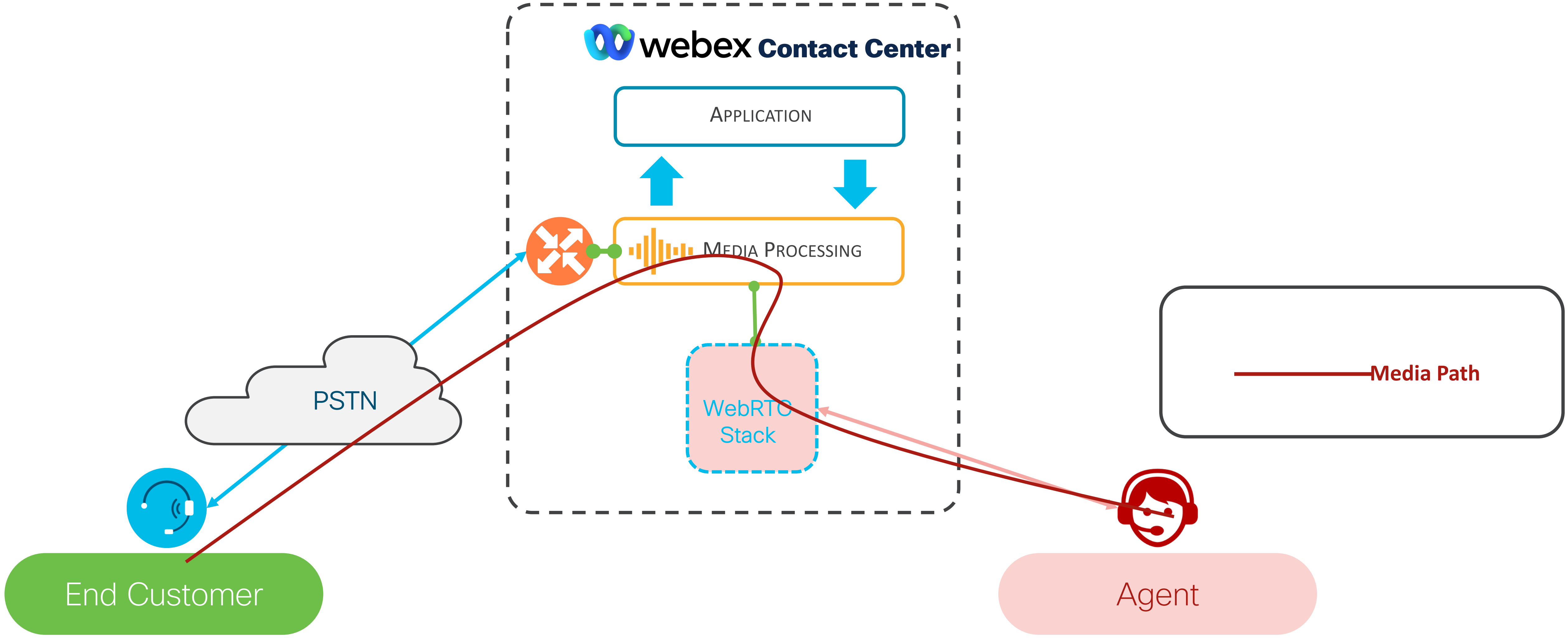
WebRTC for agent call leg



WebRTC for agent call leg



WebRTC for agent call leg (Cont.'d)

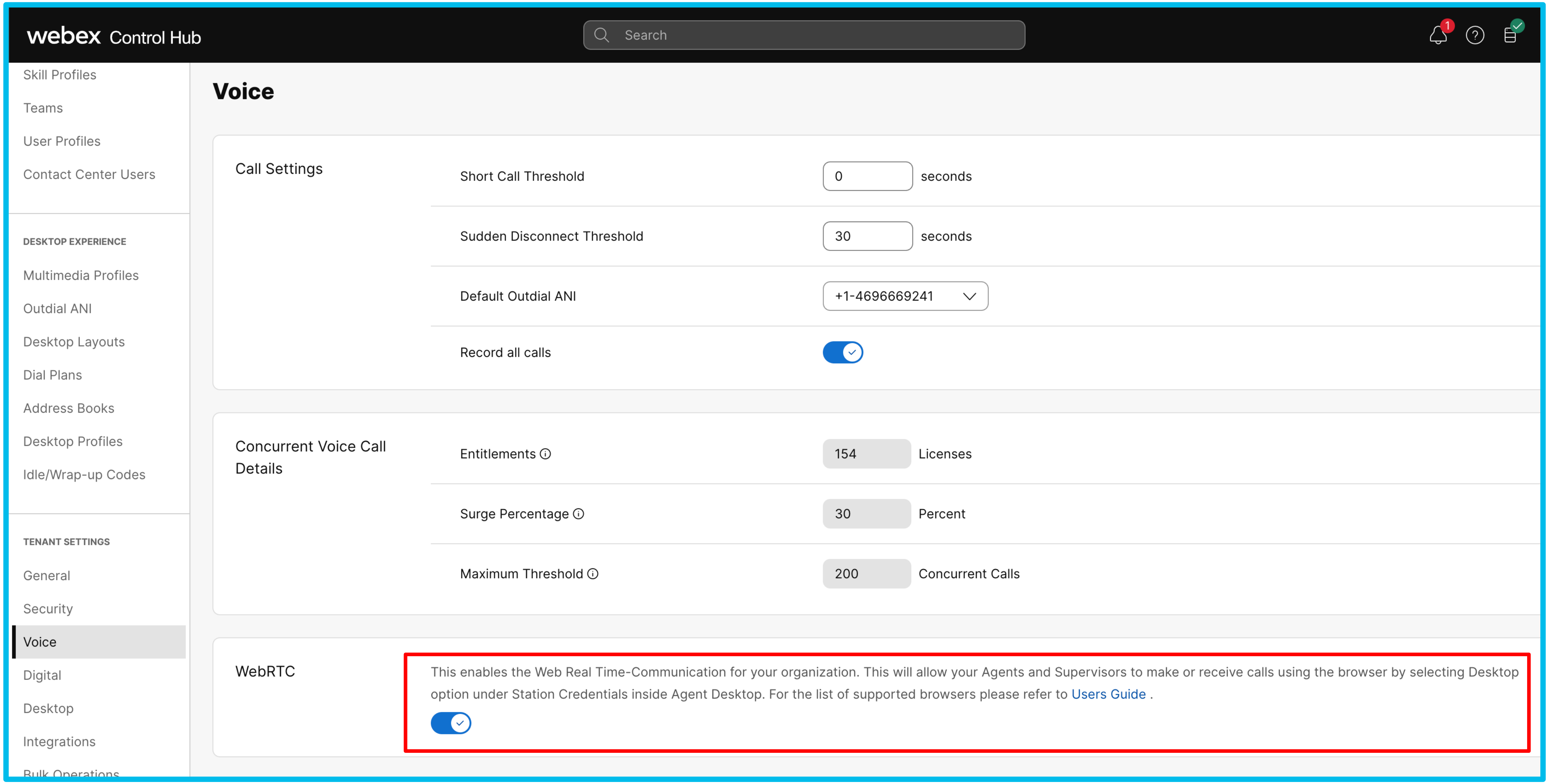


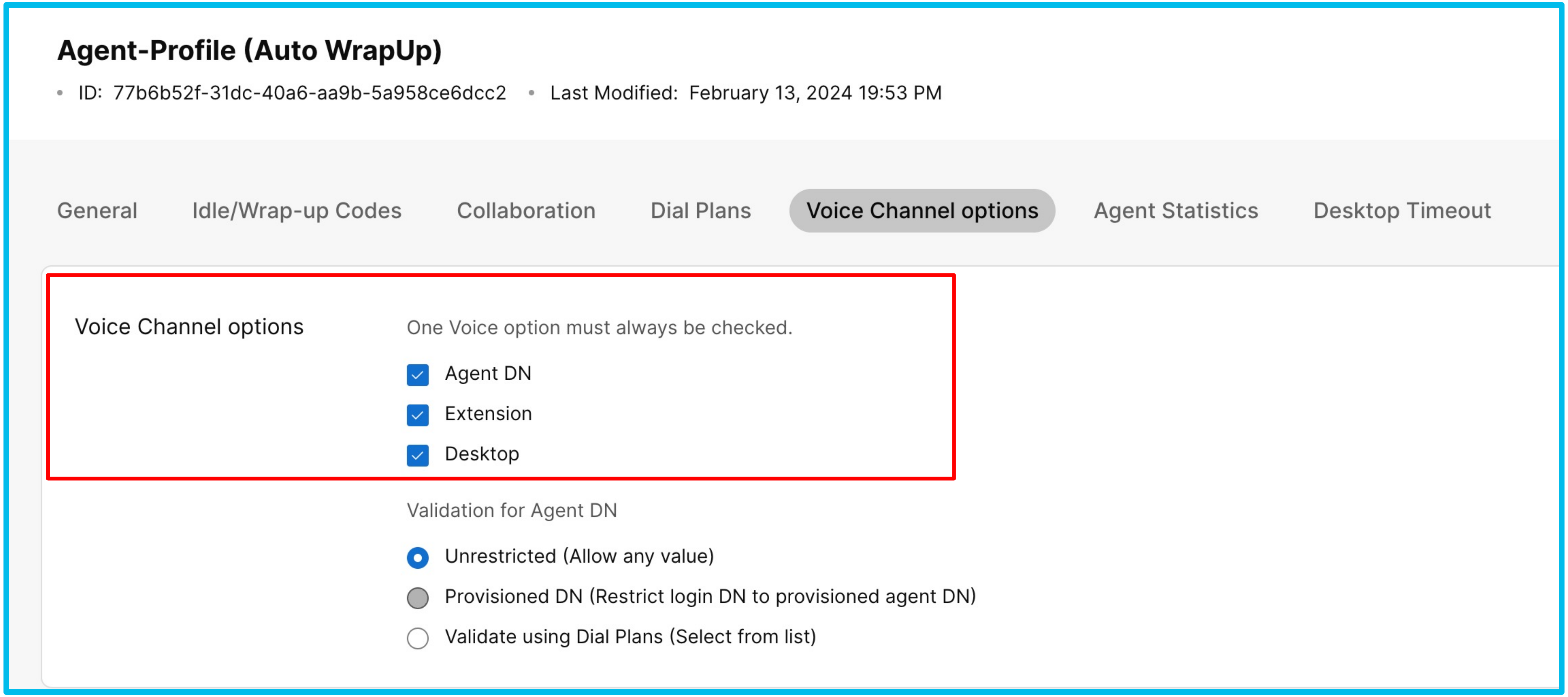
Additional notes

- WebRTC Desktop phone is not currently available for Supervisor Desktop.
- WebRTC has the internal logic to select the closest WebRTC stack region based on the PC/Laptop IP detection and its mapping to the country.
- If an Agent is using a VPN to remote country would get connected to nearest WebRTC stack to that remote country.

WebRTC

WebRTC Control Hub Configuration

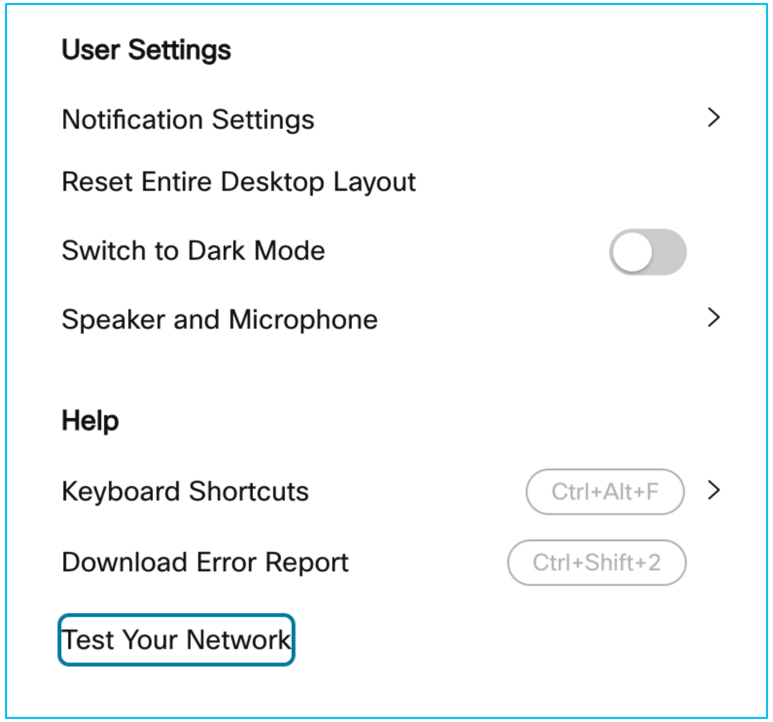


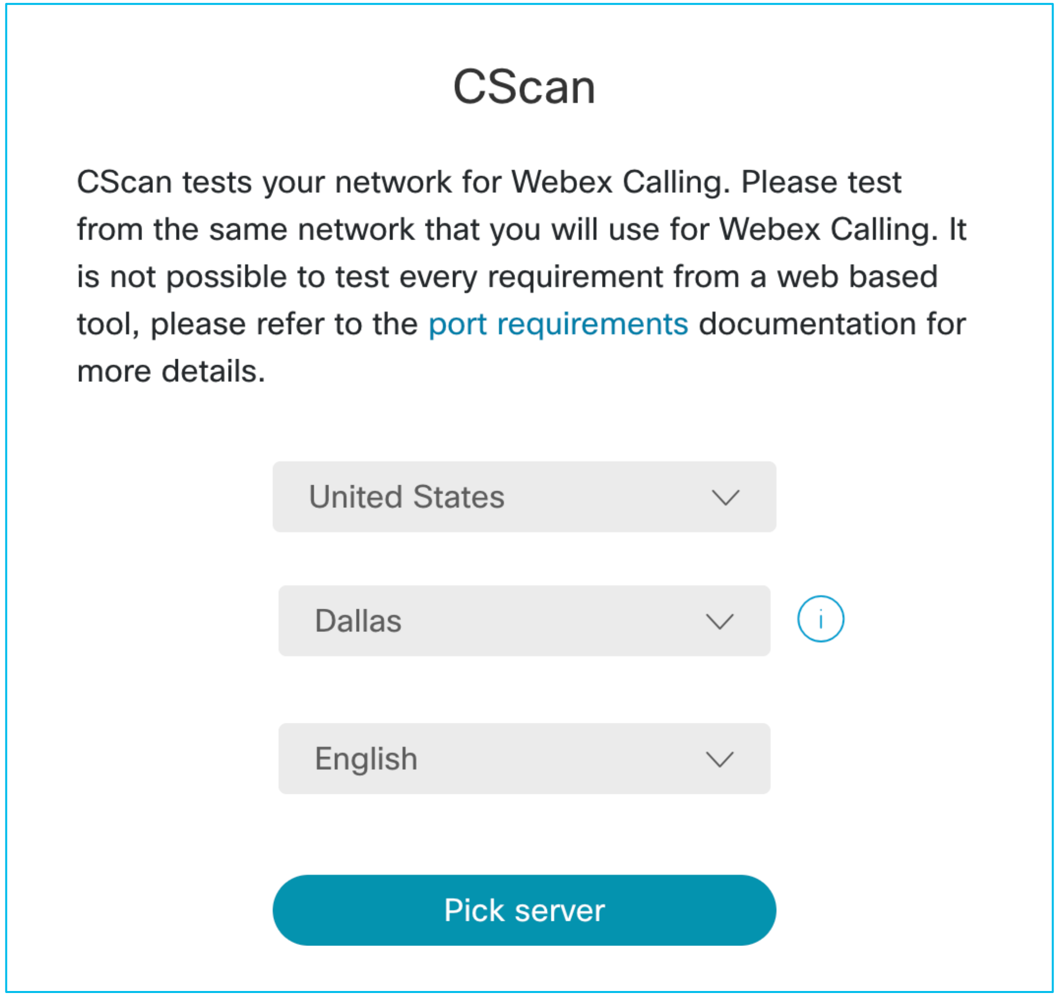


Agent Desktop Profile Configuration

CS Scan – Network Check

- Agent can use “Test Your Network” to test the network showing details like speed, packet loss, jitter etc.





CS Scan Results

Your connection **meets requirements**. Your network is ready for Webex Calling.

Ensure all required ports are open. For more details, please refer to the port requirements documentation.

Estimate of concurrent possible calls: 15

Your Public IP: 70.119.101.143

Chrome 122.0.0.0, Mac OS X,United States Dallas

Latency (RTT)	Download	Upload
26.00 ms	30.07 Mbps	8.52 Mbps

Packet loss	Jitter
Download - 1.22 %	Download - 24.00 ms
Upload - 0.00 %	Upload - 24.46 ms

Ready	Port	Use
✓	443	Device configuration and firmware management
✓	8934	Call Signalling to Webex Calling

Test Again

Test Another Server

Analyzer Report

Agent Endpoint DN for WebRTC shows up as webrtc-<uuid>

Search Export

Entrypoint ID	Activity Start Timestamp	Activity End Timestamp	Activity Dura...	Agent Endpoint (DN)
4d9b-7103-4b1b-af12-f1...	2/23/2024 1:03:57 PM	2/23/2024 1:03:57 PM	0 ms	
4d9b-7103-4b1b-af12-f1...	2/23/2024 1:05:40 PM	2/23/2024 1:05:40 PM	0 ms	
	2/23/2024 1:05:40 PM	2/23/2024 1:05:40 PM	32 sec	webrtc-7a5138bf-1c10-4cf5-ae5b-d43f8e76ba9a
4d9b-7103-4b1b-af12-f1...	2/23/2024 1:05:41 PM	2/23/2024 1:05:41 PM	0 ms	

Webex CC WebRTC Phasing

ROAD MAP

Omni-channel Use Cases

Differentiation & digital channel innovation

a) Channel escalation (e.g. Digital to Voice, Voice to Video)
b) Co-browse
c) Video(Agent side? Or Customer side?)

WebRTC SDK

Customer-side & custom desktop SDK

a) Enables click-to-call from web and mobile apps
b) SDK
c) CRM Connector
d) Mobile App

supervisor Desktop WebRTC Support

Top use case enabling complete IP Contact Center

- Supervisor Desktop support
- Voice-Only

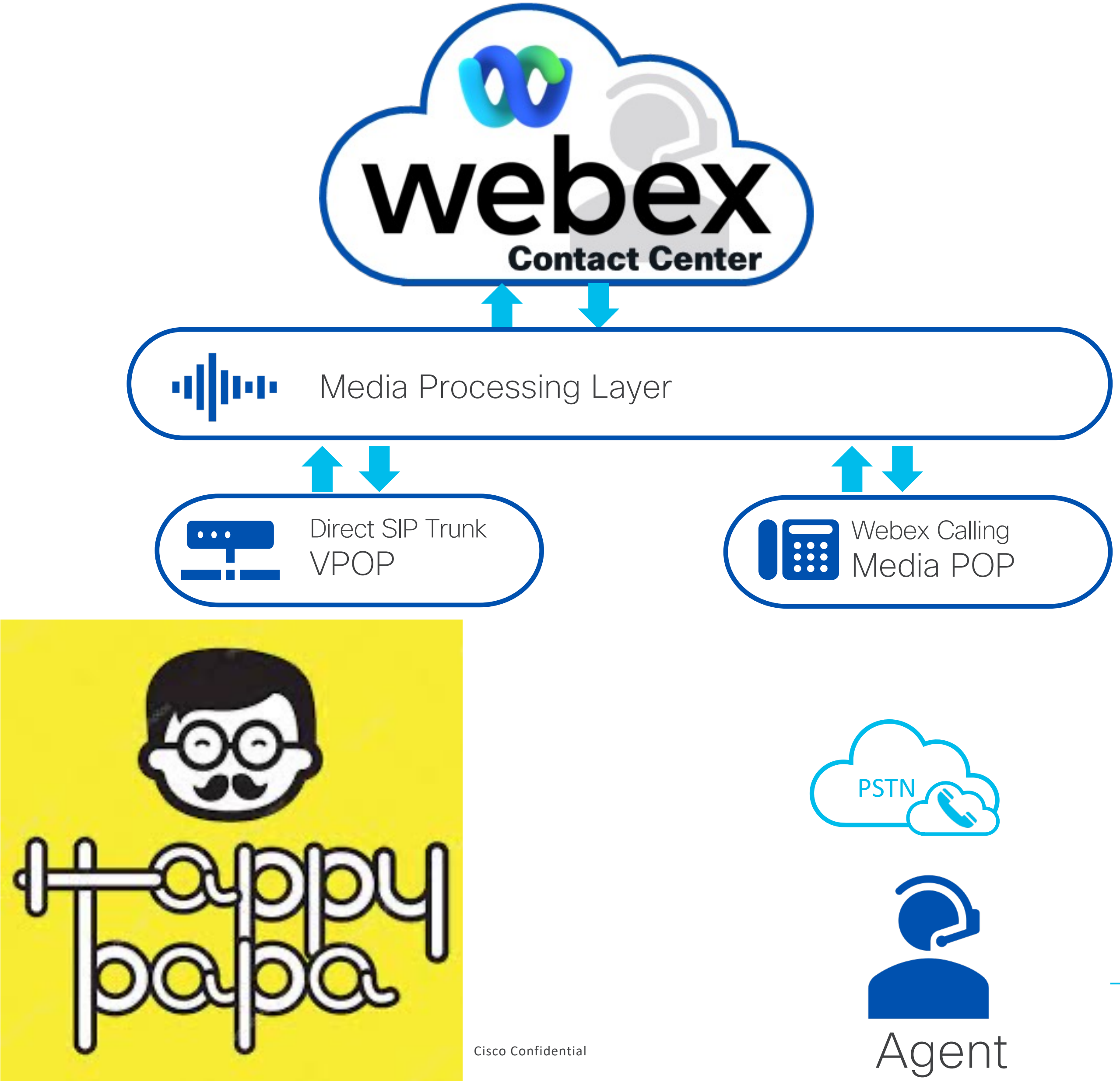
Agent-side WebRTC

- Agent-side WebRTC in agent desktop browser
- Supported for Bundled PSTN, vPOP and LGW (Calling) PSTN
- Voice-Only

Customer Use cases

The “5” steps

The 5 steps for most deployment



(1) Select Home Region

(2) Select PSTN Region(s)

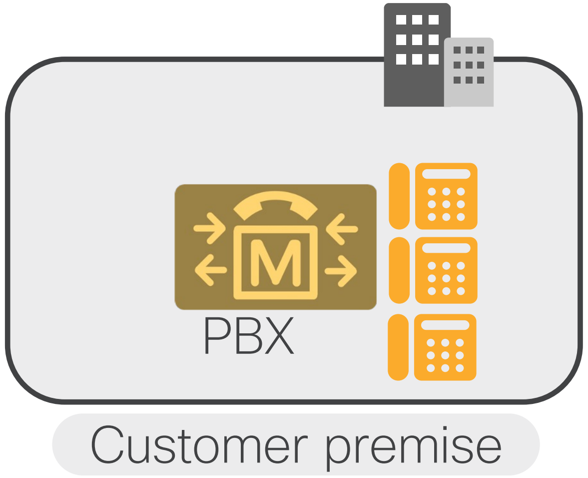
(3) Select Access Layer

(4) Select PSTN

(5) Select Agent Delivery

Customer 1– Existing PBX with endpoints

US based customer wants to move CC to the cloud but wants to keep existing third-party PBX due to high investment in endpoints still under support.



Step 1- Select Home Region = US

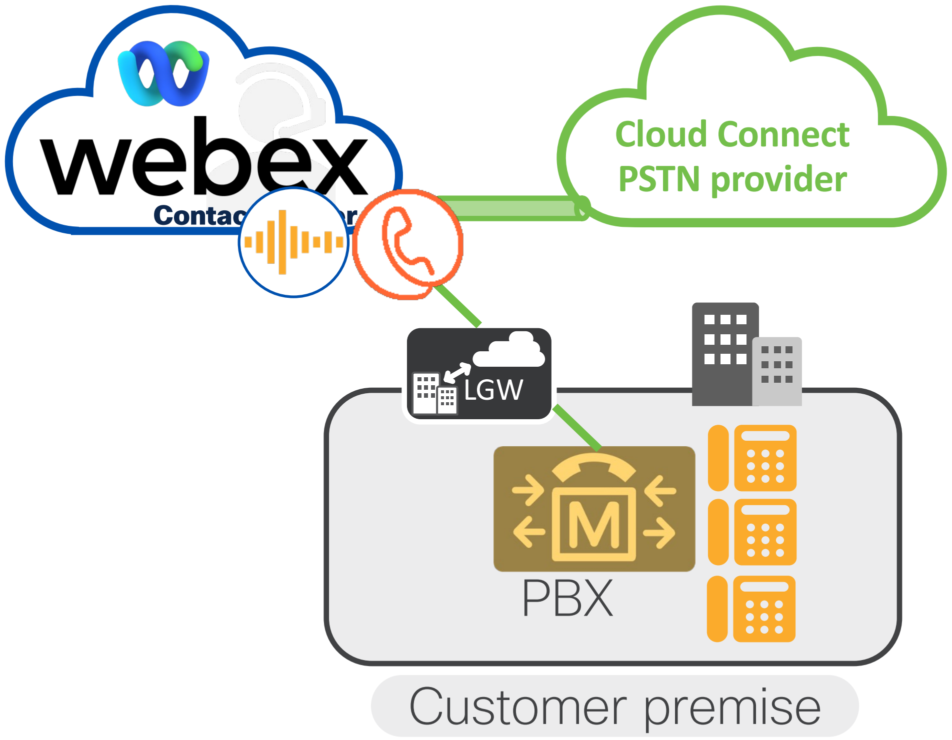
Step 2- Select PSTN Region(s) = US (Default)

Step 3- Select Access Layer

- Both **Webex Calling** or **VPOP** can interface with third-party PBX
- **Best practice:** Choose **Webex Calling/Media POP**
- Use **Local GW** to connect the on-premise PBX to Webex Calling

Customer 1– Existing PBX with endpoints

US based customer wants to move CC to the cloud but wants to keep existing third-party PBX due to high investment in endpoints still under support.



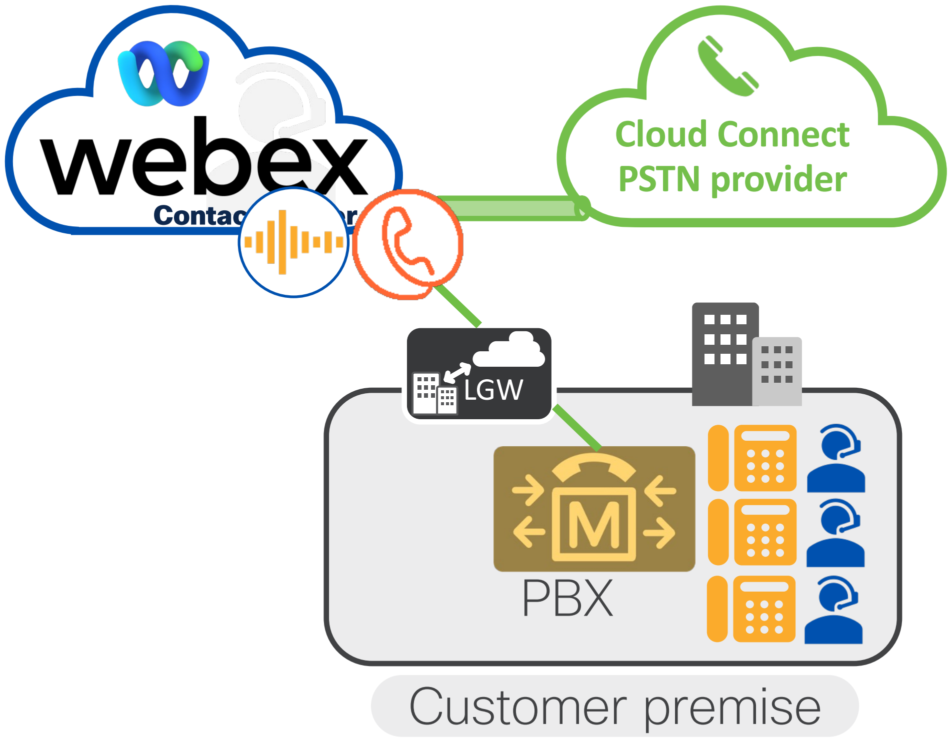
Step 4- Select PSTN

- No specific requirement from customer.

- **Best practice?**
- Use **Cloud connect for Webex Calling** to reduce use of BW

Customer 1– Existing PBX with endpoints

US based customer wants to move CC to the cloud but wants to keep existing third-party PBX due to high investment in endpoints still under support.



Step 5 - Choose Agent Call Delivery

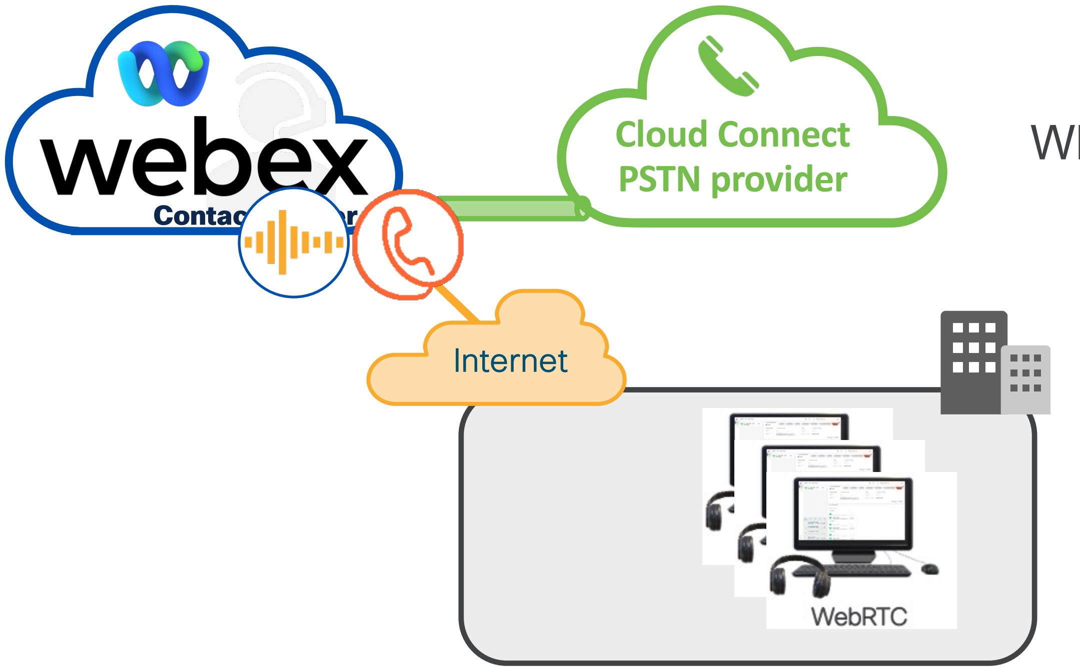
Dictated by customer requirement

Can we optimize & improve this deployment further?

Best practice: WebRTC can serve as alternative method for agent call delivery as it is included in the Standard agent license

Customer 1– Existing PBX with endpoints

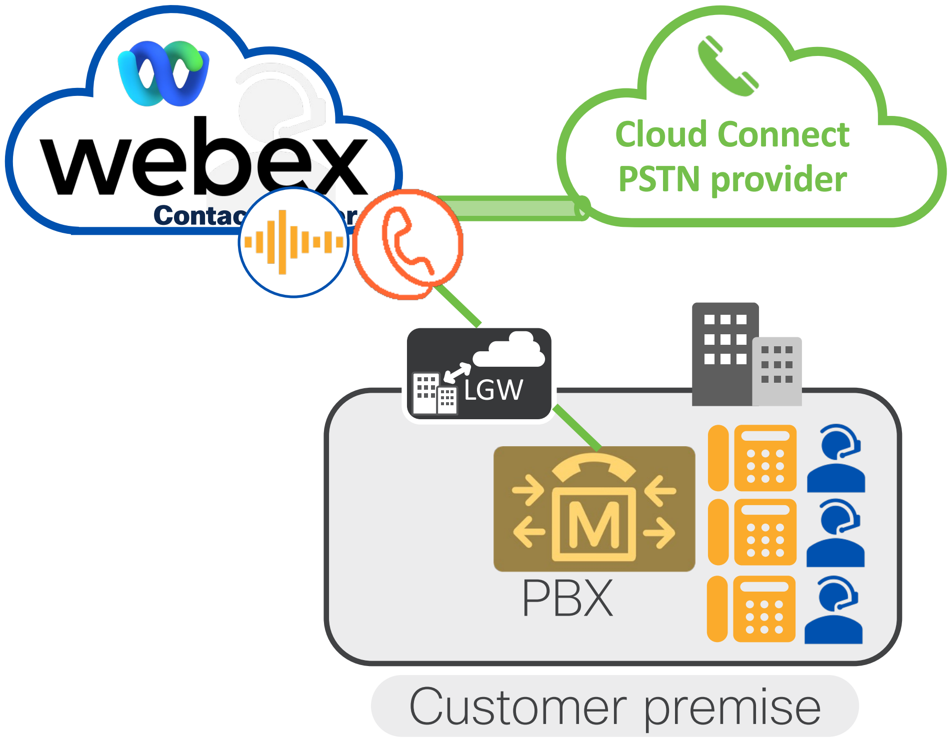
US based customer wants to move CC to the cloud but wants to keep existing third-party PBX due to high investment in endpoints still under support.



What about if the customer wants to remove the PBX?

Customer 1– Existing PBX with endpoints

US based customer wants to move CC to the cloud but wants to keep existing third-party PBX due to high investment in endpoints still under support.

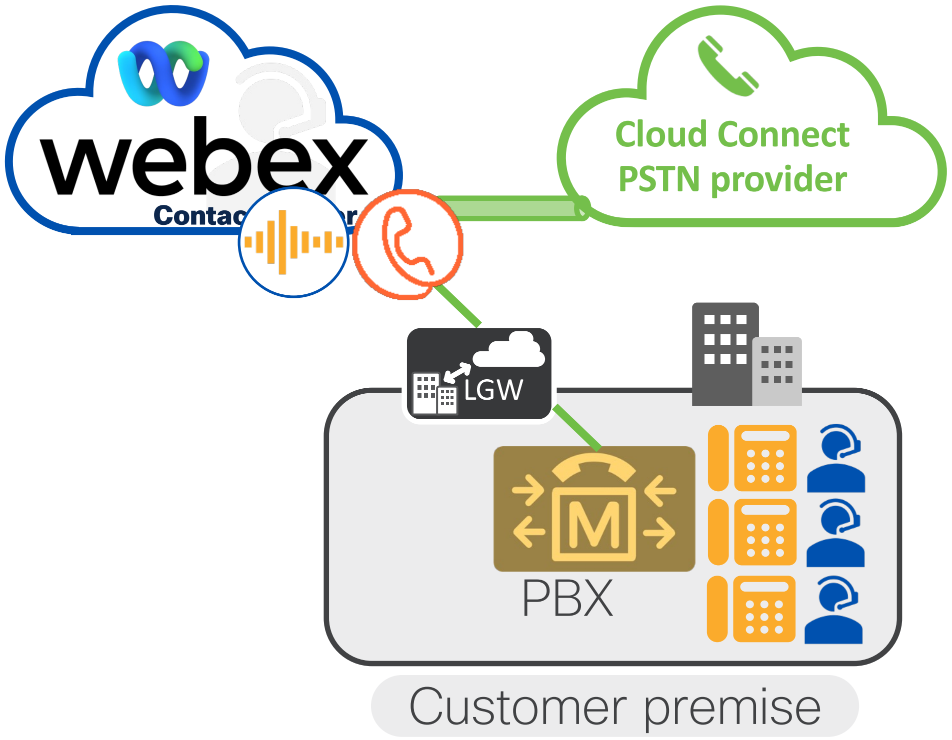


Additional notes

- Cloud Connect PSTN provider must have CC rates for the required country
- Country dial plan must be supported by Webex Calling
- Do I need at least ONE Webex Calling user license?
    - No, Not anymore!
- CUBE licences needed for Local GW

Customer 1– Existing PBX with endpoints

US based customer wants to move CC to the cloud but wants to keep existing third-party PBX due to high investment in endpoints still under support.



If the customer at peek time has 100 agents logged in, and 100 calls in the IVR, how many CUBE licenses required?

0

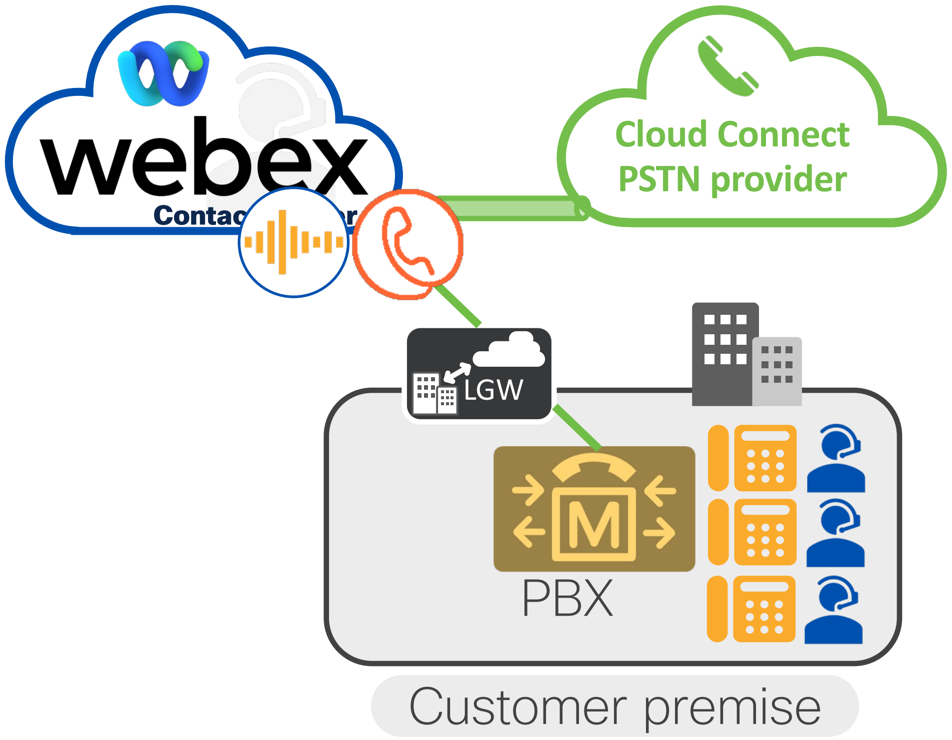
100

200

300

Customer 1– Existing PBX with endpoints

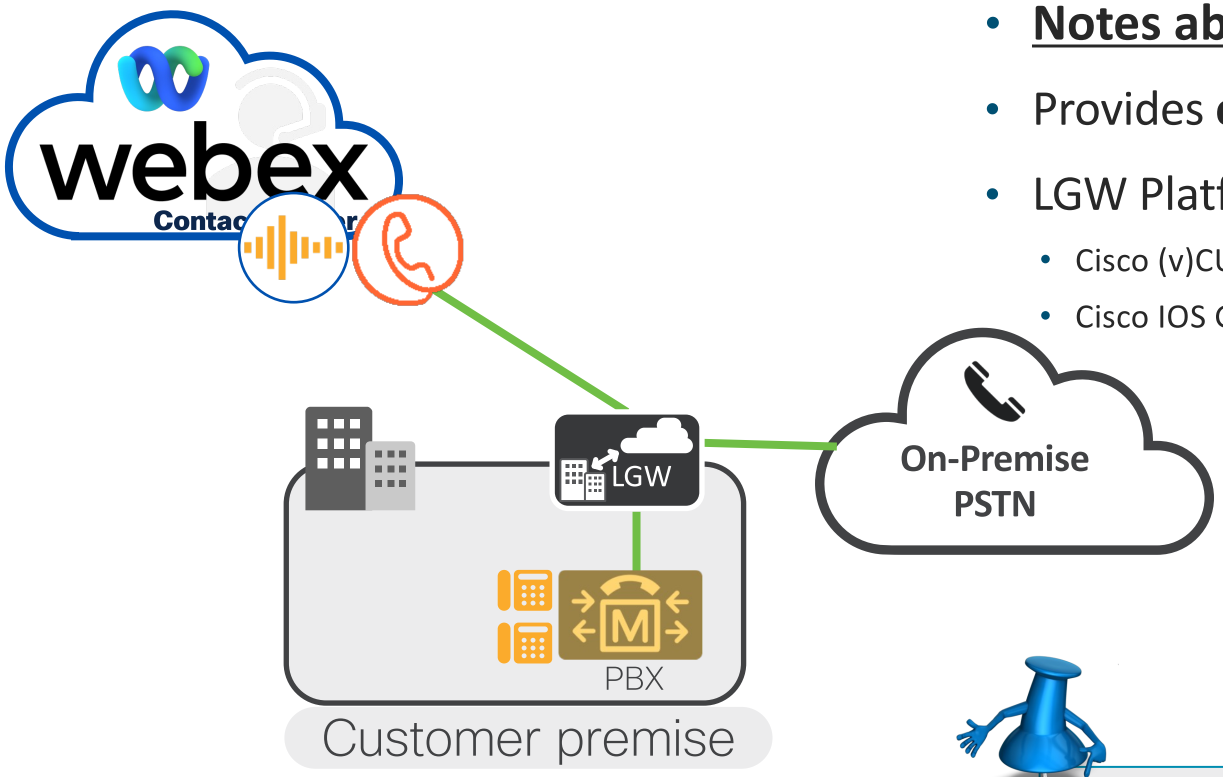
US based customer wants to move CC to the cloud but wants to keep existing third-party PBX due to high investment in endpoints still under support.



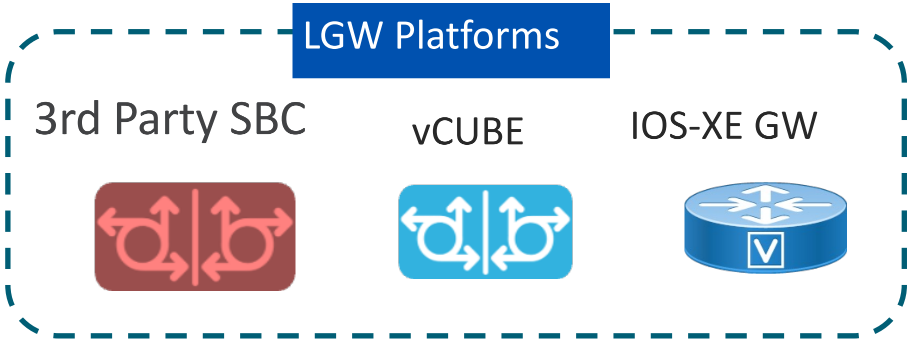
What about if the customer wants to to keep on premise PSTN?

Customer 1– Existing PBX with endpoints

US based customer wants to move CC to the cloud but wants to keep existing third-party PBX due to high investment in endpoints still under support.



- **Notes about LGW:**
- Provides **connectivity** between Webex Calling and Customer premises
- LGW Platforms
  - Cisco (v)CUBE for IP-based PSTN
  - Cisco IOS Gateway for TDM-based PSTN Certified 3rd Party SBC



- https://blog.webex.com/cloud-calling/local-gateway-support-for-webex-calling/
- https://help.webex.com/en-us/article/t9xctu/Get-started-with-Local-Gateway
- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2024/pdf/BRKCOL-2312.pdf

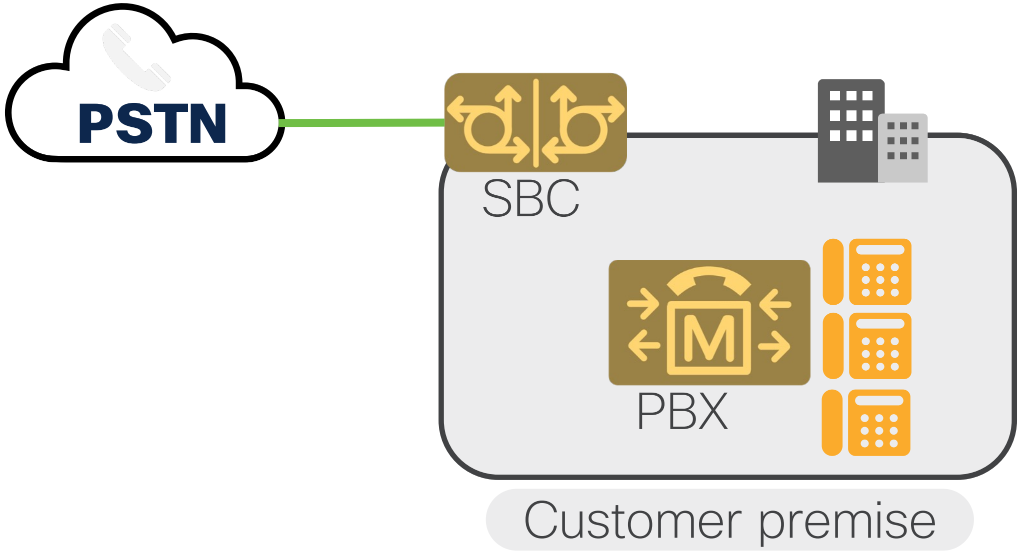
NEW

- Simplification **of Edge services for Webex Contact Center**
  - Common connection **for** Webex Calling **and** Webex Contact Centre.
  - Plus, No **Webex Calling Subscription required.**
  - Faster deployment with self service provisioning in control hub
  - Access to Cisco cloud connected PSTN providers for Webex contact center
  - Cisco Calling plan options for both knowledge workers and service numbers (CC) – PLANNED
  - Easier to deploy to multiple service providers or multiple regions.

Use case #2

Customer 2 – Existing on-premise PSTN

US based customer wants to keep existing **On-premise PSTN** because of long-term contract but is ready to move their PBX and Contact Center to the cloud. They want collaboration tools to sync presence state.



Step 1 - Home region = US

Step 2 - PSTN region = US (default)

Step 3 - Choose Access Layer

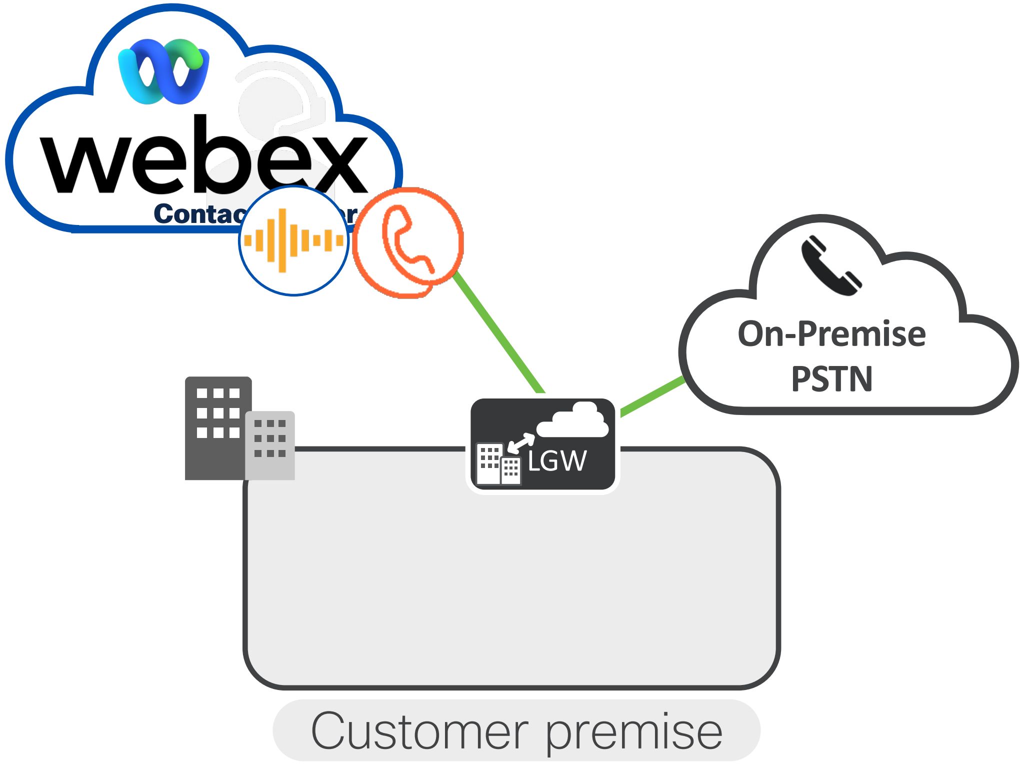
Both **Webex Calling** or **VPOP** can interface with on-premise PSTN

Customer wants an enterprise cloud PBX, Webex Calling fits that role too

Use **Local GW** to connect the on-premise PSTN to Webex Calling

Customer 2 – Existing on-premise PSTN

US based customer wants to keep existing **On-premise PSTN** because of long-term contract but is ready to move their PBX and Contact Center to the cloud. They want collaboration tools to sync presence state.



Step 4 – Choose PSTN

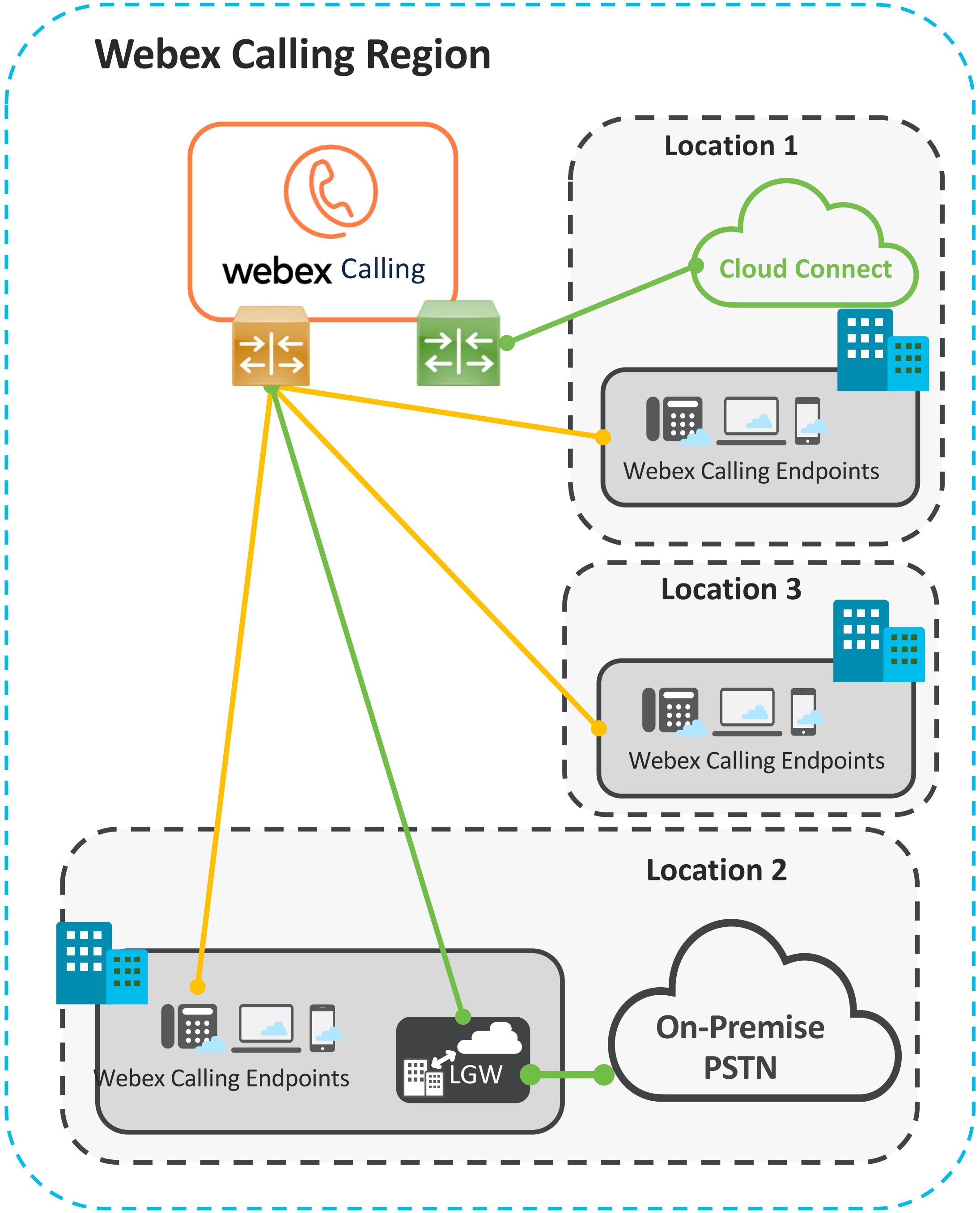
Dictated by customer requirement

Best practice:

- **Cloud connect for Webex Calling** can work in parallel with on-premise PSTN.
- Existing PSTN provider might be in the list of Webex Calling Cloud Connect providers.
- New numbers could come with different provider over time using a different Location configuration in Webex Calling.

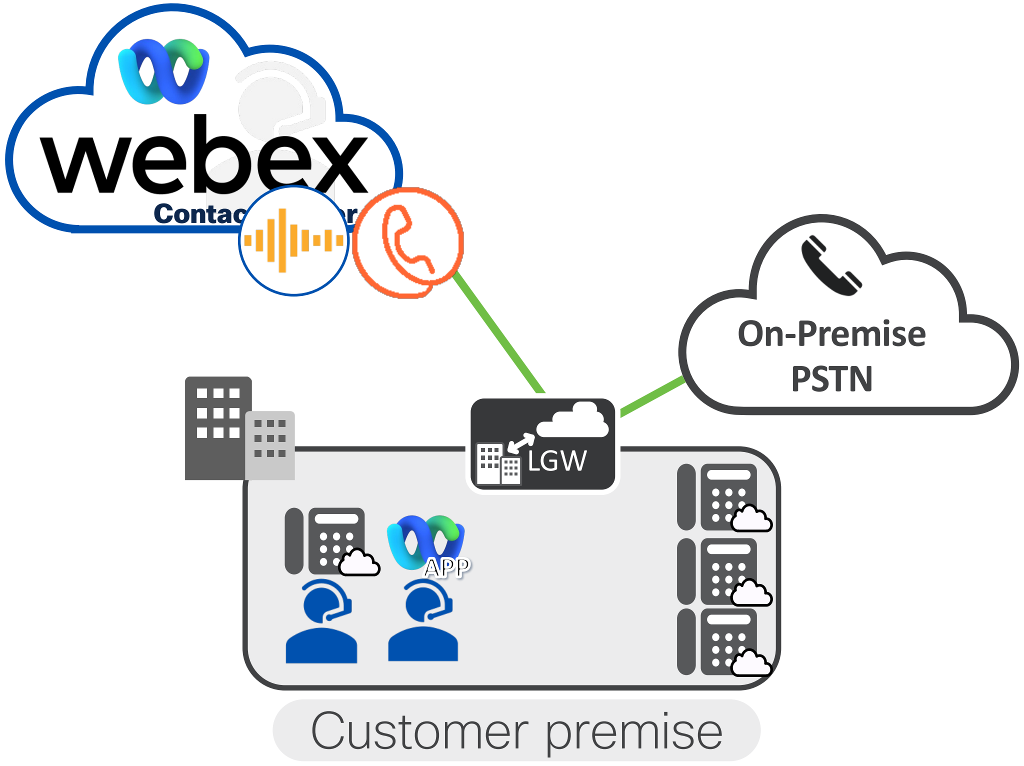
Webex Calling Region & Locations - PSTN access

- A **Region** can have multiple **Locations**
- **Cloud Connect, Cisco Calling Plan** <u>or</u> **LGW** must be selected as the PSTN access method for each **Location**
- Only ONE **Cloud Connect, Cisco Calling Plan** <u>or</u> **LGW** per **Location** (Multiple LGWs per location requires Route Group/Trunks)
- Same **Cloud Connect, Cisco Calling Plan** or **LGW** can be used for multiple WxC **Locations**



Customer 2 – Existing on-premise PSTN

US based customer wants to keep existing **On-premise PSTN** because of long-term contract but is ready to move their PBX and Contact Center to the cloud. They want collaboration tools to sync presence state.



Step 5 – Choose Agent Call Delivery

Webex Calling endpoints or WebRTC

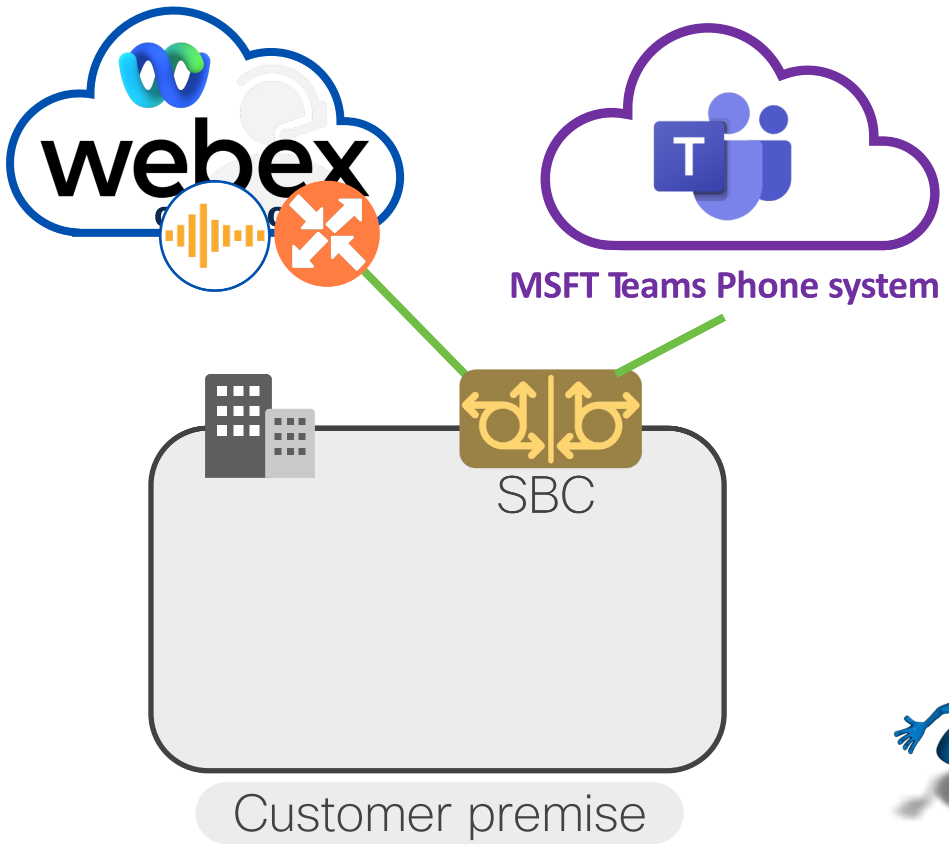
Any CUBE licenses required?

- Local Gateway CUBE licences included if agents have Webex Calling Pro license
- If using WebRTC for agents, CUBE licenses are required

Use case #3

Customer 3 – MSFT Teams Phone System

US based customer just spent $$$ on E5 licenses and wants agents to be able to transfer CC calls to office backend MSFT Teams users. They also want presence synchronization.



Step 1 - Home region = US

Step 2 - PSTN region = US (default)

Step 3 - Choose Access Layer

Only VPOP is currently supported for MSFT Teams for the Connect Model

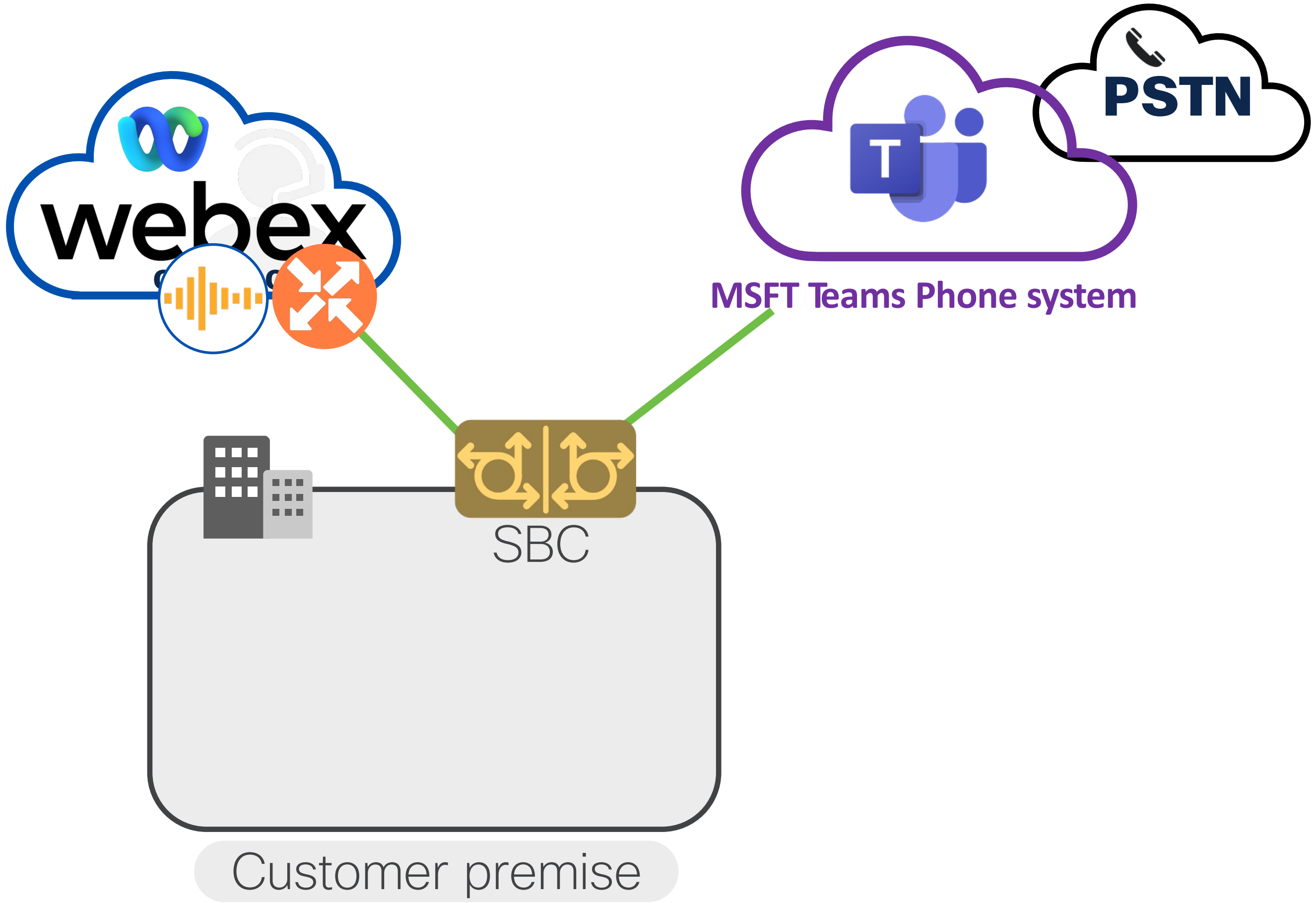
Support with Local GW is in the roadmap (SOON!)

Setup SIP trunk from VPOP to the MSFT Direct Routing SBC

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1hqL2

Customer 3 – MSFT Teams Phone System

US based customer just spent $$$ on E5 licenses and wants agents to be able to transfer CC calls to office backend MSFT Teams users. They also want presence synchronization.

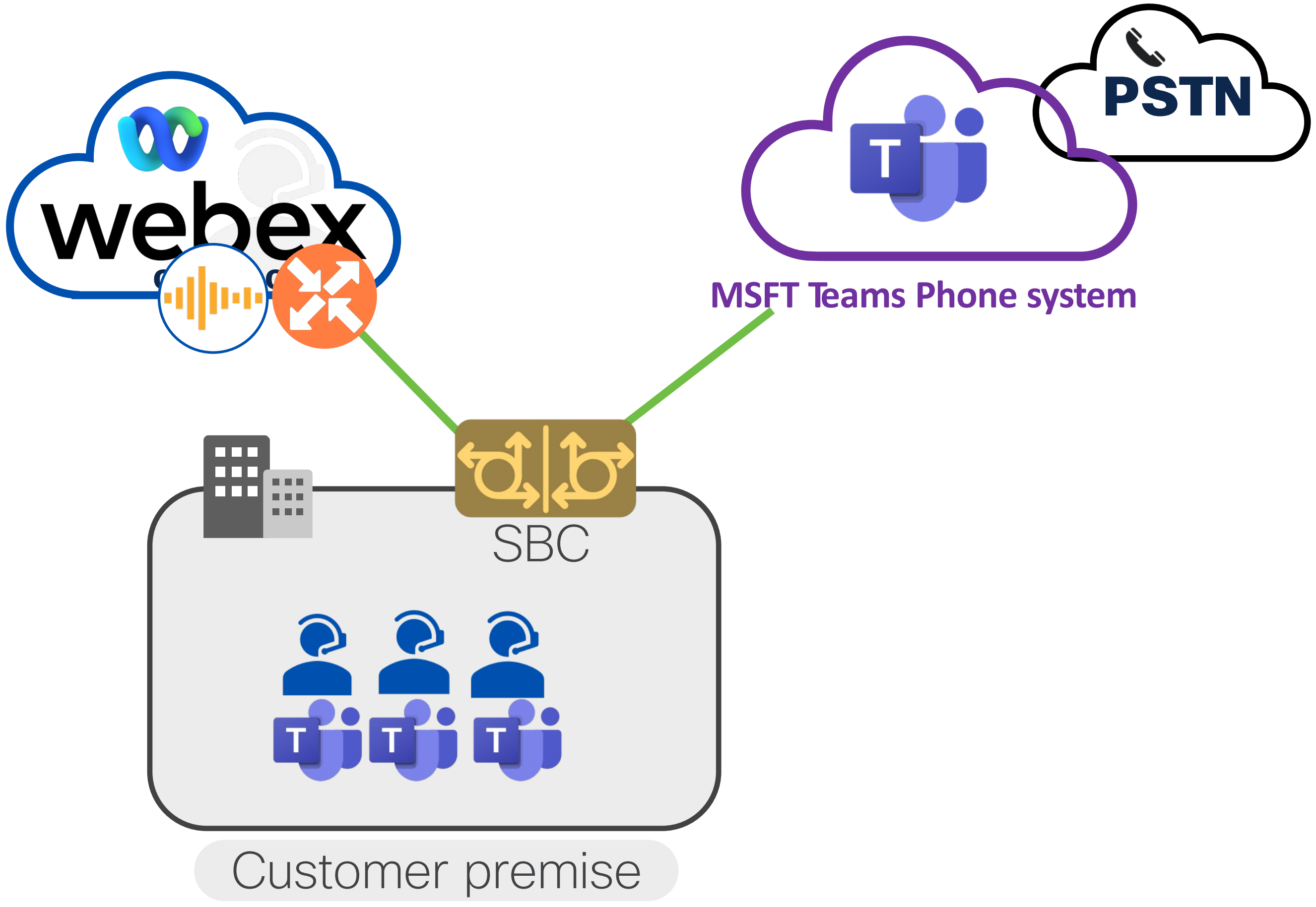


Step 4 – Choose PSTN

- PSTN typically will be part of MSFT Teams Phone System deployment
- Connecting such PSTN will be equivalent to an on-premise PSTN integration from Webex Contact Center perspective

Customer 3 – MSFT Teams Phone System

US based customer just spent $$$ on E5 licenses and wants agents to be able to transfer CC calls to office backend MSFT Teams users. They also want presence synchronization.



Step 5 – Choose Agent Call Delivery

- Dictated by customer requirement
- Agents Login to Webex Contact Center Agent desktop with MS Teams +E164 DID
- Webex Contact Center has Presence integration with MSFT Teams and Consult/Transfer to MSFT Teams backend users

Can we optimize the deployment cost?

- Suggest the use of WebRTC Agents as agents are anyway using Browser as Agent Desktop

MSFT Teams Integration options

Connect Model

Most common level of integration

- Uses certified SBC and direct routing to connect to MS Phone System
- Calls arrive via SBC to WxCC
- WxCC finds the right agent (Teams user) and then sends the call to MS Teams via the SBC

Extend Model

Use Azure Bots and Graph Api's

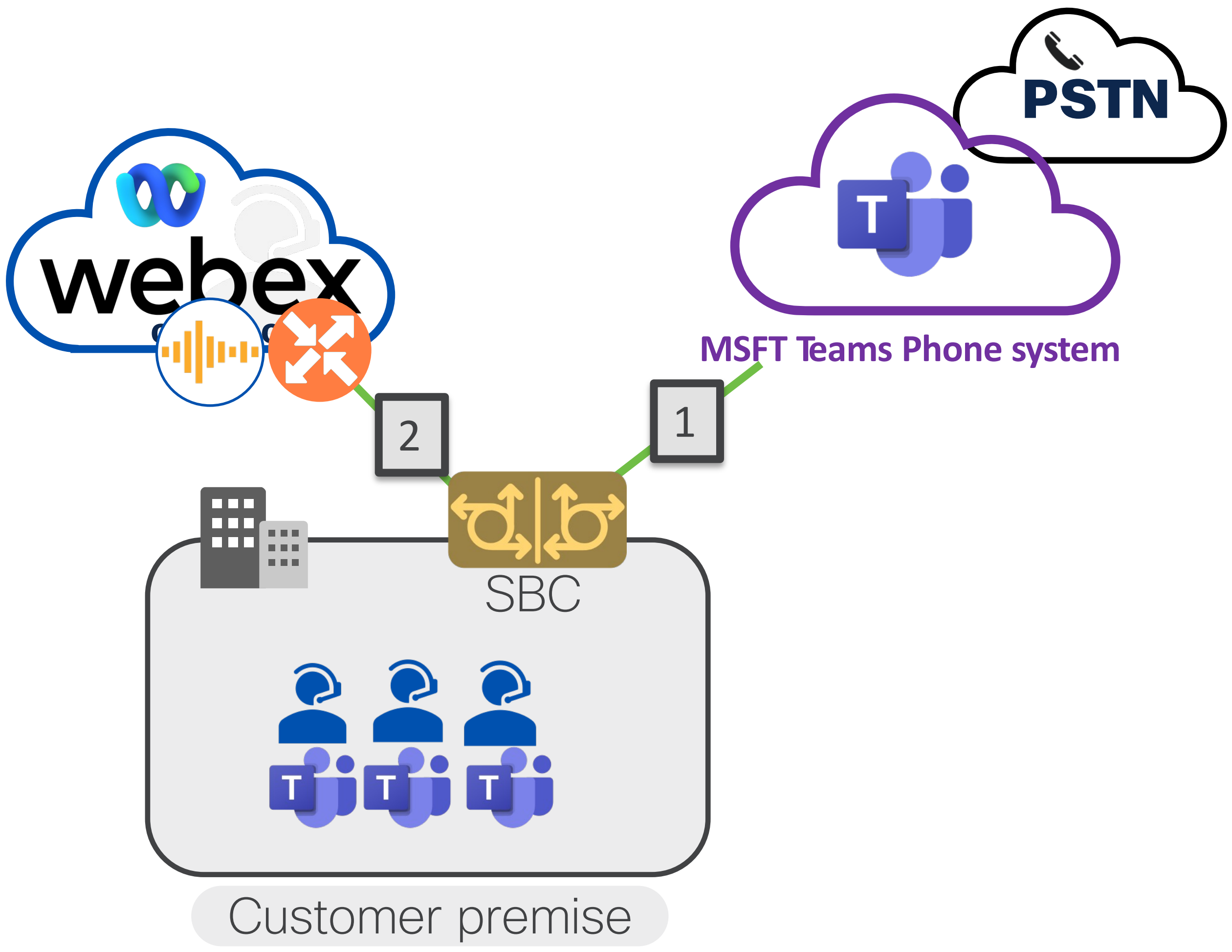
- Utilizing teams calling infrastructure
- Calls arrive and are handled in the team's platform.
- WxCC tells teams how to route calls

Power Model

Allows the use of SDK

- Allows to embed native team's experience in Apps
- Extended Contact Centre capabilities can be adopted

SBC Configurations

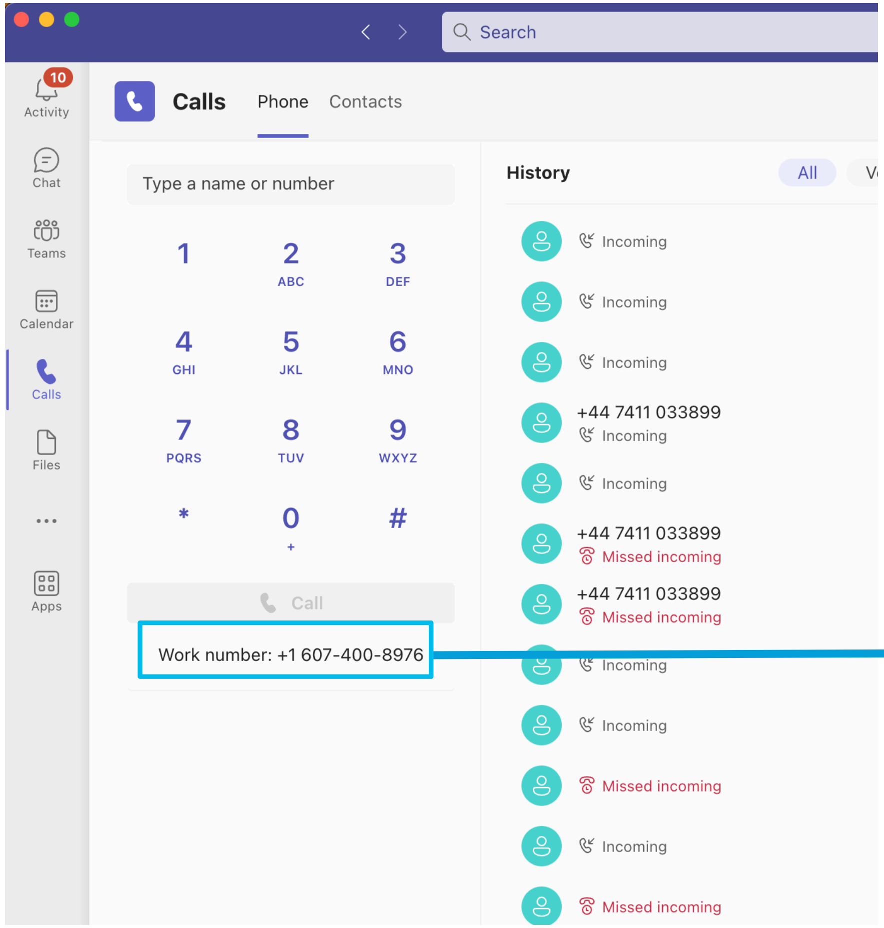


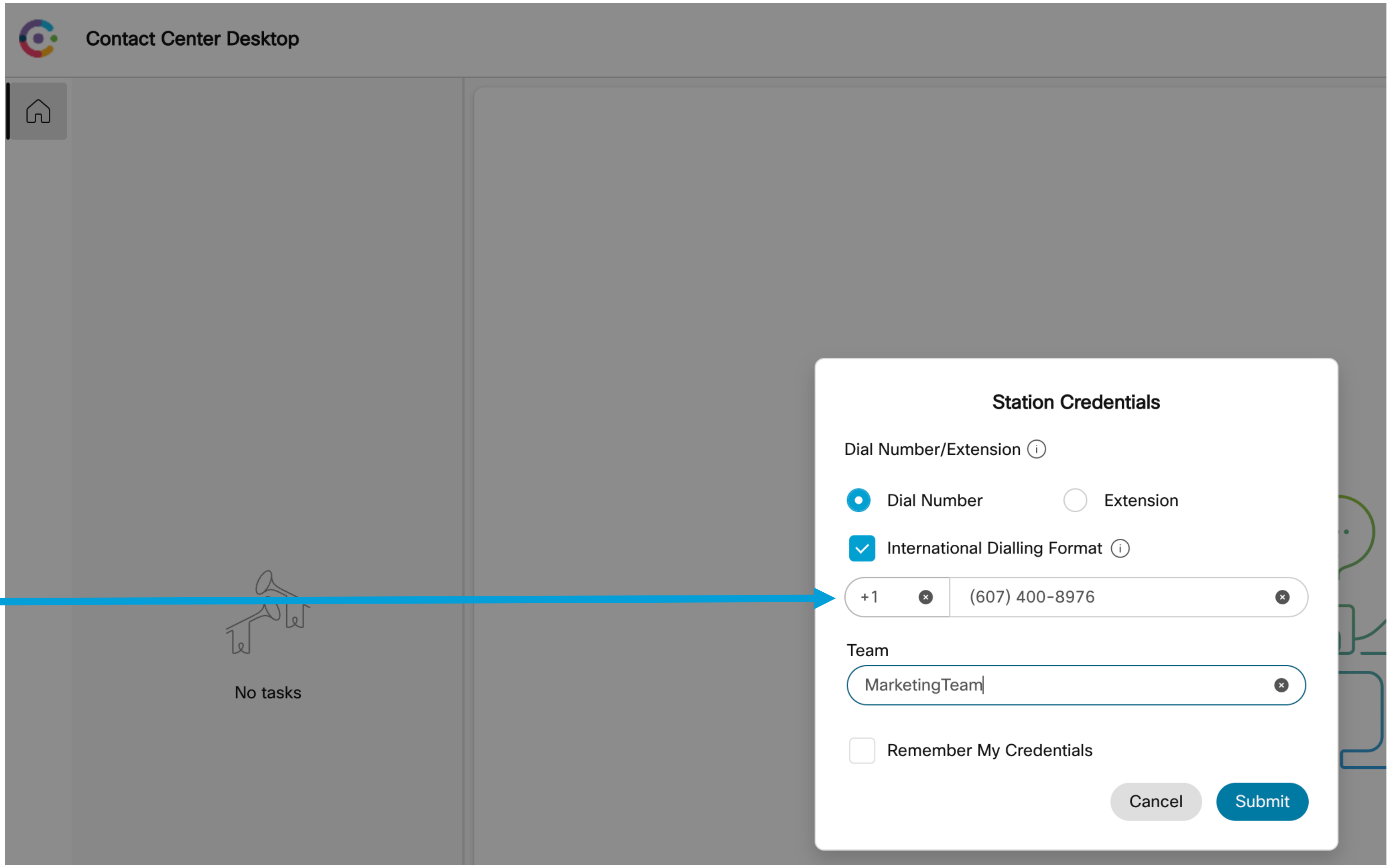
1. Direct Routing SBC to MSFT Teams

2. SBC to VPOP

See appendix

Agent Login using MSFT Teams DID

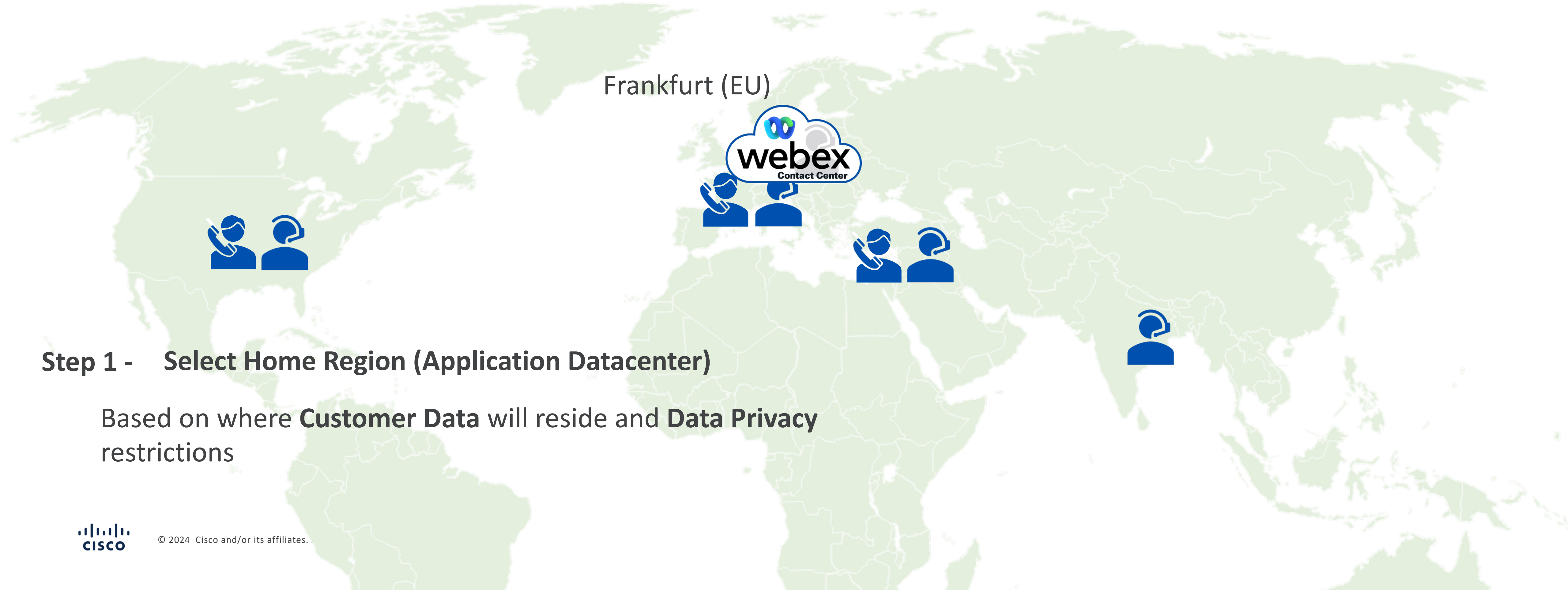




Use case #4

Customer 4 – Global customer with PSTN and Agents spread around the globe

Customer wants a Cloud contact center solution that can serve all the countries they have presence, including USA, EU, and UAE with some agents in India



Step 1 - **Select Home Region (Application Datacenter)**

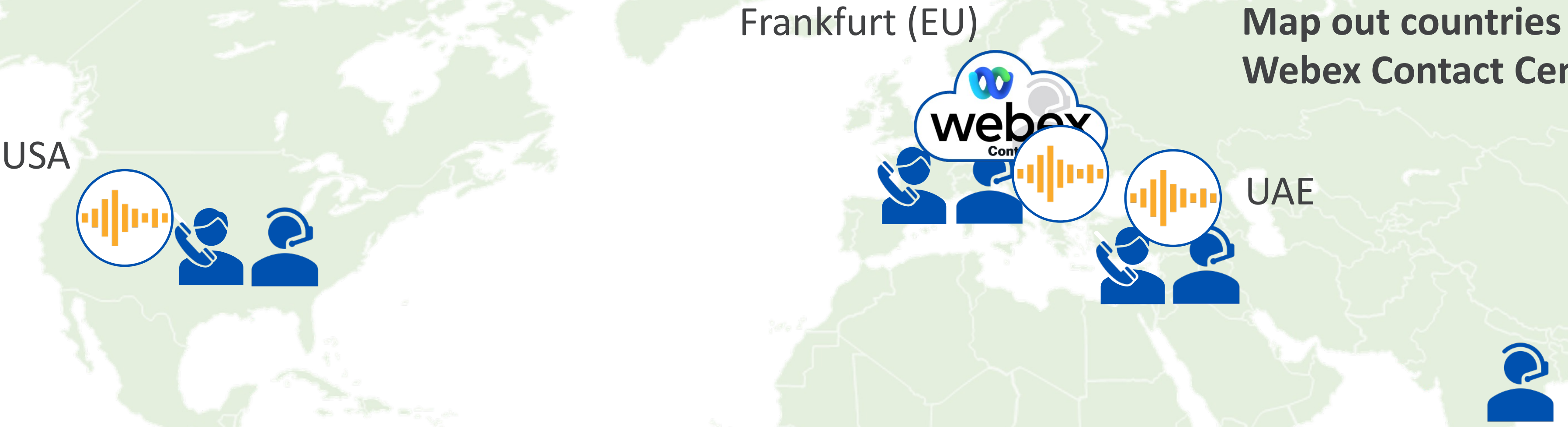
Based on where **Customer Data** will reside and **Data Privacy** restrictions

Customer 4 – Global customer with PSTN and Agents spread around the globe

Customer wants a Cloud contact center solution that can serve all the countries they have presence, including USA, EU, and UAE with some agents in India

Step 2- Select PSTN Region(s)

Map out countries with PSTN requirements to Webex Contact Center PSTN regions

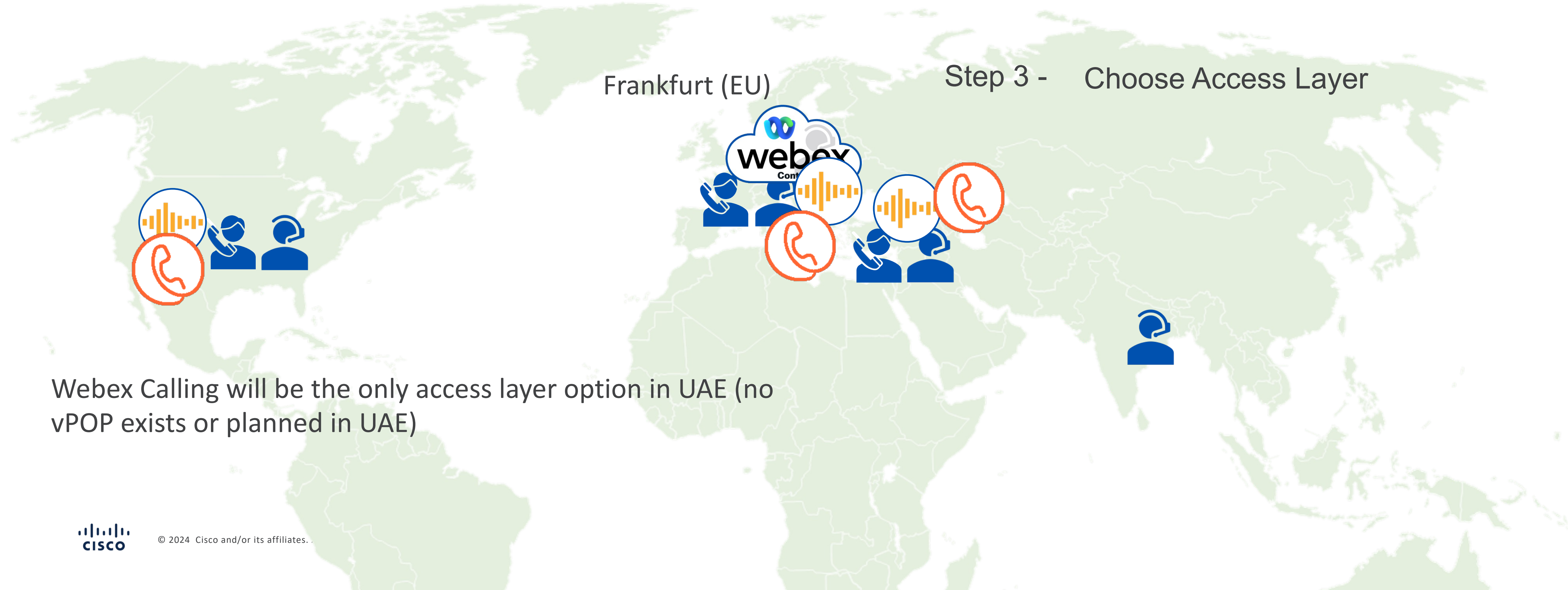


EU, US already have **Media Processing Layer** deployed
UAE will have it soon. As **New PSTN Regions** become available, they **light up** also in existing Webex Contact Center Tenants

Customer 4 – Global customer with PSTN and Agents spread around the globe

Customer wants a Cloud contact center solution that can serve all the countries they have presence, including USA, EU, and UAE with some agents in India

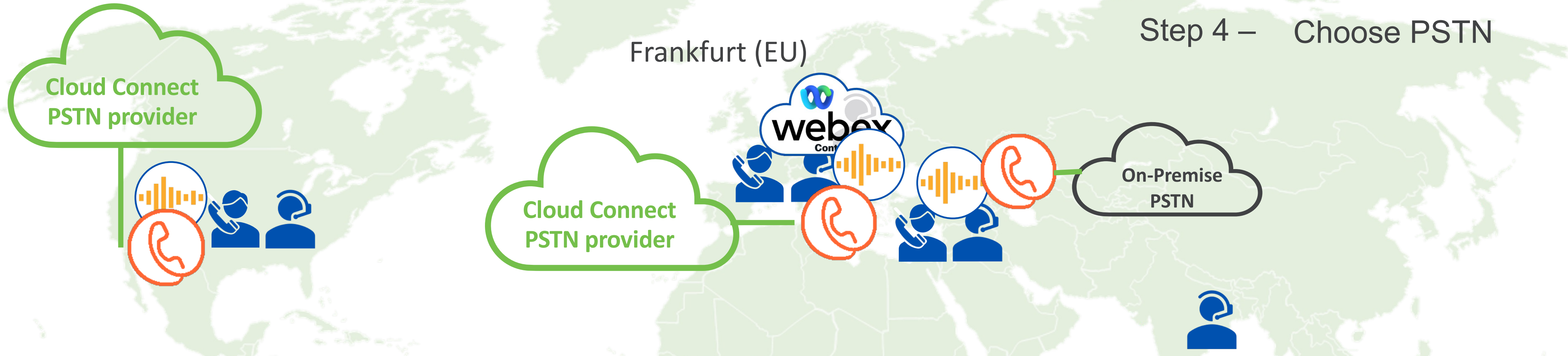
Step 3 - Choose Access Layer



Webex Calling will be the only access layer option in UAE (no vPOP exists or planned in UAE)

Customer 4 – Global customer with PSTN and Agents spread around the globe

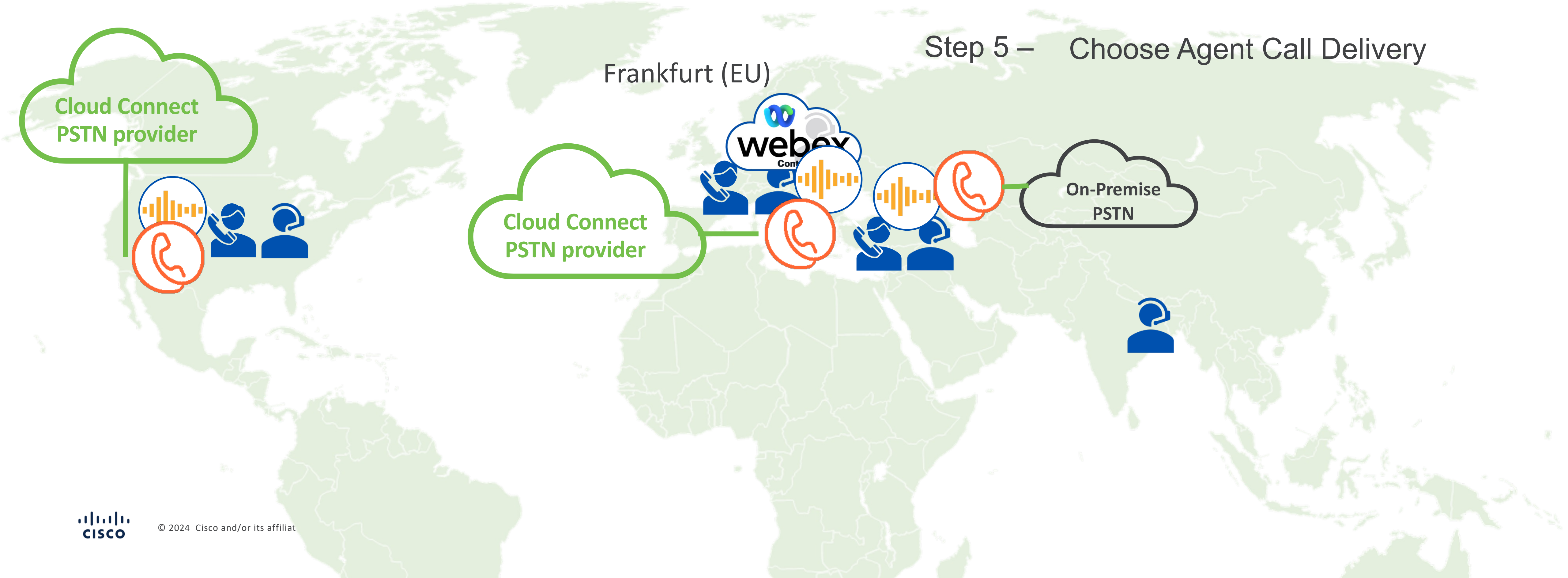
Customer wants a Cloud contact center solution that can serve all the countries they have presence, including USA, EU, and UAE with some agents in India



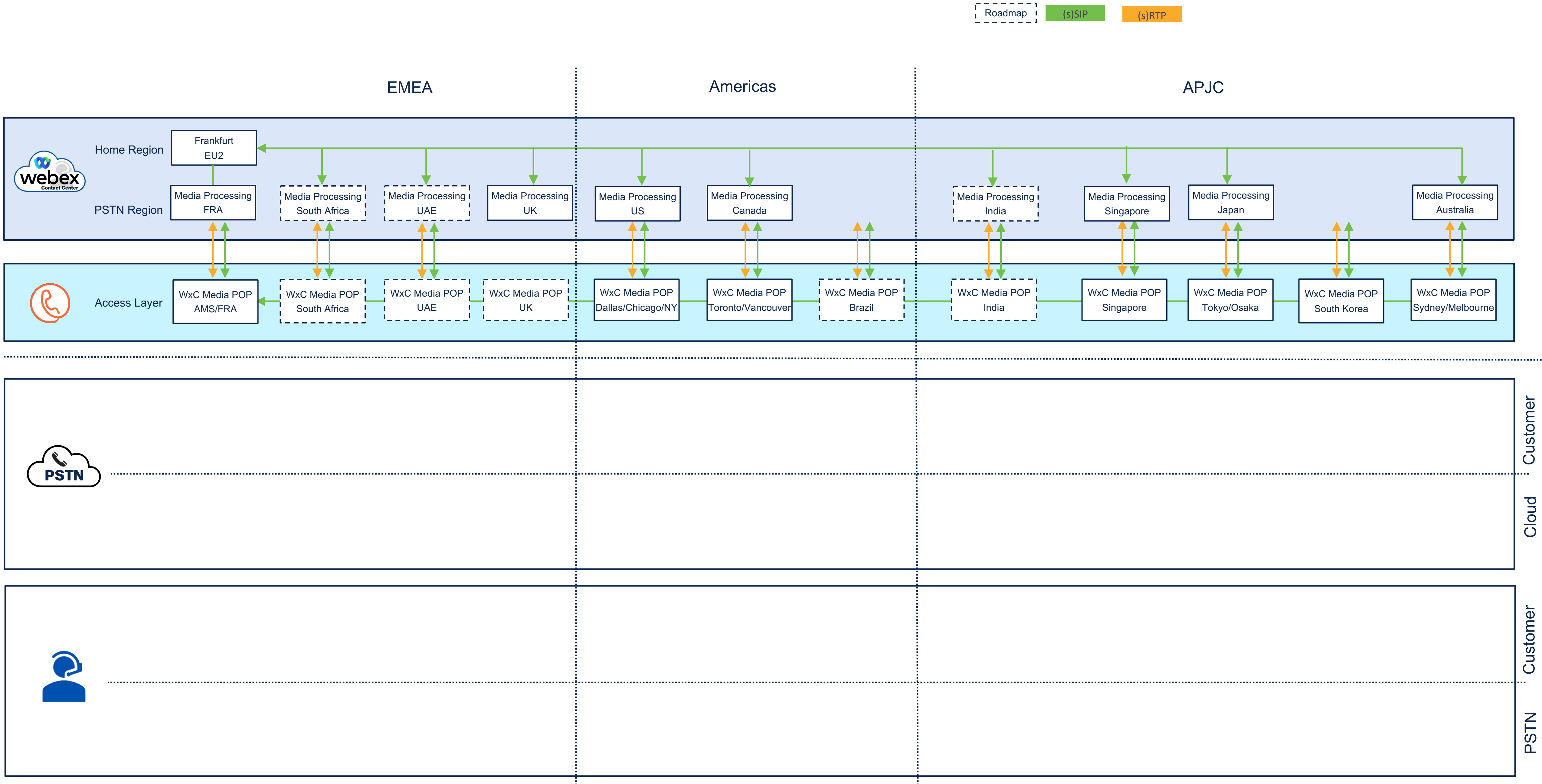
- PSTN options can be different based on customer requirements and ease of migration for each CC site
- Agent Call Delivery method in India has to be compliant with regulations
  https://help.webex.com/en-us/article/7q0b45/Enable-Webex-Calling-for-India-locations

Customer 4 – Global customer with PSTN and Agents spread around the globe

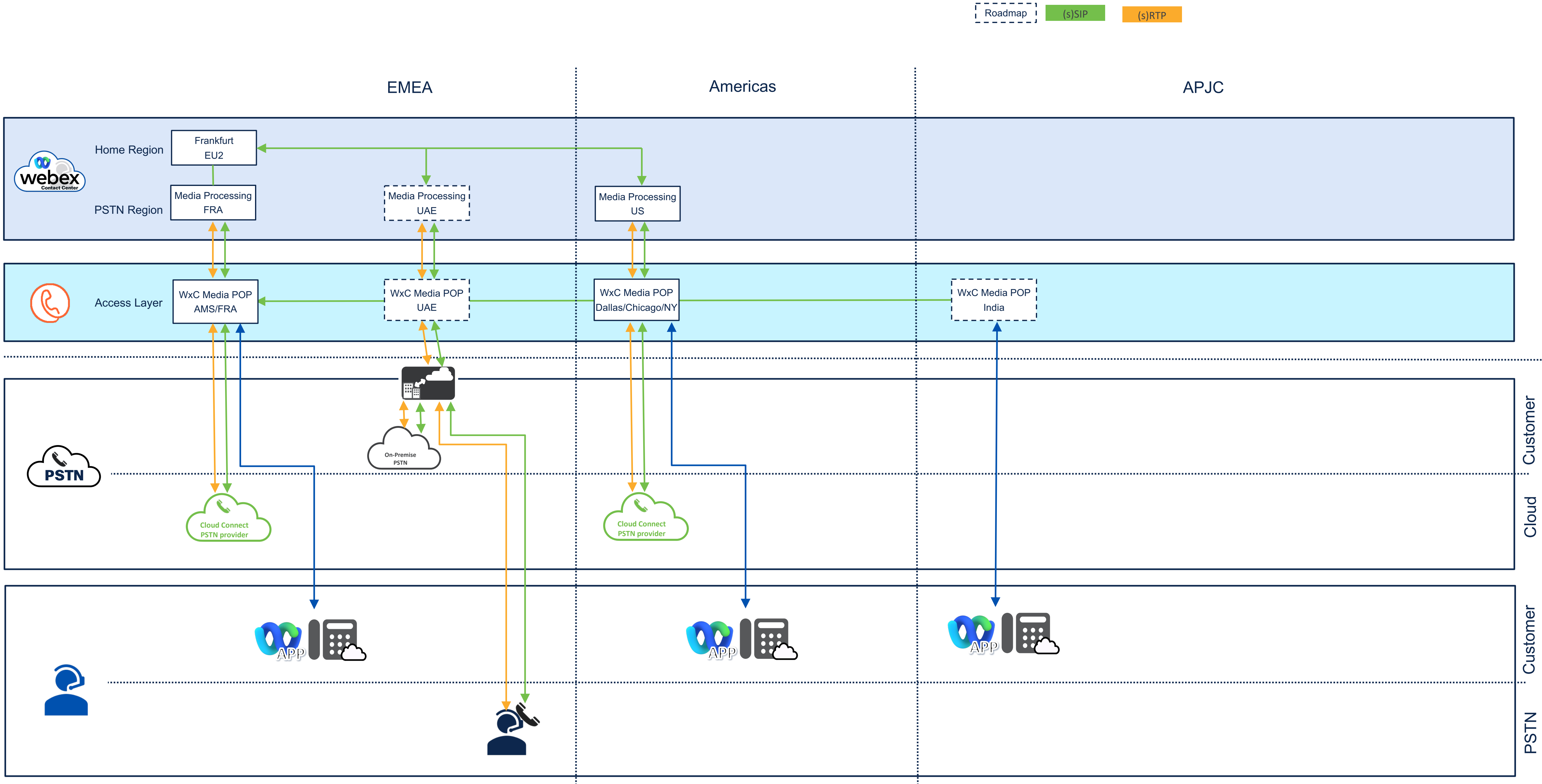
Customer wants a Cloud contact center solution that can serve all the countries they have presence, including USA, EU, and UAE with some agents in India



A2Q standard diagrams (Draft)



Roadmap
(s)SIP
(s)RTP
EMEA
Americas
APJC
Home Region
PSTN Region
Frankfurt EU2
Media Processing FRA
Media Processing South Africa
Media Processing UAE
Media Processing UK
Media Processing US
Media Processing Canada
Media Processing India
Media Processing Singapore
Media Processing Japan
Media Processing Australia
Access Layer
WxC Media POP AMS/FRA
WxC Media POP South Africa
WxC Media POP UAE
WxC Media POP UK
WxC Media POP Dallas/Chicago/NY
WxC Media POP Toronto/Vancouver
WxC Media POP Brazil
WxC Media POP India
WxC Media POP Singapore
WxC Media POP Tokyo/Osaka
WxC Media POP South Korea
WxC Media POP Sydney/Melbourne
PSTN
Customer
Cloud
Customer
PSTN



Roadmap
(s)SIP
(s)RTP
EMEA
Americas
APJC
webex Contact Center
Home Region
Frankfurt EU2
PSTN Region
Media Processing FRA
Media Processing UAE
Media Processing US
Access Layer
WxC Media POP AMS/FRA
WxC Media POP UAE
WxC Media POP Dallas/Chicago/NY
WxC Media POP India
PSTN
On-Premise PSTN
Cloud Connect PSTN provider
Cloud Connect PSTN provider
APP
APP
APP
Customer
Cloud
Customer
PSTN

Your homework! (actual customer requirements)

- Global Customer spread across APAC, EMEA and NA
- APAC – Indonesia, S. Korea
- EMEA – Netherlands, Germany
- NA – Canada and US
- Telco Termination
    - In Country termination
    - S. Korea – Long term contract with existing telco
    - Indonesia – Open for telco in the cloud
    - Netherlands and Germany – Open for telco in the cloud

PBX Used

- MS Teams for Knowledge Workers (Globally)
    - Desire to extend MS Teams to Contact Center agents
- Webex Calling
    - Testing Webex Calling for one region, and willing to explore for other regions
- North America and EMEA
    - On-Premise CUCM

Recap

Appendix

Additional MS teams integration info

MSFT License Requirement

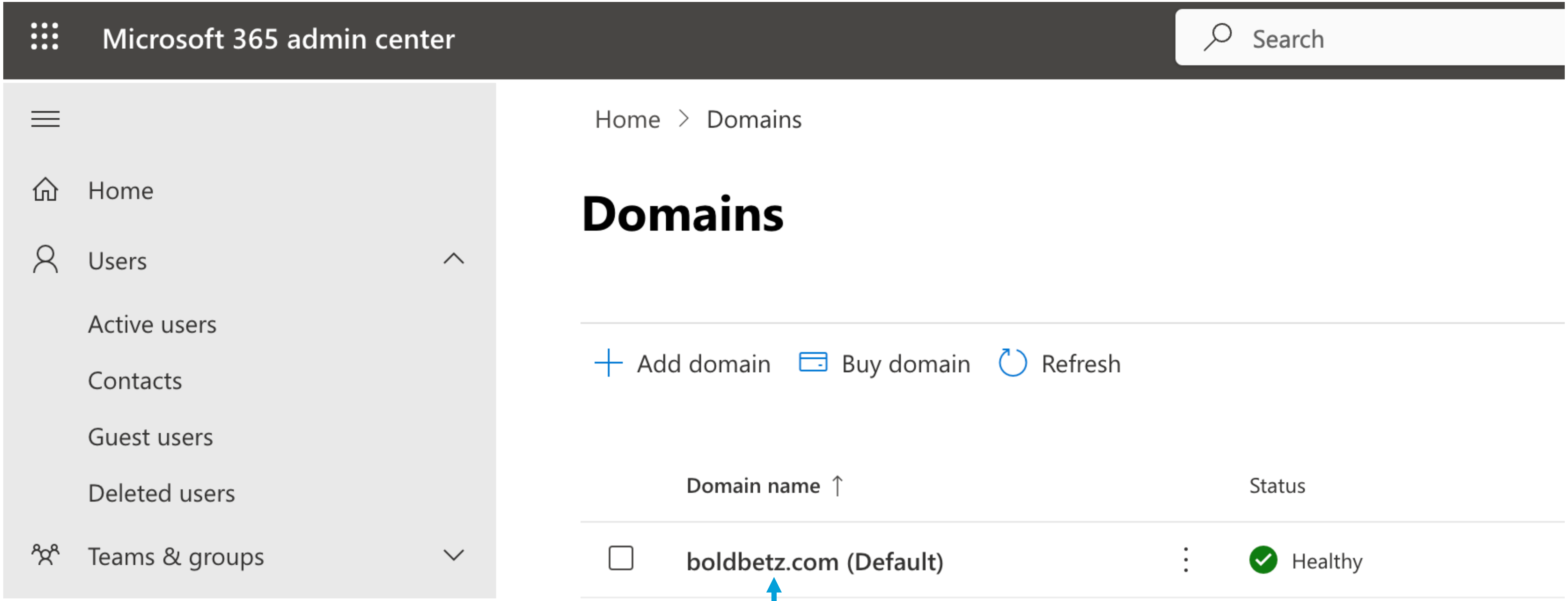
MSFT E5 licenses (MSFT Phone System License included)

MSFT 365 Business Basic, Standard or Premium and Teams Phone Standard (incl. MSFT phone system and Calling)

MSFT 365 E1/E3 or A1/G1 or A3/G3, Teams Phone Standard and MSFT Calling(incl MSFT Phone System)

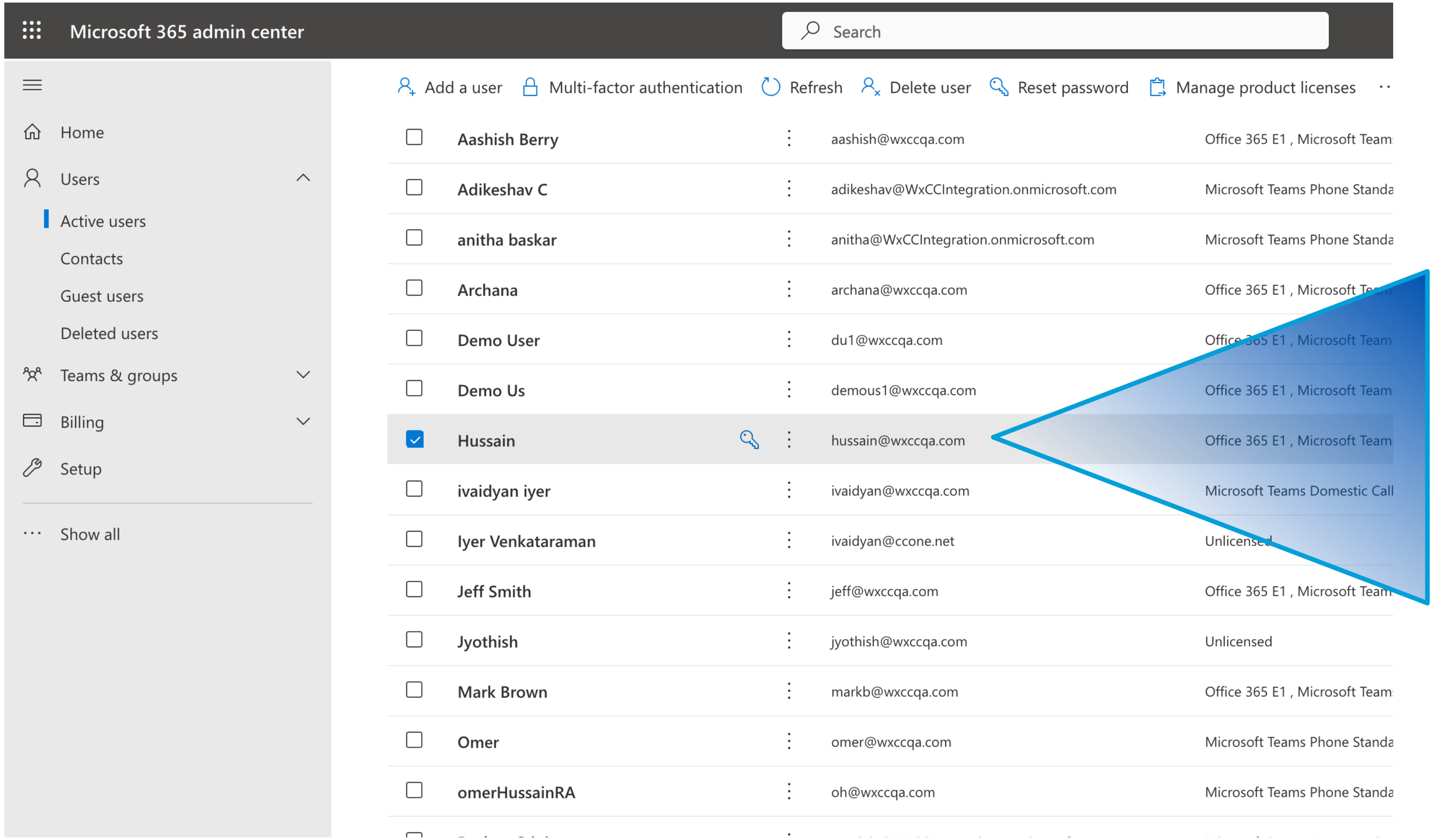
MSFT License Options

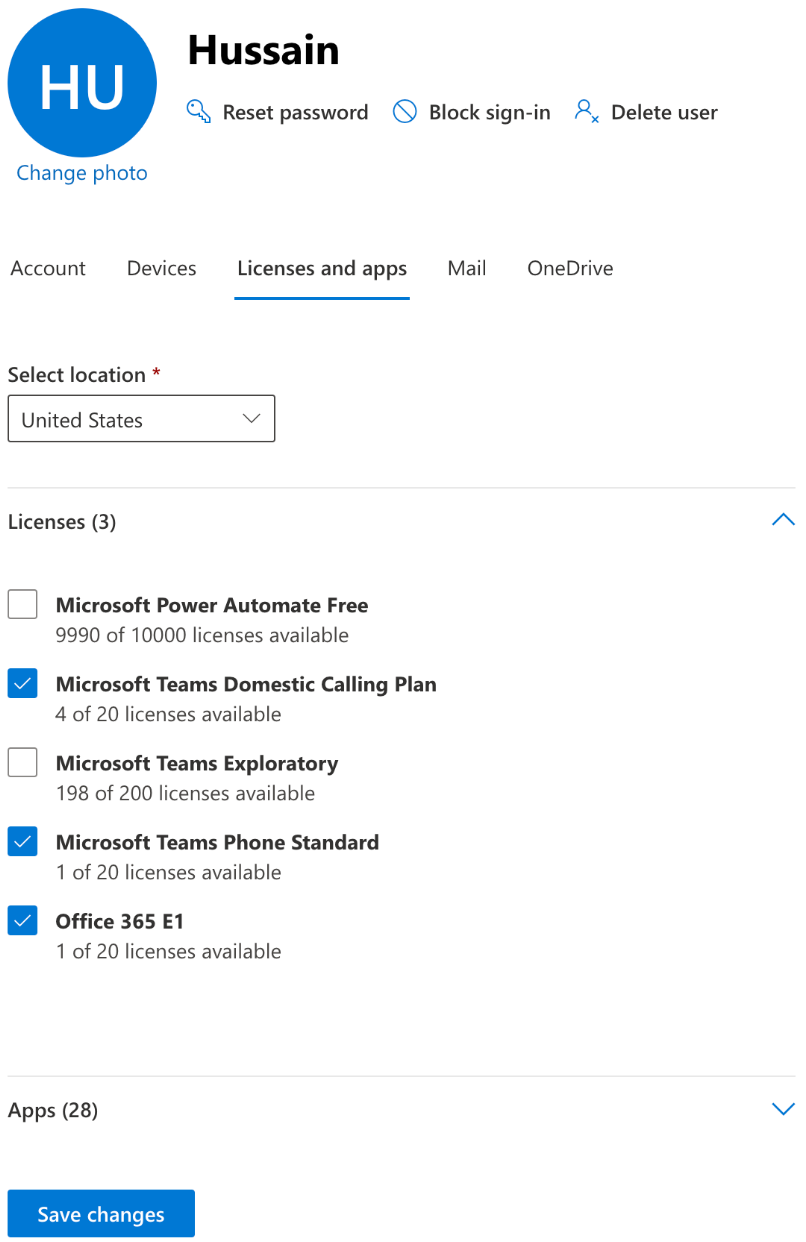
Microsoft Domain Verification



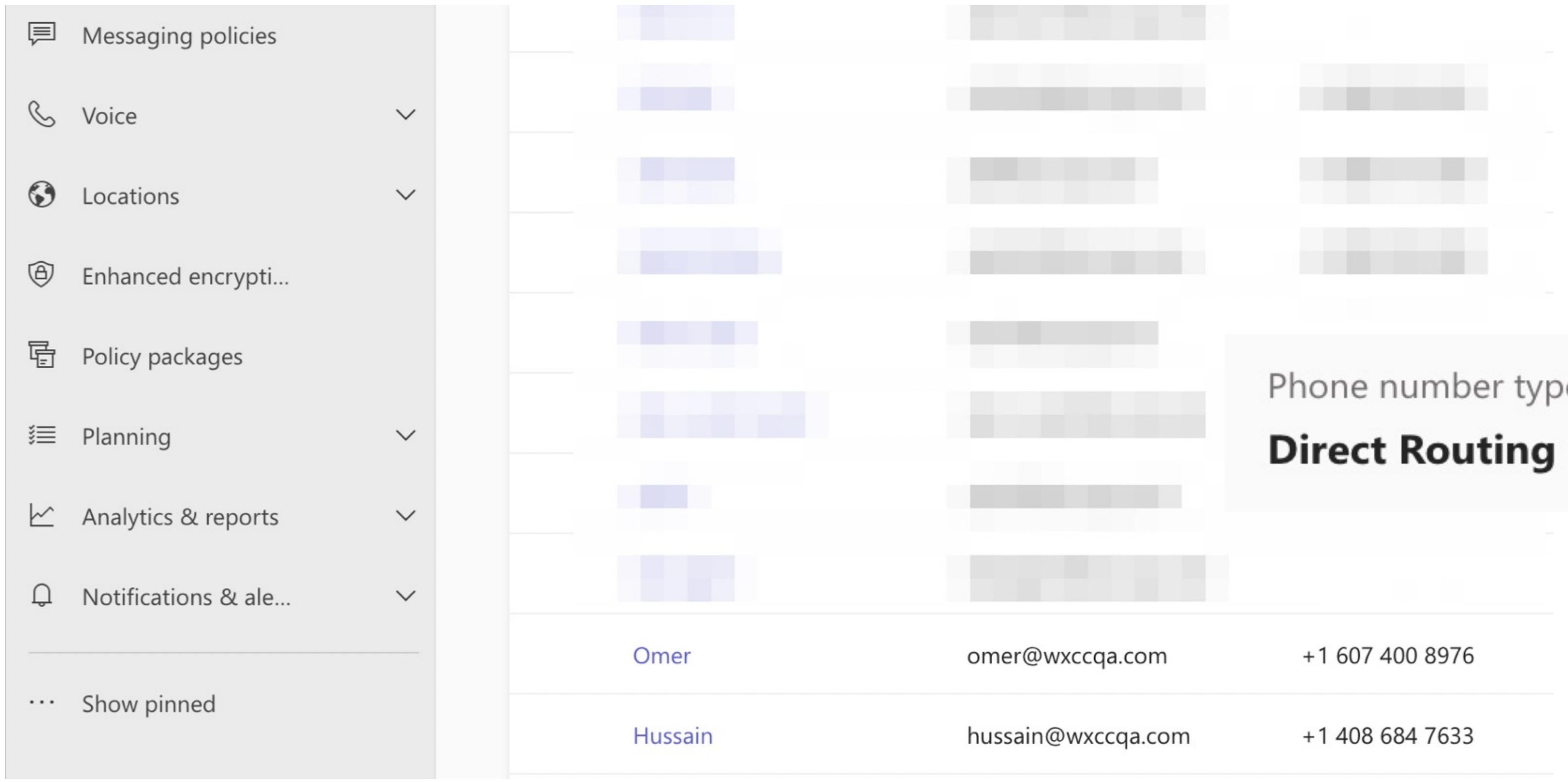
Make sure your domain is verified and in Healthy state

Assign Licenses to the users

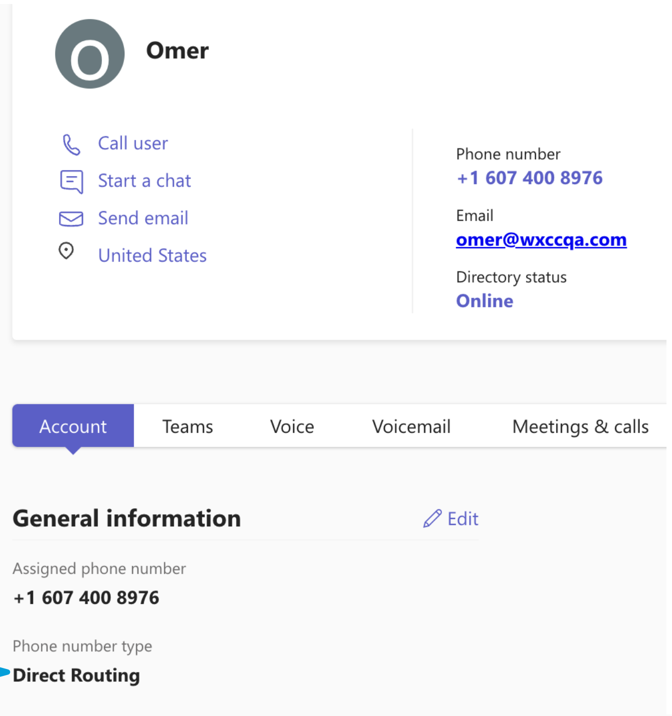


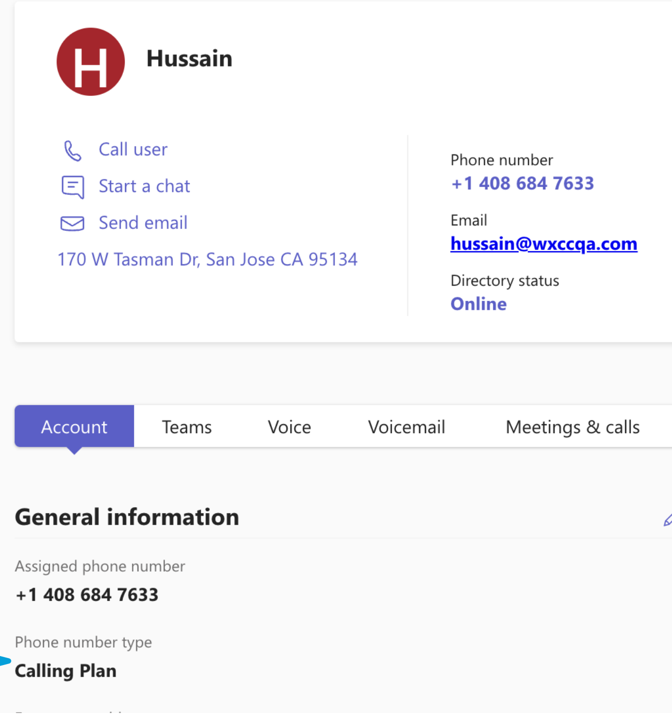


Microsoft Teams – Admin portal (Users)



Phone number type
Direct Routing





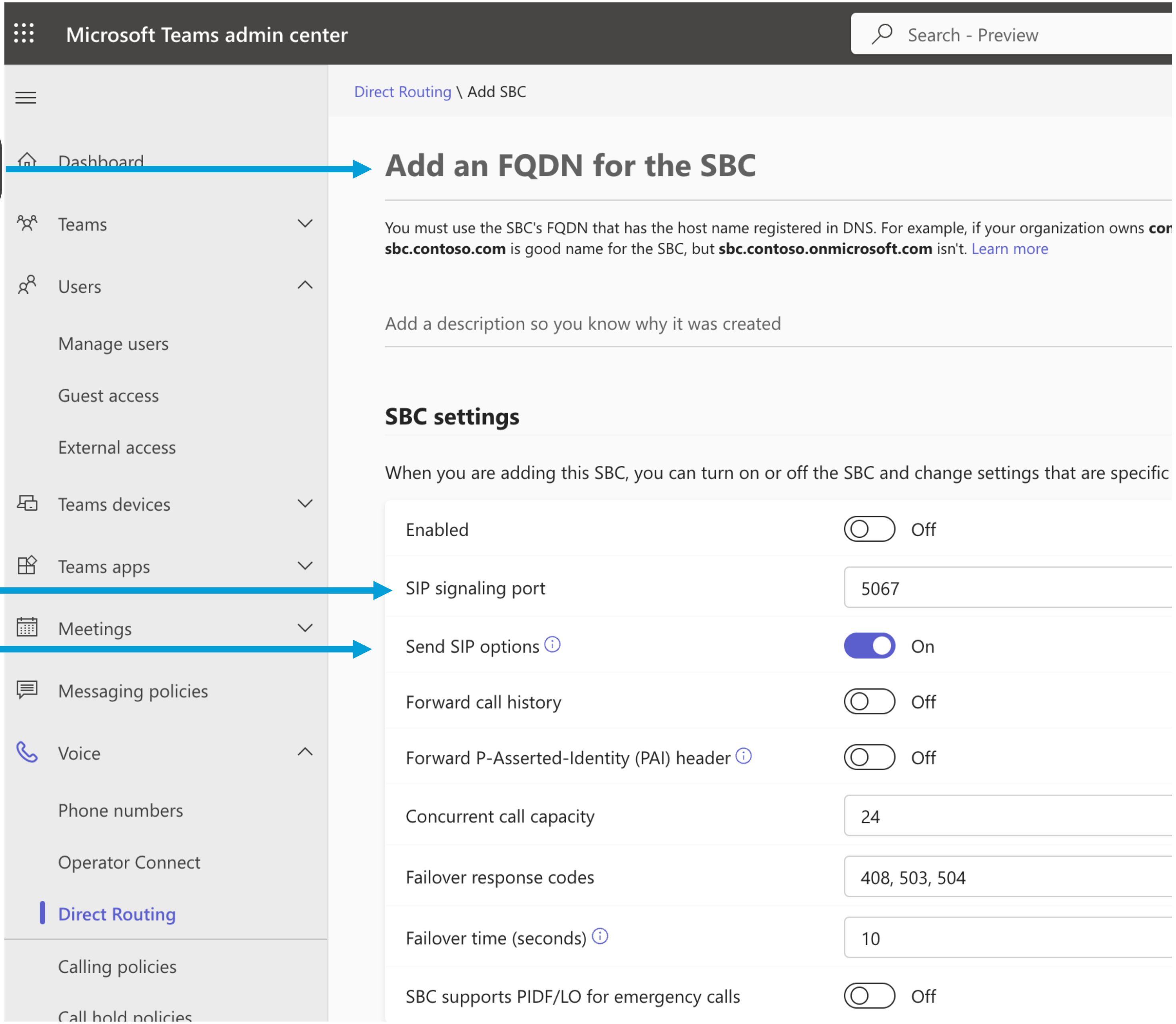
Phone number type
Calling Plan

Configuring Direct Routing(Voice -> Direct Routing)

Provide the FQDN for your SBC

Port to connect to SBC

Enable SIP Options to maintain trunk availability



CUBE Configurations
- Direct Routing
- WxCC

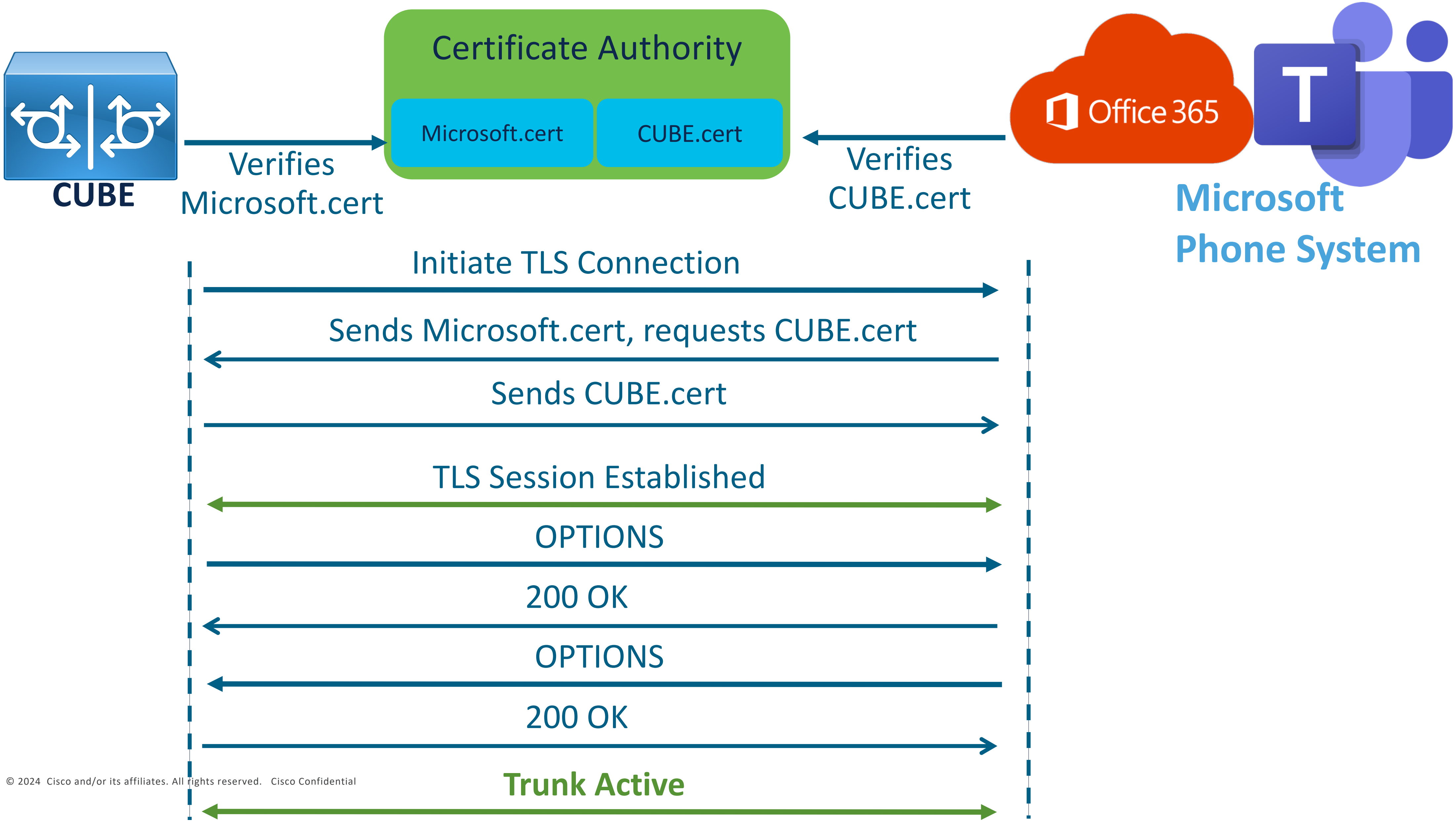
Direct Routing Configuration

References in this presentation

- The presentation uses the following in screenshots / command lines

Top level Domain	cube-tme.com
SBC/CUBE's FQDN (should be publicly reachable – even though CUBE can be behind a NAT)	sbc2.cube-tme.com
Static Public IP associated with the CUBE FQDN	198.135.2.118
CUBE SSL certificate issued by	GoDaddy

Establishing Secure Connectivity b/w CUBE and Teams with mutual TLS



SIP OPTIONS to Microsoft `(debug ccsip non-call)`

```
Sent:
OPTIONS sip:sip.pstnhub.microsoft.com:5061;user=phone SIP/2.0
Via: SIP/2.0/TLS 198.135.2.118:5061;branch=z9hG4bK1DDA183F
From: <sip:sbc2.cube-tme.com>;tag=3FFCBCEA-65F
To: <sip:sip.pstnhub.microsoft.com>
Date: Wed, 20 May 2020 05:37:10 GMT
Call-ID: C93E2513-999211EA-BC31FAE3-190A3E31@198.135.2.118
User-Agent: Cisco-SIPGateway/IOS-17.2.1r
X-MS-SBC: Cisco UBE/ISR4321/IOS-17.2.1r
Max-Forwards: 70
CSeq: 101 OPTIONS
Contact: <sip:sbc2.cube-tme.com:5061;transport=tls>
Content-Length: 0
```

200 OK From Microsoft

```
Received:
SIP/2.0 200 OK
FROM: <sip:sbc2.cube-tme.com>;tag=3FFCBCEA-65F
TO: <sip:sip.pstnhub.microsoft.com>
CSEQ: 101 OPTIONS
CALL-ID: C93E2513-999211EA-BC31FAE3-190A3E31@198.135.2.118
VIA: SIP/2.0/TLS 198.135.2.118:5061;branch=z9hG4bK1DDA183F
CONTENT-LENGTH: 0
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
SERVER: Microsoft.PSTNHub.SIPProxy v.2020.5.13.3 i.USEA.3
```

SIP OPTIONS From Microsoft

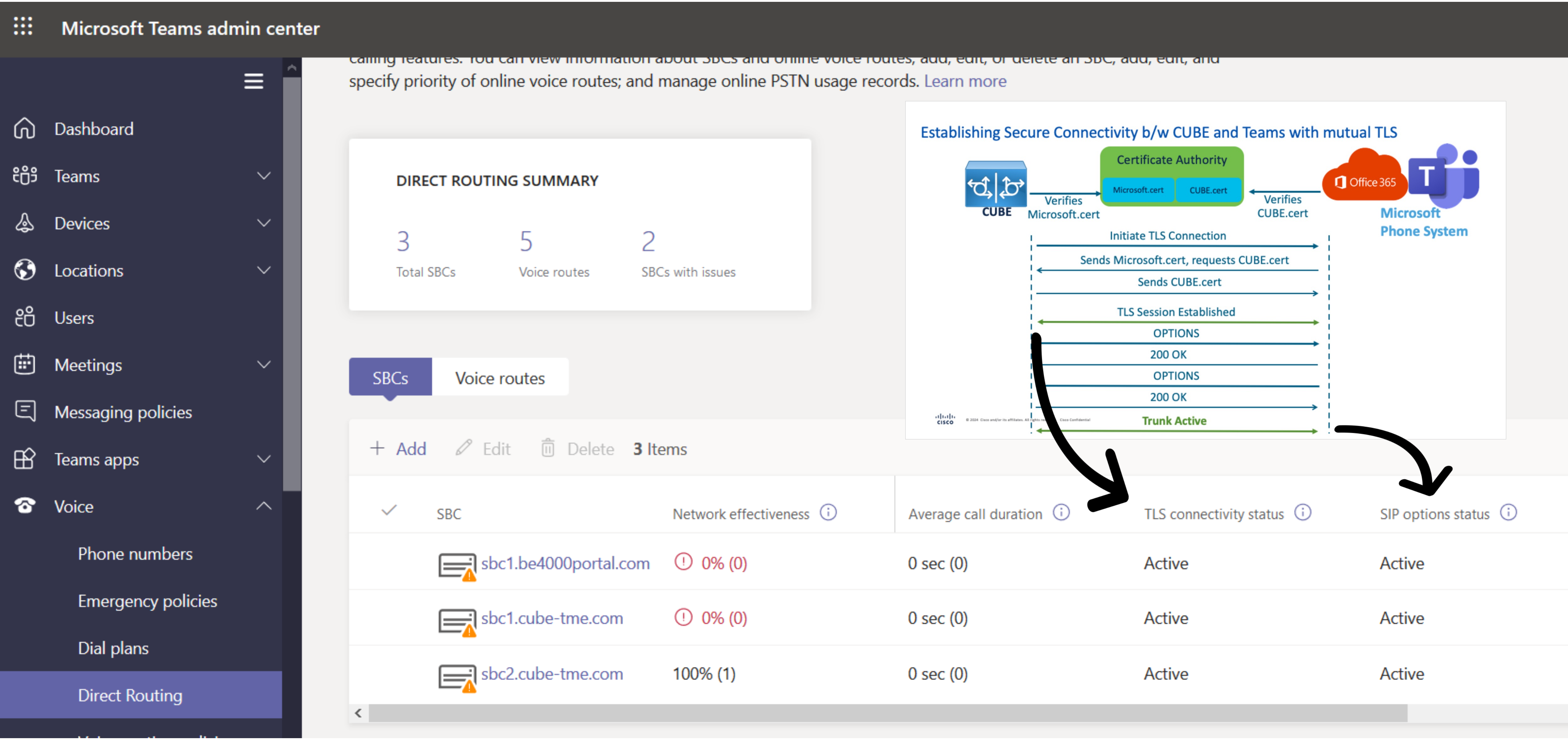
```
Received:
OPTIONS sip:sbc2.cube-tme.com:5061;transport=tls SIP/2.0
FROM: <sip:sip-du-a-us.pstnhub.microsoft.com:5061>;tag=be0ffb4b-a7ac-
47ff-bc9f-9e97dd1728f8
TO: <sip:sbc2.cube-tme.com>
CSEQ: 1 OPTIONS
CALL-ID: 5c421d1e-8e04-4149-9a72-0185a6abe314
MAX-FORWARDS: 70
VIA: SIP/2.0/TLS 52.114.132.46:5061;branch=z9hG4bK2b28d4c2
CONTACT: <sip:sip-du-a-us.pstnhub.microsoft.com:5061>
CONTENT-LENGTH: 0
USER-AGENT: Microsoft.PSTNHub.SIPProxy v.2020.5.13.3 i.USEA.3
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
```

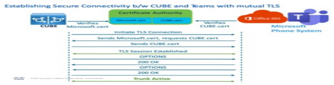
200 OK To Microsoft

```
Sent:
SIP/2.0 200 OK
Via: SIP/2.0/TLS 52.114.132.46:5061;branch=z9hG4bK2b28d4c2
From: <sip:sip-du-a-us.pstnhub.microsoft.com:5061>;tag=be0ffb4b-a7ac-47ff-bc9f-9e97dd1728f8
To: <sip:sbc2.cube-tme.com>;tag=3FFCD85D-48C
Date: Wed, 20 May 2020 05:37:17 GMT
Call-ID: 5c421d1e-8e04-4149-9a72-0185a6abe314
Server: Cisco-SIPGateway/IOS-17.2.1r
X-MS-SBC: Cisco UBE/ISR4321/IOS-17.2.1r
CSeq: 1 OPTIONS
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Accept: application/sdp
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Content-Type: application/sdp
Content-Length: 373

v=0
o=CiscoSystemsSIP-GW-UserAgent 1823 3082 IN IP4 198.135.2.118
s=SIP Call
c=IN IP4 198.135.2.118
t=0 0
m=audio 0 RTP/AVP 18 0 8 9 4 2 15 3
c=IN IP4 198.135.2.118
m=image 0 udptl t38
c=IN IP4 198.135.2.118
a=T38FaxVersion:0
a=T38MaxBitRate:9600
a=T38FaxRateManagement:transferredTCF
a=T38FaxMaxBuffer:200
a=T38FaxMaxDatagram:320
a=T38FaxUdpEC:t38UDPRedundancy
```

TLS Sockets

```
sbc2#show sip-ua connection tcp tls detail
Total active connections      : 6
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 1
No. of inactive conn. ageouts : 0
TLS client handshake failures : 1
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:52.114.76.76, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher                          Curve
  =========== ======= =========== =========== ============= =========== =============================== =====
         5061       8 Established           0 70.237.100.25     TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-384
         5128       9 Established           0 70.237.100.25     TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:52.114.7.24, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher                          Curve
  =========== ======= =========== =========== ============= =========== =============================== =====
         5061       5 Established           0 70.237.100.25     TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-384
         7232       7 Established           0 70.237.100.25     TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:52.114.148.0, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher                          Curve
  =========== ======= =========== =========== ============= =========== =============================== =====
         5061       3 Established           0 70.237.100.25     TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-384
         3136       6 Established           0 70.237.100.25     TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-256
```


Microsoft Teams admin center
calling features. You can view information about SBCs and online voice routes, add, edit, or delete an SBC, add, edit, and
specify priority of online voice routes; and manage online PSTN usage records. Learn more
Dashboard
Teams
Devices
Locations
Users
Meetings
Messaging policies
Teams apps
Voice
Phone numbers
Emergency policies
Dial plans
Direct Routing
DIRECT ROUTING SUMMARY
3
Total SBCs
5
Voice routes
2
SBCs with issues
SBCs
Voice routes
+ Add
Edit
Delete
3 Items
SBC
Network effectiveness
Average call duration
TLS connectivity status
SIP options status
sbc1.be4000portal.com
0% (0)
0 sec (0)
Active
Active
sbc1.cube-tme.com
0% (0)
0 sec (0)
Active
Active
sbc2.cube-tme.com
100% (1)
0 sec (0)
Active
Active
Establishing Secure Connectivity b/w CUBE and Teams with mutual TLS
Certificate Authority
Microsoft.cert
CUBE.cert
CUBE
Verifies
Microsoft.cert
Verifies
CUBE.cert
Office 365
Microsoft
Phone System
Initiate TLS Connection
Sends Microsoft.cert, requests CUBE.cert
Sends CUBE.cert
TLS Session Established
OPTIONS
200 OK
OPTIONS
200 OK
Trunk Active



Direct Routing

Onboarding Process

Platform Licenses and IOS-XE versions

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
14.0	17.3.1a	July 2020	17.3.6
14.1	17.3.2*	Oct 2020	17.3.6
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	17.6.5
14.4	17.7.1a	Nov 2021	17.7.2
14.5	17.8.1a	March 2022	
14.6	17.9.1a	July 2022	17.9.4
14.6	17.10.1a	Nov 2022	
14.6	17.11.1a	March 2023	
14.7	17.12.1a	July 2023	

Last release for ISR4K except ISR4461

Configure Platform Licensing

- Configure required platform license on the gateway
  - Cisco ISR 4000 series -
    - `license boot level uck9`
    - `license boot level securityk9`
  - Cisco Catalyst 8300 and 8200 Series -
    - `license boot level network-advantage addon dna-advantage`
    - `platform hardware throughput crypto 25M`
  - Cisco Catalyst 8000V Edge Software –
    - `license boot level network-advantage addon dna-essential`
    - `platform hardware throughput level MB 1000`

Step by Step CUBE config:
Common Global Configuration

Step 1 :

Base Platform configuration and Certificates

CUBE Reference platform configuration

- Before proceeding with CUBE configuration, ensure baseline platform configuration such as NTPs, ACLs, enable passwords, IP routing, IP Addresses, etc. are configured according to your organization's policies and procedures

- IP address which is advertised in m line of SDP must be publicly reachable and used for media traffic (inbound and outbound). In case NAT is used, it should be bidirectional, and SIP/SDP Profiles should be configured on CUBE appropriately

- Latest of IOS-XE 17.9+ or 17.12+ is recomended.

```
interface GigabitEthernet0/0/0
 description To MS Phone System - Public IP recommended
 ip address 198.135.2.118 255.255.255.0
```

Configure IP Name Server to enable DNS lookup, Domain-name, NTP, and TCP synwait-time

```
CUBE#config terminal
CUBE(config)#hostname sbc2
sbc2(config)#ip domain-name cube-tme.com
sbc2(config)#ip name-server 208.67.222.222 208.67.220.220
sbc2(config)#ntp server 0.us.pool.ntp.org
sbc2(config)#ip tcp synwait-time 5
sbc2(config)#end
```

- DNS Servers: ensure the ip name-server is reachable by successfully pinging it. Used to resolve addresses for Microsoft Direct Routing servers
- Set the same top level domain name for the router as used for the Microsoft 365 tenant: `cube-tme.com`

Certificates

Generate an RSA key pair – sbc2-key

```
crypto key generate rsa general-keys label sbc2-key
modulus 2048 exportable
```

- Most CAs require private key size to be at least 2048 bit

Create a PKI trustpoint for CUBE using the RSA key

```
crypto pki trustpoint sbc2.cube-tme.com
 enrollment terminal
 fqdn sbc2.cube-tme.com
 subject-name CN=sbc2.cube-tme.com
 subject-alt-name sbc2.cube-tme.com
 revocation-check crl
 rsakeypair sbc2-key
```

- **sbc2.cube-tme.com – Trustpoint name can be anything**
- The SBC domain name must be from one of the names registered in Domains of the Microsoft 365 tenant. You cannot use the *.onmicrosoft.com tenant for the FQDN name of the SBC
- FQDN must be reachable by Microsoft Teams and CA, i.e. should resolve to a public IP
- **subject-name CN=sbc2.cube-tme.com –** The certificate needs to have the SBC FQDN as the common name (CN) in the subject field.
- Alternatively, Direct Routing supports a wildcard conforming to standard RFC2818 (HTTP Over TLS) in the SAN.
- https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sbc-domain-names

Generate a CSR on CUBE

```
crypto pki enroll sbc2.cube-tme.com

% Start certificate enrollment..

% The subject name in the certificate will include: cn=sbc2.cube-tme.com
% The subject name in the certificate will include: sbc2.cube-tme.com
Display Certificate Request to terminal? [yes/no]: yes
```

- Input certificate details, make sure the CN is the CUBE FQDN https://www.sslshopper.com/csr-decoder.html
- Copy and save the CSR
- Send the CSR to your CA, who will send back a certificate for the host and also the root/intermediate CAs
- You may need to add the CUBE FQDN `(sbc2.cube-tme.com)` record to your public DNS before your CA will issue you the cert
- Note: CSCsk85992 – IOS-XE platform does not add the subjectAltName (Subject Alternative Name) extension to a certificate signing request (CSR)

Paste Certificate Signing Request (CSR)

-----BEGIN CERTIFICATE REQUEST-----
MIICpDCCAYwCAQAwPjEaMBgGA1UEAxMRc2JjMi5jdWJlLXRtZS5j
hkiG9w0BCQIWEXNiYzIuY3ViZS10bWUuY29tMIIBIjANBgkqhkiG9
AQ8AMIIBCgKCAQEAjBuVXcBKtrPeAHQM1ips3MxaDYlZT6e9N1h
EtIQPvVnFDjSXS2LTMx9FHnmdpEgYkGOzxVjdd0G+aVcsrG/JqtJeS
yJT86Yre9M5uvswEWiwYy/uq3nz3CDFd5NpyUa3sHYqsdnY5/nAo
2T12i3jMpIMqjoDAnP2izd/zPqJBouRPAkx5LVVGATYm1mjfcggAW
KbuoE0Hqaot89mkJxVYKdTHFKZGt1xtQy8QXNMzyiXAe/ElqTbTi5
vCOzcA3ecOWrjrTsbd5hinLq654cyF1c2YVSTQIDAQABoCEwHwYJ
MRIwEDAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQAD
DTCNQTOpzsCjqI6f5l1z6/DGISwy2Lvm5j9SdTZZ7M7NZndEcFubq
c8az2Ss6i0fWP5+JxF1ptbWy1ValsA4fxSgeSHNS2nvLriy9el3F7u8H
B1J5hdtqRzanCLR1IJgTKRFWqOM/NHqgTWX4LpDmePIq66XAsv+
2b3kCUGYL324Ys1+9VfuoUeSKUj4lccwNaZmRImCGF0ItgUnCUPk
JeuxjTJFdu1MZtXYMfXFCV99axLEgAuGl6Acp6LtpQfvE0rgWgKv+22
Ke9XS3t4KYM=
-----END CERTIFICATE REQUEST-----

CSR Information:

Common Name: sbc2.cube-tme.com

Import Cisco Trusted Root CA bundle to validate Microsoft

```
crypto pki trustpool policy
 no cabundle url http://www.cisco.com/security/pki/trs/ios_core.p7b
 cabundle url http://www.cisco.com/security/pki/trs/ios.p7b
 revocation-check crl
crypto pki trustpool import ca-bundle
```

Create PKI trustpoint for the CA (multiple CAs may be required, just repeat with a new TrustPoint name)

```
crypto pki trustpoint GoDaddy-CA
 enrollment terminal
 revocation-check crl
!
crypto pki trustpoint GoDaddy-CA-2
 enrollment terminal
 revocation-check crl
```

- CUBE must have a public trusted certificated signed by one of the CAs listed here
- https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc
- We are using GoDaddy in our example which provides two certificates.

Authenticate the CA certs as shown below

- With GoDaddy you get gd_bundle-g2-g1.pem with the following format:

-----BEGIN CERTIFICATE-----
… ! This is the Intermediate
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE----
… ! Paste this in GoDaddy-CA-2
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
… ! Paste this in GoDaddy-CA
-----END CERTIFICATE-----

```
! Install host CUBE cert. Paste in the top
! level intermediate cert only that can
! authenticate the host cert
crypto pki authenticate sbc2.cube-tme.com
-----BEGIN CERTIFICATE-----
… ! This is the Intermediate
-----END CERTIFICATE-----

! Install Root CA cert, not the Intermediate
crypto pki authenticate GoDaddy-CA-2
-----BEGIN CERTIFICATE----
… ! Paste this in GoDaddy-CA-2
-----END CERTIFICATE-----

! Install Root CA cert, not the Intermediate
crypto pki authenticate GoDaddy-CA
-----BEGIN CERTIFICATE-----
… ! Paste this in GoDaddy-CA
-----END CERTIFICATE-----
```

Import the signed CA (GoDaddy) host certificate

- GoDaddy provides the host certificate in pem format (e.g. 97de0728cd9183f1.pem). This is a text file with the following format. Copy the text to install as follows:

-----BEGIN CERTIFICATE-----
… ! This is the host cert
-----END CERTIFICATE-----

```
! Import the host certificate as shown below
crypto pki import sbc2.cube-tme.com certificate

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
… ! This is the host cert
-----END CERTIFICATE-----
```

- **sbc2.cube-tme.com – Trustpoint label to associate certificate or pkcs-12 file**

Exporting RSA key and certificate from CUBE 1 for CUBE-HA

```
crypto pki export sbc2.cube-tme.com pkcs12
ftp://<username>:<password>@x.x.x.x password xxxx

Address or name of remote host [x.x.x.x]?
Destination filename [sbc2.cube-tme.com]?
Writing sbc2.cube-tme.com Writing pkcs12 file to
ftp://<username>@x.x.x.x/sbc2.cube-tme.com
!
CRYPTO_PKI: Exported PKCS12 file successfully
```

Importing RSA key and certificate in CUBE 2 for CUBE-HA

```
crypto pki import sbc2.cube-tme.com pkcs12
ftp://<username>:<password>@x.x.x.x/ sbc2.cube-tme.com password
xxxx
% Importing pkcs12...

Address or name of remote host [x.x.x.x]?
Source filename [sbc2.cube-tme.com]?
Reading file from ftp://<username>@x.x.x.x/sbc2.cube-tme.com!
[OK - 4931/4096 bytes]

CRYPTO_PKI: Imported PKCS12 file successfully
```

Step by Step CUBE config:

Common Global Configuration

Step 2:

Trunk Enablement

Specify the default trustpoint and TLS version under SIP-UA

```
sip-ua
 no remote-party-id
 retry invite 2
 transport tcp tls v1.2
 crypto signaling default trustpoint sbc2.cube-tme.com
 handle-replaces
```

- `transport tcp tls v1.2` – Default TLS version to be 1.2
- `handle-replaces` – Handles INVITEs with replaces. Required for Phone System

SIP Header Pass-through and Codec Lists

```
voice class sip-hdr-passthrulist 290
 passthru-hdr Referred-By
!
voice class codec 1
 codec preference 1 g711ulaw
```

- Pass-through Referred-By header to be used in the REFER INVITE send to Phone System
- Only add codecs supported by both legs to VCC. Only codec @ preference 1 will be used for transferred calls.

Configure Global CUBE settings (`voice service voip`)

```
voice service voip
 ip address trusted list
  ipv4 52.112.0.0 255.252.0.0  ! Microsoft cloud services
  ipv4 52.120.0.0 255.252.0.0  ! Microsoft cloud services
 rtcp keepalive
 rtp-ssrc multiplex
 mode border-element
 allow-connections sip to sip
 no supplementary-service sip refer
 supplementary-service media-renegotiate
 sip
  session refresh
  header-passing
  error-passthru
  no conn-reuse
  pass-thru headers 290
  sip-profiles inbound
```

- Full Azure cloud range. See https://aka.ms/dr-PlanFQDNPorts. Add ISTP addresses here too
- No 'license capacity' from 17.2.1r
- `rtcp keepalive` - Enables CUBE to send RTCP keepalive packets for the session keepalive

SIP Profile 200 – Manipulation of outbound messages to Phone System

```
voice class sip-profiles 200
 rule 10 request ANY sip-header Contact modify "@198.135.2.118:" "@sbc2.cube-tme.com:"
 rule 20 response ANY sip-header Contact modify "@198.135.2.118:" "@sbc2.cube-tme.com:"
 rule 30 request ANY sip-header SIP-Req-URI modify "sip:(.*):5061 (.*)" "sip:\1:5061;user=phone \2"
 rule 40 request ANY sip-header User-Agent modify "(IOS.*)" "\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 50 response ANY sip-header Server modify "(IOS.*)" "\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 60 request ANY sdp-header Audio-Attribute modify "a=sendonly" "a=inactive"
 rule 70 response 200 sdp-header Audio-Connection-Info modify "0.0.0.0" "198.135.2.118"
 rule 80 request ANY sdp-header Audio-Attribute modify "(a=crypto:.*inline:[A-Za-z0-9+/=]+)" "\1|2^31"
 rule 90 response ANY sdp-header Audio-Attribute modify "(a=crypto:.*inline:[A-Za-z0-9+/=]+)" "\1|2^31"
 rule 100 request ANY sdp-header Audio-Attribute modify "a=candidate.*" "a=label:main-audio"
 rule 110 response ANY sdp-header Audio-Attribute modify "a=candidate.*" "a=label:main-audio“
 rule 120 response 486 sip-header Reason modify "cause=34;" "cause=17;"
```

Above SIP Profile required for:

- Replace CUBE IP address with Fully qualified domain names (FQDN) in both the ‘From’ and ‘Contact’ headers of INVITE and OPTIONS messages. It is essential that the FQDN in the contact header matches the domain name configured for the Phone System tenant.
- Microsoft Phone System Requires “user=phone” in all requests.
- Add the “X-MS-SBC” header containing SBC version details in all request and response. Ensure that the platform model is correct in each case. See next slide.
- Call on hold attribute to be inactive instead of send only.
- To set crypto life-time as 2^31 in all SDP sent from CUBE.
- Remove ICE candidate headers ONLY when Media Bypass is disabled in Phone System.
- For a CUBE deployed behind NAT, refer to the rule suggestions in the notes section of this slide.

X-MS-SBC Header Options

- To aid with support, Microsoft require the specific SBC model to be included in SIP messages. Select the correct string from the following options:

Platform	Profile string
ISR1100 (any)	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR1100**/\1"
ISR4321	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4321**/\1"
ISR4331	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4331**/\1"
ISR4351	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4351**/\1"
ISR4431	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4431**/\1"
ISR4451-X	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4451**/\1"
ISR4461	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ISR4461**/\1"
CSR1000V	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**CSR1000**/\1"
Catalyst 8300	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**CAT8300**/\1"
ASR1001-X	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ASR1001X**/\1"
ASR1002-X	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ASR1002X**/\1"
ASR1004	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ASR1004**/\1"
ASR1006/RP2	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ASR1000RP2**/\1"
ASR1006/RP3	"\1\x0D\x0AX-MS-SBC: Cisco UBE/**ASR1000RP3**/\1"

SIP Profile 290 – Message Manipulations for Inbound Messages from Microsoft Phone System

```
voice class sip-profiles 290
 rule 10 request REFER sip-header From copy "@(.*com)" u04
 rule 15 request REFER sip-header From copy "sip:(sip.*com)" u04
 rule 20 request REFER sip-header Refer-To modify "sip:\+(.*)@.*:5061" "sip:+AAA\1@\u04:5061"
 rule 30 request REFER sip-header Refer-To modify "<sip:sip.*:5061" "<sip:+AAA@\u04:5061"
 rule 40 response ANY sip-header Server modify "(IOS.*)" "\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
 rule 50 request ANY sdp-header Audio-Attribute modify "a=ice-.*" "a=label:main-audio"
 rule 60 request ANY sdp-header Attribute modify "a=ice-.*" "a=label:main-audio"
```

Above SIP Profile required:

- Handle REFER and ensure that the subsequent INVITE is sent to the correct Phone System proxy.
- Add a routing prefix to the user part of REFER To header to direct the subsequent INVITE to Microsoft Phone System
- Add the “X-MS-SBC” header containing SBC version details in all request and response. Ensure that the platform model is correct in each case. Check previous slide
- With Direct Routing configured for Media bypass OFF, Teams does not require “Ice-Candidates” in SDP request and response. (ONLY required for Media Bypass disabled)

SIP Profile 280 – Message Manipulations for Outbound REFER INVITE to Microsoft Phone System

```
voice class sip-profiles 280
rule 10 request ANY sip-header User-Agent modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
rule 20 response ANY sip-header Server modify "(IOS.*)"
"\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
rule 30 request INVITE sip-header SIP-Req-URI copy "@(.*:5061)" u01
rule 40 request INVITE sip-header From copy "@(.*)>" u02
rule 71 request INVITE sip-header SIP-Req-URI modify "sip:\+AAA@" "sip:"
rule 80 request INVITE sip-header SIP-Req-URI modify "sip:\+AAA" "sip:+"
rule 90 request INVITE sip-header History-Info modify "<sip:\+AAA@" "<sip:"
rule 100 request INVITE sip-header History-Info modify "<sip:\+AAA" "<sip:+"
rule 110 request INVITE sip-header To modify "<sip:\+AAA@(.*)>" "<sip:\u01>"
rule 120 request INVITE sip-header To modify "<sip:\+AAA(.*)@.*>" "<sip:+\1@\u01>"
rule 130 request ANY sip-header Contact modify "@.*:" "@\u02:"
rule 140 response ANY sip-header Contact modify "@.*:" "@\u02:"
rule 150 request ANY sdp-header Audio-Attribute modify "a=sendonly" "a=inactive"
rule 160 response 200 sdp-header Session-Owner copy "IN IP4 (.*)" u04
rule 170 response 200 sdp-header Audio-Connection-Info modify "0.0.0.0" "\u04"
rule 180 response 486 sip-header Reason modify "cause=34;" "cause=17;"
```

With the above, REFER-TO user part modification, the dial-peer 280 will be matched and the INVITE sent to Teams after removing the user part prefix.

OPTIONS Keepalive and SRTP Crypto

```
voice class sip-profiles 299
 rule 10 request OPTIONS sip-header From modify "<sip:198.135.2.118" "<sip:sbc2.cube-tme.com"
 rule 20 request OPTIONS sip-header Contact modify "<sip:198.135.2.118" "<sip:sbc2.cube-tme.com"
 rule 30 request OPTIONS sip-header User-Agent modify "(IOS.*)" "\1\x0D\x0AX-MS-SBC: Cisco UBE/ISR4321/\1"
!
voice class sip-options-keepalive 200
 sip-profiles 299
 transport tcp tls
!
voice class srtp-crypto 1
 crypto 1 AES_CM_128_HMAC_SHA1_80
```

- Above SIP Profile required for:
  - Replace CUBE IP address with Fully qualified domain names (FQDN) in both the ‘From’ and ‘Contact’ headers of OPTIONS messages. It is essential that the FQDN in the contact header matches the domain name configured for the Phone System tenant.
  - Add the “X-MS-SBC” header containing SBC version details in all request and response. Ensure that the platform model is correct in each case.
  - For a CUBE deployed behind NAT, refer to the rule suggestions in the notes section of this slide.

- **`crypto 1 AES_CM_128_HMAC_SHA1_80`** – Used to set the crypto cipher for the Microsoft Phone System trunk.

STUN ICE-Lite (For Media Bypass enabled only)

```
voice class stun-usage 1
 stun usage ice lite
```

- Used to enable STUN with ICE-Lite, <u>only for Media bypass enabled </u>in Microsoft Phone System trunk
- Will be applied to Microsoft Phone System facing dial-peers

Tenant 200 – Microsoft Phone System Tenant on CUBE

```
voice class tenant 200
  srtp-crypto 1
  localhost dns:sbc2.cube-tme.com
  session transport tcp tls
  no referto-passing
  bind media source-interface GigabitEthernet0/0/0
  bind control source-interface GigabitEthernet0/0/0
  pass-thru headers 290
  no pass-thru content custom-sdp
  sip-profiles 200
  sip-profiles 290 inbound
  early-offer forced
  block 183 sdp present
```

- For inbound calls towards Microsoft Phone System to work with ring back, 183 messages with SDP are blocked in CUBE.

Step by Step CUBE config:

Step 3:

Call Routing (+E.164 based)

Outbound Dial-peer to Phone System using TLS with sRTP

- To ensure the correct failover order, the following prioritized dial peers are used.
  1. Dial-peer voice 200 voip (Preference 1 – Highest preference)
  2. Dial-peer voice 201 voip (Preference 2)
  3. Dial-peer voice 202 voip (Preference 3 – Lowest preference)

- To simply configuration, a common E164 pattern map defining all numbers and prefixes used by Phone System is used for all 3 dial peers.

- The configuration for all three dial peers is the same, with the exception of preference and Phone System proxy FQDN.

- This dial-peer structure ensures Microsoft's requirement of sending OPTIONS to all three proxies simultaneously is met while the highest proxy is tried for calls first

- https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sip-signaling-fqdns

Outbound Dial-peer 200 – Towards Phone System Proxy 1

```
voice class e164-pattern-map 200
  e164 +14086847633
 !
dial-peer voice 200 voip
 description towards Phone System Proxy 1
 preference 1
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:sip.pstnhub.microsoft.com
 destination e164-pattern-map 200
 voice-class codec 1
 !! – 'voice class stun-usage 1' For Media Bypass enabled only – !!
 voice-class stun-usage 1
 voice-class sip tenant 200
 voice-class sip options-keepalive profile 200
 dtmf-relay rtp-nte
 srtp
 fax protocol none
 no vad
```

Outbound Dial-peer 201 – Towards Phone System Proxy 2

```
dial-peer voice 201 voip
 description towards Phone System Proxy 2
 preference 2
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:sip2.pstnhub.microsoft.com
 destination e164-pattern-map 200
 voice-class codec 1
 !! - 'voice class stun-usage 1' For Media Bypass enabled only - !!
 voice-class stun-usage 1
 voice-class sip tenant 200
 voice-class sip options-keepalive profile 200
 dtmf-relay rtp-nte
 srtp
 fax protocol none
 no vad
```

Outbound Dial-peer 202 – Towards Phone System Proxy 3

```
dial-peer voice 202 voip
 description towards Phone System Proxy 3
 preference 3
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:sip3.pstnhub.microsoft.com
 destination e164-pattern-map 200
 voice-class codec 1
 !! - 'voice class stun-usage 1' For Media Bypass enabled only - !!
 voice-class stun-usage 1
 voice-class sip tenant 200
 voice-class sip options-keepalive profile 200
 dtmf-relay rtp-nte
 srtp
 fax protocol none
 no vad
```

Inbound Dial-peer 290 – From Phone System using TLS with sRTP

```
voice class uri 290 sip
 host sbc2.cube-tme.com
!
dial-peer voice 290 voip
 description inbound from Microsoft Phone System
 translation-profile incoming 200
 rtp payload-type comfort-noise 13
 session protocol sipv2
 incoming uri to 290
 voice-class codec 1
 !! - 'voice class stun-usage 1' For Media Bypass enabled only - !!
 voice-class stun-usage 1
 voice-class sip tenant 200
 dtmf-relay rtp-nte
 srtp
 no vad
```

- The inbound dial-peer from Phone System is selected using the CUBE's FQDN as presented in the incoming TO: header. (dial-peer 290)
- NOTE : Inbound calls from the ITSP or UCM should use a different inbound dial-peer match criteria (e.g. VIA headers) and not CUBE's FQDN as shown above to ensure inbound dial-peer matching from the Microsoft Phone system does not break.

Outbound Dial-peer 280 – To Phone System for REFER Handling

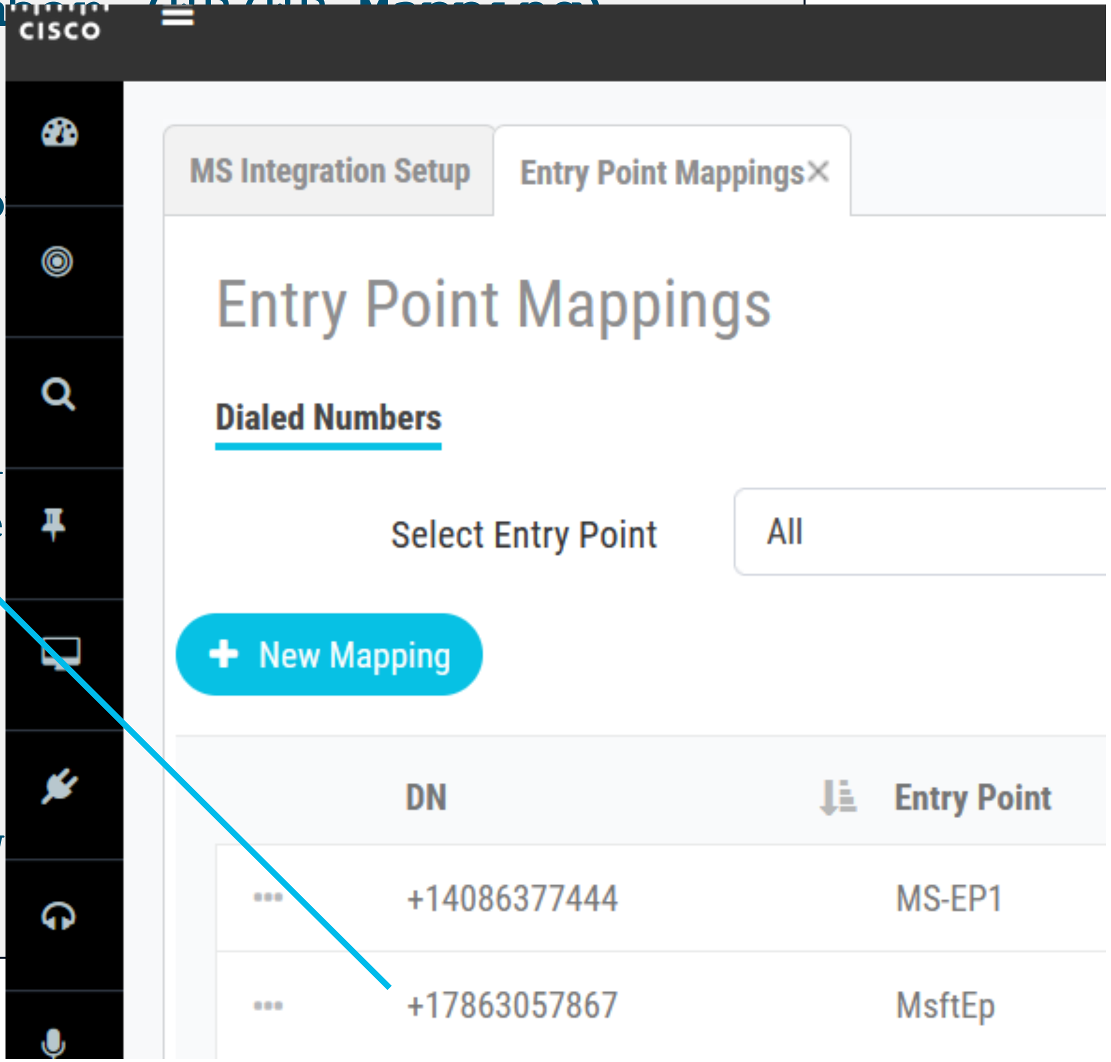
```
dial-peer voice 280 voip
 description Phone System REFER routing
 destination-pattern +AAAT
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target sip-uri
 voice-class codec 1
 voice-class sip profiles 280
 !! - 'voice class stun-usage 1' For Media Bypass enabled only - !!
 voice-class stun-usage 1
 voice-class sip tenant 200
 voice-class sip requri-passing
 dtmf-relay rtp-nte
 srtp
 no vad
```

- To correctly handle call transfers, INVITEs following a REFER from Phone System, must be directed back to Phone System. Inbound REFER messages are processed by dial peer 290 and the associated SIP profile adds a routing prefix (AAA) to the refer-to header. The subsequent INVITE is therefore, routed to Phone System through the above dial peer after the routing prefix is removed.

CUBE Config for WxCC

Inbound and Outbound ITSP facing Dial-peer for the IVR Phone Number

```
voice class uri 410 sip
 pattern +17863057867 ! <- WxCC IVR Num
!
dial-peer voice 401 voip
 description *** Incoming Dial Peer fro
 session protocol sipv2
 incoming uri request 410
 codec g711ulaw
 voice-class sip bind control source-in
 voice-class sip bind media source-inte
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 402 voip
 description *** Outbound Dial Peer tow
 . . .
```



Create a URI and a Server-group of WxCC VPOP IP Addresses

```
voice class uri ProdUSURI sip
 host ipv4:208.92.126.68
 host ipv4:208.92.126.69
 host ipv4:208.92.124.68
 host ipv4:208.92.124.69
!
voice class server-group 101
 ipv4 208.92.126.68
 ipv4 208.92.126.69
 ipv4 208.92.124.68
 ipv4 208.92.124.69
 description - ProdUS VPOP
```

Outbound VPOP facing Dial-peer for the IVR Phone Number

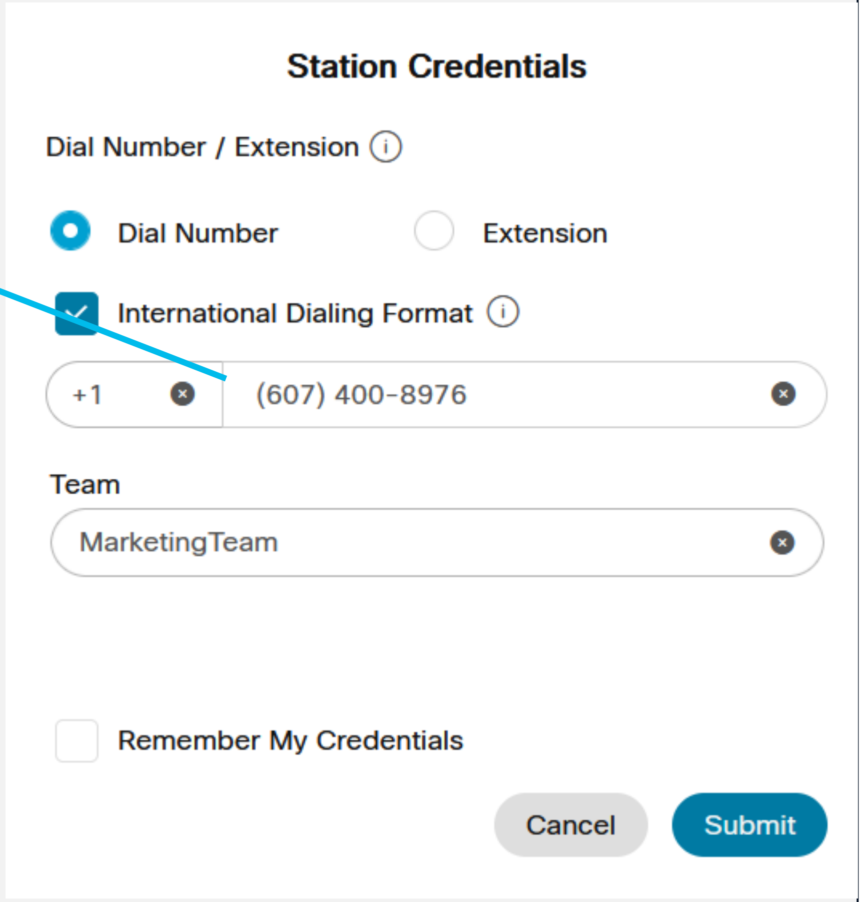
```
voice class e164-pattern-map 910
 description Towards ProdUS
  e164 +17863057867
!
dial-peer voice 901 voip
 description Outbound Towards Production US VPOP
 session protocol sipv2
 session server-group 101
 destination e164-pattern-map 910
 voice-class sip options-keepalive profile 167
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
!
voice class sip-options-keepalive 167
 transport udp
```

Inbound VPOP facing Dial-peer

```
voice class uri ProdUSURI sip
 host ipv4:208.92.126.68
 host ipv4:208.92.126.69
 host ipv4:208.92.124.68
 host ipv4:208.92.124.69
!
!
dial-peer voice 900 voip
 description Inbound from Production US VPOP
 session protocol sipv2
 incoming uri via ProdUSURI
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
```

Outbound MS Phone System facing Dial-peer for Agent Dial Numbers / Extensions

```
voice class e164-pattern-map 200
  e164 +14086847633
  e164 +16074008976 !<- Agent Dial Number / Extensions
 !
!
dial-peer voice 200 voip
 description towards Phone System Proxy 1
 preference 1
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:sip.pstnhub.microsoft.com
 destination e164-pattern-map 200
 voice-class codec 1
 voice-class sip tenant 200
 voice-class sip options-keepalive profile 200
 dtmf-relay rtp-nte
 srtp
 no vad
```



CISCO

The bridge to possible