

The background features a vibrant, abstract design with a color gradient from dark blue on the left to bright yellow and white on the right. The design consists of overlapping, wavy horizontal bands and a series of radiating lines that create a sense of motion and energy, resembling a stylized sunburst or a dynamic wave pattern.

CISCO *Live!*

Let's go



The bridge to possible

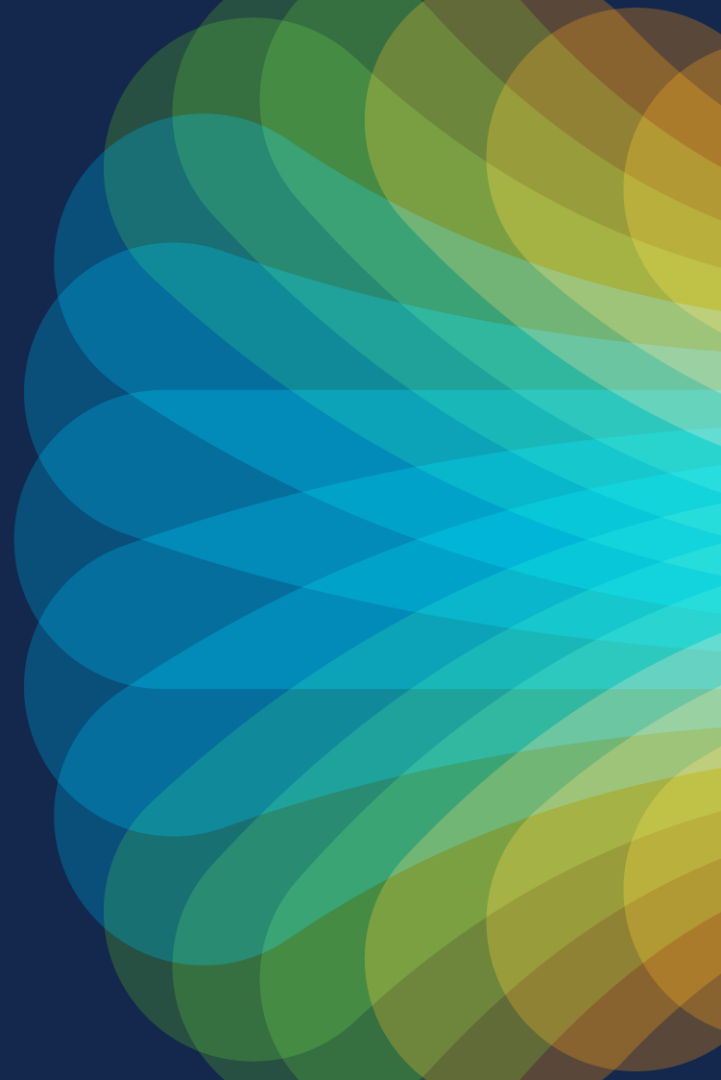
# CUBE v14 Updates

Hussain Ali, Technical Marketing Engineer  
[linkedin.com/in/hussaincube](https://www.linkedin.com/in/hussaincube)

# Agenda

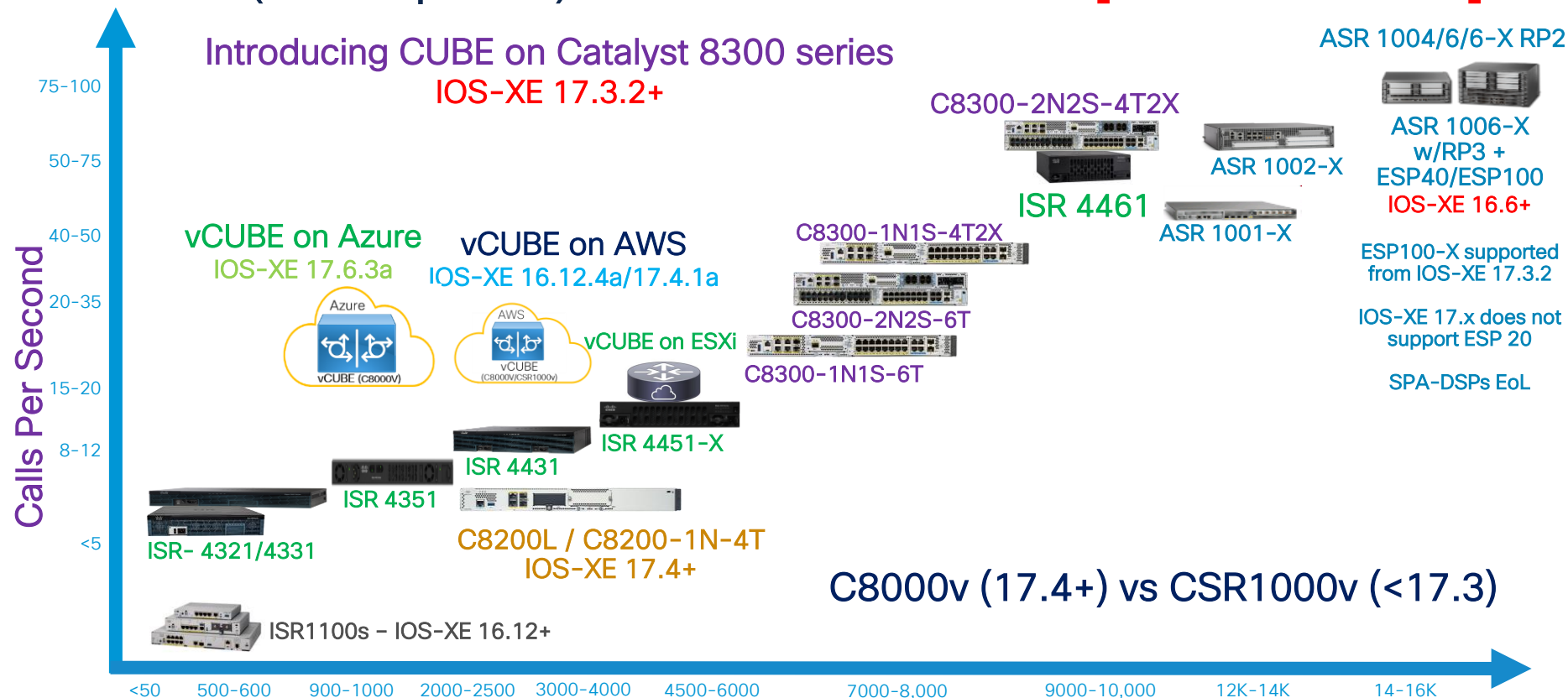
- **New Platforms for CUBE/vCUBE and Sizing Updates**
- Introducing Multiple SIP Listen ports
- Managing Gateways from the Cloud
- NAT traversal using RTP keepalives
- CUBE High Availability Updates
- DNS SRV Load Balancing
- Enabling 3<sup>rd</sup> party Cloud Calling with CUBE
- Direct Routing for Microsoft Phone System
- Resources

# New Platforms for CUBE/vCUBE and Sizing Updates



# New 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 |
|--------------|---------------------------------------------------------------|------------|-------------------------------------------------|
| 14.1         | 17.3.2*                                                       | Oct 2020   | 17.3.8a                                         |
| 14.2         | 17.4.1a                                                       | Nov 2020   | 17.4.2                                          |
| 14.3         | 17.5.1                                                        | March 2021 | 17.5.1a                                         |
| 14.4         | 17.6.1a                                                       | July 2021  | 17.6.6a                                         |
| 14.4         | 17.7.1a                                                       | Nov 2021   | 17.7.2                                          |
| 14.5         | 17.8.1a                                                       | March 2022 |                                                 |
| 14.6         | 17.9.1a                                                       | July 2022  | 17.9.4a                                         |
| 14.6         | 17.10.1a                                                      | Nov 2022   |                                                 |
| 14.6         | 17.11.1a                                                      | March 2023 |                                                 |
| 14.7         | 17.12.1a                                                      | July 2023  | 17.12.2                                         |
| 14.8         | 17.13.1a                                                      | Nov 2023   |                                                 |
| 14.9         | 17.14.1a                                                      | March 2024 |                                                 |

Last release for  
ISR4K except  
ISR4461

# Sizing Updates

# CUBE IP Telephony (Collab) Session Capacity Summary

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

# CUBE IP Telephony (Collab) Session Capacity Summary

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

## CUBE Encrypted IPT Audio Call Capacity

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

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

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

# CUBE Encrypted IPT Audio Call Capacity

<sup>1</sup>CSR1Kv - Based on tests using Cisco UCS \* C240 host with Intel \* Xeon \* 6132  
2.60GHz processors running VMware ESXi 6.0.

Audio IP Telephony calls  
RTP(G711)-RTP(G711)

Encrypted Audio (**SHA1\_80**) calls  
**sRTP(G711)**-RTP(G711)

CPS

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

# vCUBE on AWS / Azure

# vCUBE on Amazon Web Services (AWS) / Microsoft Azure

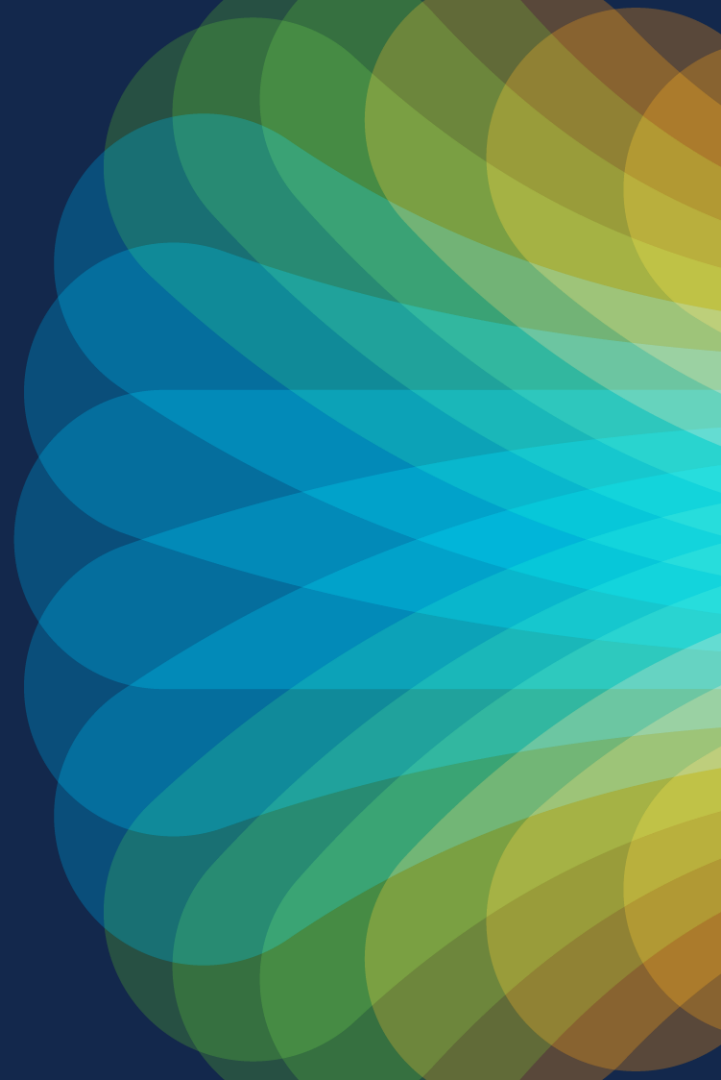


- [AWS] Platform validated and currently supported – c5.large [2vCPU, 4GB RAM, 8GB SSD] and c5n.large [2vCPU, 5.3 GB]
  - IOS-XE versions validated – CSR1000v (16.12.4a, 17.3.2), C8000V (17.4.1a) [Subsequent releases also supported]
- [Azure] Platform validated and currently tested – D2\_v2 [2 vCPUs, 7 GB memory]
  - IOS-XE versions validated – 17.3.4a [Subsequent releases also supported]
- BYOL – Instance billed only for hosting by AWS/Azure and licensing managed through Cisco Smart Licensing [DNA Network Essentials or above for C8000V]
- vCUBE in AWS/Azure session counts same as vCUBE – 2 vCPU

# AWS and Azure deployment considerations

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

# Introducing multiple SIP listen ports



# Introducing voice class TLS-profile



## Prior to IOS-XE 17.3.1

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

## Starting IOS-XE 17.3.1

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

```
    tls-profile      Associate a tls-profile
```

```
    trustpoint       Associate a trustpoint
```

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

# SIP Listening Port on CUBE before IOS-XE 17.8.1a

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

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

# Multi Tenant – SIP listen ports

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

# SIP listen ports

## Considerations

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

# Multi Tenant – SIP listen ports

## Design Considerations

- The non-secure port range is 5000 – 5500. This is to avoid overlap between UDP/RTP port range
- TLS port range is 1 to 65535
- For listen-port based multi tenant support on CUBE, you **MUST** configure
  - TLS profile under voice class tenant configuration mode
  - Listen port under voice class tenant configuration mode
- Functionality:
  - The inbound dial-peers are filtered based on the tenant tag associated to the dial-peer
  - Inbound call to Listen port → tenant → Inbound dial-peers

# Multi Tenant – SIP listen ports – Configuration

- Configure voice class tls-profile

```
CUBE(config)#voice class tls-profile <tag>
```

```
CUBE(config-class)#cn-san validate ?
```

|                      |                                                                 |
|----------------------|-----------------------------------------------------------------|
| <b>bidirectional</b> | Enable CN/SAN validation for both client and server certificate |
| <b>client</b>        | Enable CN/SAN validation for client certificate                 |
| <b>server</b>        | Enable CN/SAN validation for server certificate                 |

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

```
CUBE(config)#voice class tenant <tag>
```

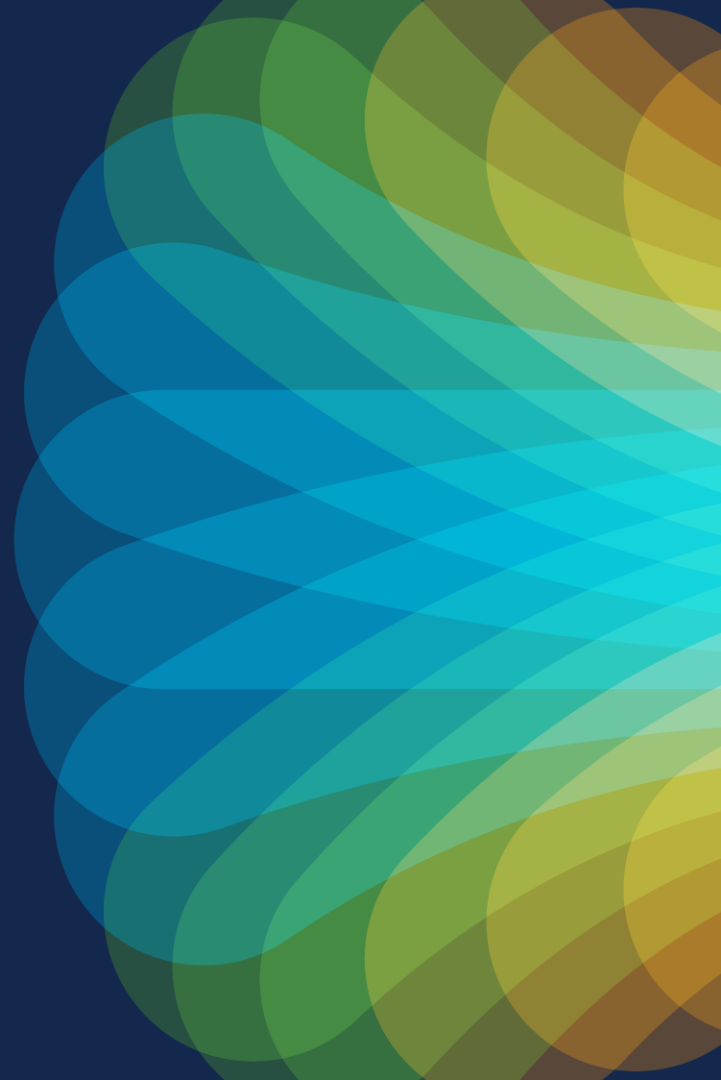
```
CUBE(config-class)#listen-port ?
```

|                   |                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------|
| <b>non-secure</b> | Change UDP/TCP SIP listen port (have bind configured under this tenant for the config to take effect) |
| <b>secure</b>     | Change TLS SIP listen port (have bind configured under this tenant for the config to take effect)     |

```
CUBE(config-class)#tls-profile <tag>
```

```
<1-10000> Specify the tls-profile tag number
```

# Managing Gateways from the Webex Control Hub



# Introducing Gateway Connectors

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

# Connector Considerations

- ISR 1100 series are not supported
- CUBE High Availability (HA) mode is not supported
- Controller or SD-WAN mode is not supported (only IOS-XE Autonomous mode is supported)
- Currently two services are supported:
  - Registration-based Local Gateway Configuration Validation
  - Survivability Gateway Configuration template (BRKCOL-2993)
- IOS-XE version required:
  - Local Gateways—Cisco IOS XE 17.3.4a or later
  - Survivability Gateways—Cisco IOS XE 17.9.3a or later

# Connector Installation Prerequisites

- The platform must have the following configured:

- DNS Server `ip name-server <IP Address>`

- HTTP Proxy

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

```
ip http client username <username>
```

```
ip http client password <password>
```

- Default AAA lists to authenticate and authorize NETCONF access

```
aaa new-model
```

```
aaa authentication login default radius local
```

```
aaa authorization exec default radius local if-authenticated
```

```
username test privilege 15 secret <password>
```

- Import the IOS-XE public CA bundle

```
crypto pki trustpool import url
```

```
http://www.cisco.com/security/pki/trs/ios.p7b
```

# Add a New Gateway Instance in Control Hub

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

webex Control Hub

Nav Item

MONITORING

Analytics

Troubleshooting

MANAGEMENT

Users

Locations

Devices

Apps

Account

Organization settings

SERVICES

Messaging

Meetings

Calling

Contact Center

Frontline

Calling

NumbersCall RoutingManaged GatewaysFeaturesOrdersDedicated InstanceService Settings



Managed Gateways

By connecting your on-premises Cisco IOS XE platforms to Control Hub, you can benefit from enhanced management, service visibility and new gateway services. Make sure that you have direct access to both your device and Control Hub before selecting Add Gateway below. [Learn More.](#)

Add Gateway

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

## Add a Managed Gateway

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

tcsh https://binaries.webex.com/ManagedGatewayScriptProdStable/gateway\_onboarding.tcl 

☐ I have installed the management connector on the gateway.

# Run the Management Connector deployment Script

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

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

# Select the External Interface to reach Webex Cloud

## Webex Gateway Connector Installation

Choose the external-interface from the below list of available interfaces:

| Number | Interface        | IP-Address   | Status |
|--------|------------------|--------------|--------|
| 1      | GigabitEthernet1 | 10.52.12.203 | up     |

Enter a number to choose the external interface: 1

# Confirm or Edit DNS and Proxy settings

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

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

```
These proxy settings were detected in the gateway configuration:
```

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

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

# Specify the Connector IP Address and Credentials

```
Enter Connector IP address: 10.52.12.216
```

```
Enter Gateway username: hussain
```

```
Enter Gateway password: *****
```

```
Confirm Gateway password: *****
```

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

# Connector Successfully Installed

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

*** Cloud connector is installed successfully. ***
-----

*** Interface Status ***
-----

Interface                IP-Address      Status
-----
GigabitEthernet1         10.52.12.203    up
VirtualPortGroup0        10.52.12.203    up
Connector                 10.52.12.216    up
-----

*** App Status ***
-----

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

# Webex Managed Gateway Connector Options

## Webex Managed Gateway Connector

### Options

- s : Display Status Page
- v : View and Modify Cloud Connector Settings
- e : Enable Guestshell
- d : Disable Guestshell
- l : Collect Logs
- r : Clear Logs
- u : Uninstall Connector
- q : Quit

Select an option from the menu: 

# vCUBE on AWS/Azure Connector Considerations

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

# vCUBE on Azure Connector Considerations

**! provision dummy lo0 interface first**

```
interface loopback0
ip address 192.168.35.1 255.255.255.0
```

**! run connector install script**

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

```
# tclsh
https://binaries.webex.com/ManagedGatewayScript
ProdStable/gateway_onboarding.tcl
```

**! Credentials for connector should be the same as the platform**

**! after installation remove lo0 interface and assign ip from it into vpg0:**

```
no int lo0
interface VirtualPortGroup0
ip address 192.168.35.1 255.255.255.0
ip nat inside
```

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

```
ip access-list standard GSNAT
10 permit 192.168.35.0 0.0.0.255
```

**! disable local http(s) server as we will be doing NAT for 443 port**

```
no ip http server
no ip http secure-server
```

```
ip nat inside source list GSNAT interface
GigabitEthernet2 overload
```

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

# Enroll the Gateway in the Control Hub

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

## Add a Managed Gateway

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

tclsh https://binaries.webex.com/ManagedGatewayScriptProdStable/gateway\_onboarding.tcl 

☒ I have installed the management connector on the gateway.

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

### Add a Managed Gateway

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

Enter the connector IP address

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

Enter a display name for the gateway

The name is for display purposes only.

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

Cancel

Next 

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



## Gateway Connector Management

Sign in

---

[Need help signing in?](#)

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

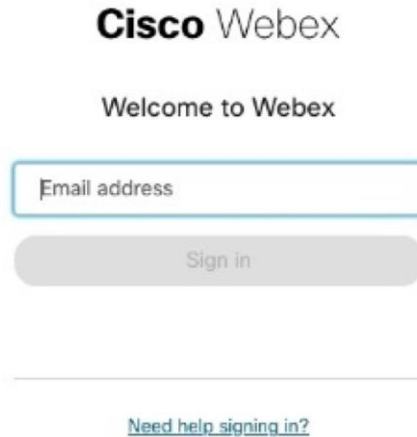
## Enroll Gateway

**To complete the enrollment process, a secure connection must be established from this connector to the Cisco Webex cloud.**

Use your Webex Calling administrator credentials to authenticate the connection on the next screen.

Enroll Now

# Sign in using a Webex Administrator account



The image shows a sign-in form for Cisco Webex. At the top, the text "Cisco Webex" is displayed in a bold, sans-serif font. Below it, the text "Welcome to Webex" is centered. The main part of the form consists of a rectangular input field with a light blue border and the placeholder text "Email address". Directly beneath this field is a rounded rectangular button with a light gray background and the text "Sign in". A thin horizontal line separates the sign-in button from a link at the bottom of the form that reads "Need help signing in?" in a smaller, blue, underlined font.

**Cisco** Webex

Welcome to Webex

Email address

Sign in

---

[Need help signing in?](#)

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

## Gateway Management Connector

### Allow Access to Gateway Management Connector

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

#### Organization

WxCSA Team Sandbox

#### FQDN or IP Address

10.52.12.216

☒ Allow Access to the Gateway Management Connector

*Only allow access to hosts you know and trust*

Continue

# Enrollment Successful

## Gateway Management Connector

### Registration Confirmed

You will now be redirected to 10.52.12.216.

**Enrollment successful.**

You can close this window and proceed to Webex Control Hub to view and associate this gateway with a service.

# Managed Gateways

## 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 | <a href="#">Location: Amsterdam Office</a>     | ...     |
| Hussain-Cat8kv |         | -                | -                     | -                                              | ...     |
| Lisbon SGW     | 17.9.3  | ● Online         | Survivability Gateway | <a href="#">Location: Lisbon Office</a>        | ...     |
| London SGW     | 17.9.3  | ● Offline        | Survivability Gateway | <a href="#">Location: London Branch Office</a> | ...     |
| Madrid SGW     | 17.9.3  | ● Online         | Survivability Gateway | <a href="#">Location: Madrid Office</a>        | ...     |
| Munich SGW     | 17.9.3  | ● Online         | Survivability Gateway | <a href="#">Location: Munich Office</a>        | ...     |
| Paris SGW      | 17.9.3  | ● Online         | Survivability Gateway | <a href="#">Location: Paris Office</a>         | ...     |
| Rome SGW       | 17.9.3  | ● Online         | Survivability Gateway | <a href="#">Location: Rome Office</a>          | ...     |
| Vienna SGW     | 17.9.3  | ● Online         | Survivability Gateway | <a href="#">Location: Vienna Office</a>        | ...     |

# 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 | <a href="#">Location: Amsterdam Office</a>     | ...     |
| Hussain-Cat8kv | 17.9.20221... | ● Online         | -                     | -                                              | ...     |
| Lisbon SGW     | 17.9.3        | ● Online         | Survivability Gateway | <a href="#">Location: Lisbon Office</a>        | ...     |
| London SGW     | 17.9.3        | ● Offline        | Survivability Gateway | <a href="#">Location: London Branch Office</a> | ...     |
| Madrid SGW     | 17.9.3        | ● Online         | Survivability Gateway | <a href="#">Location: Madrid Office</a>        | ...     |
| Munich SGW     | 17.9.3        | ● Online         | Survivability Gateway | <a href="#">Location: Munich Office</a>        | ...     |
| Paris SGW      | 17.9.3        | ● Online         | Survivability Gateway | <a href="#">Location: Paris Office</a>         | ...     |

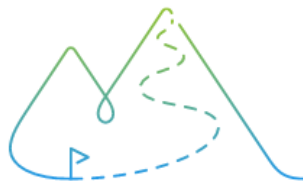
# Assign a Service to the Managed Gateway

< Managed Gateways

**Hussain-Cat8kv**

● Connector Online • Version 17.9.20221213

Actions ▾



## 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

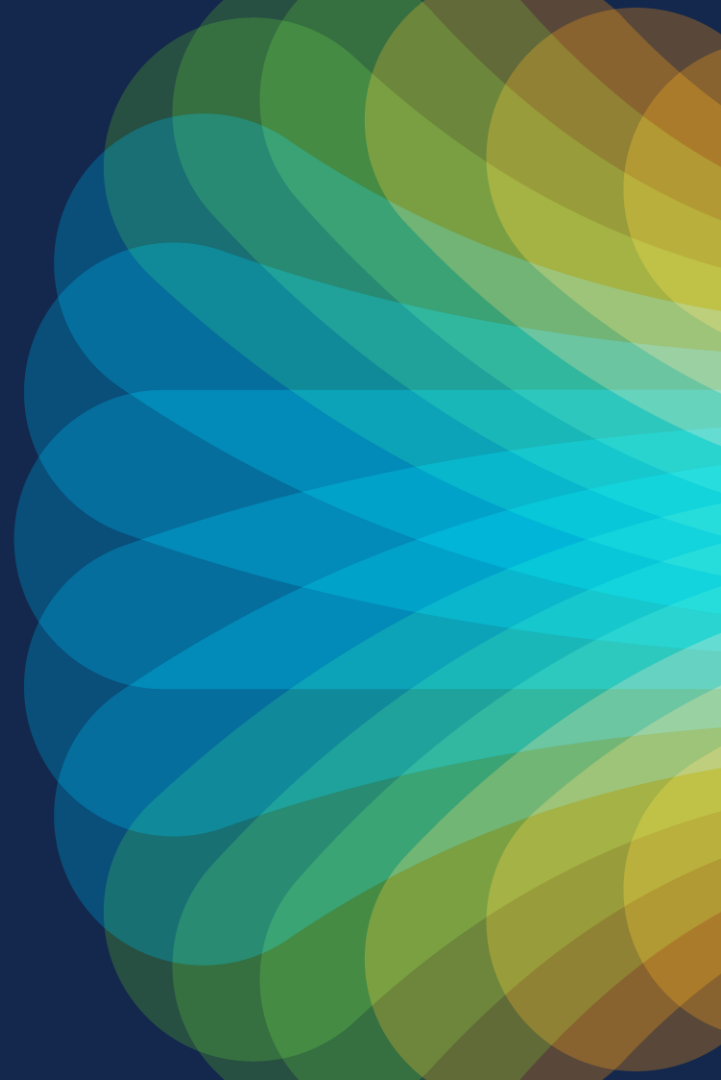
Local Gateway

Survivability Gateway

Cancel

Assign

# NAT Traversal using RTP keepalives

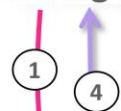


# Introducing NAT Traversal using RTP keepalives

User A



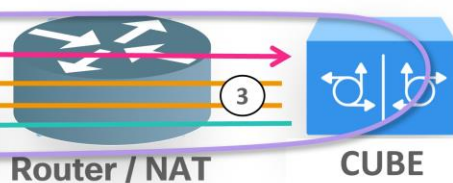
Calling-Party



- 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



External SBC



Router / NAT



CUBE



IP-PBX CUCM



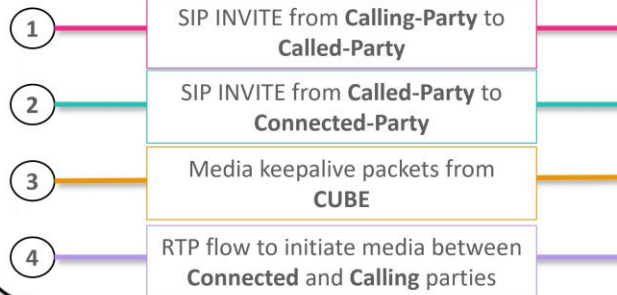
User B

Called-Party

`nat media-keepalive  
[interval]`

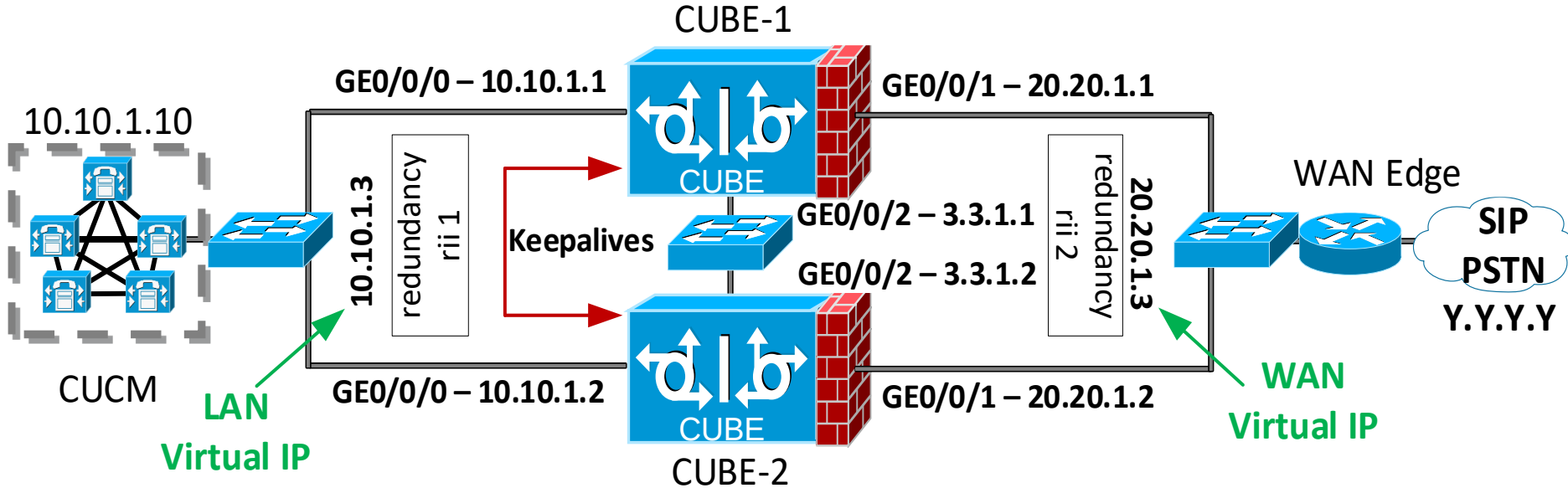


## Key



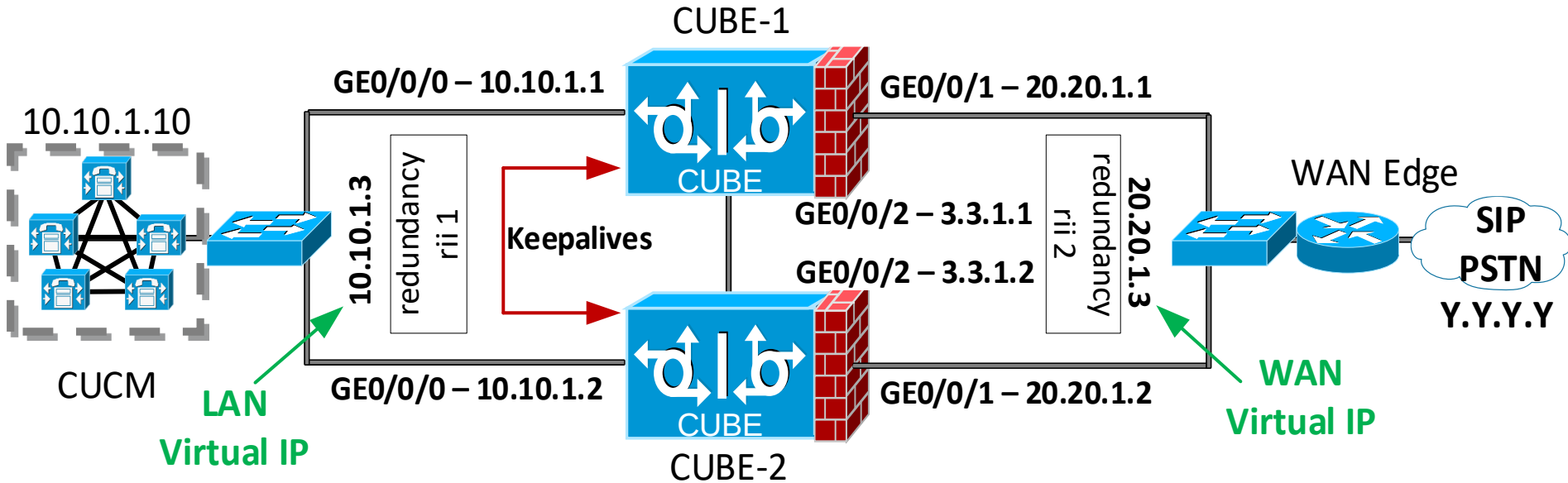
# CUBE High Availability (HA) Updates

# CUBE HA for Call Preservation



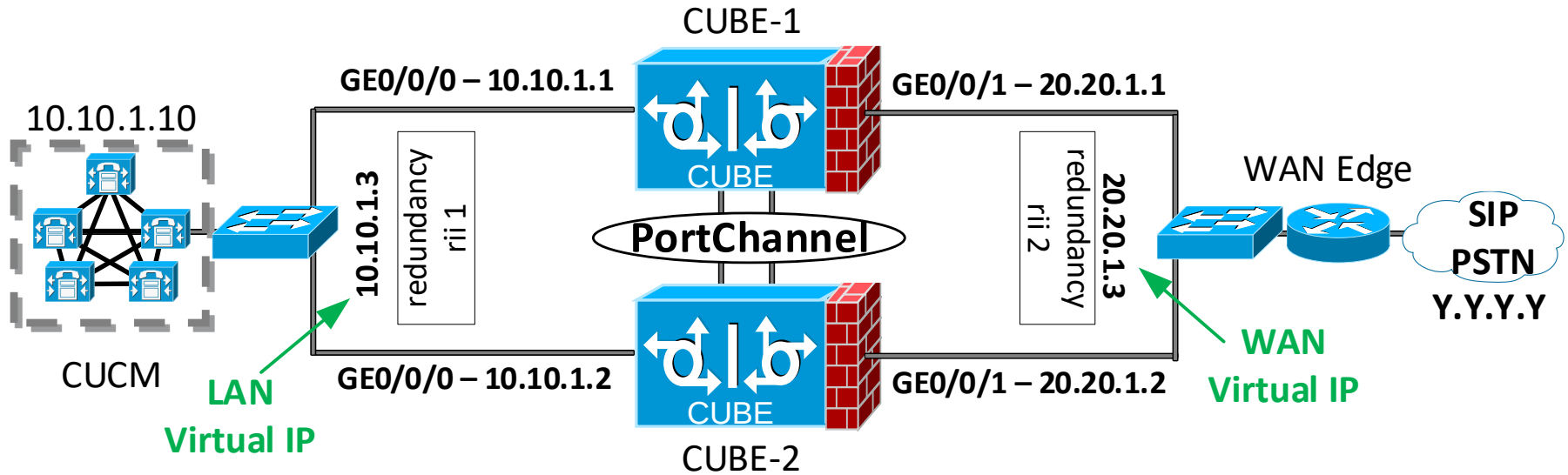
- RG Control/Data interface (G0/0/2) had to be connected via a physical switch
- It can now be connected via a back-to-back cable

# Crossover cable for Keepalive interface



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

# Port channel for keepalive interfaces



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

# CUBE HA is now supported with IPv6



- Interface configuration with IPv6

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

- Dial-peer configuration with IPv6

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

- SIP-UA configuration with IPv6

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

# DNS SRV based load balancing on Dial-peers

# Introducing DNS SRV based OPTIONS ping

# OPTIONS ping for DNS SRV hosts



- **Pre IOS-XE 17.9**

- CUBE uses the first resource obtained against an SRV lookup to send the option keepalive message. In case the response fails with the first host, CUBE does not try other hosts.

- **IOS-XE 17.9.1a or later**

- CUBE attempts OPTION keepalives with the all the hosts to determine their status and use it for routing the calls.
- This feature can be used by configuring a dial-peer target with an FQDN that resolves to a set of DNS SRV records.
- A DNS SRV lookup results in multiple targets (A records), each with its own weight, priority.
- CUBE performs DNS lookup against each record (obtained through SRV lookup) to determine the IPv4/IPv6 addresses and triggers OOD SIP Option message to each destination to monitor the status.

# Pre-requisites

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

---

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

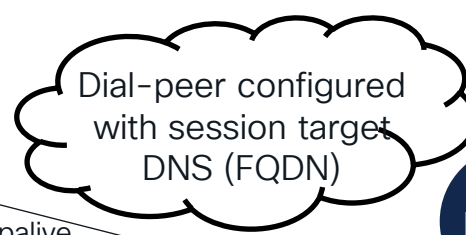
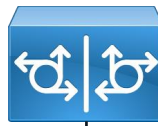
```
dial-peer voice 786 voip
  session target dns:webex.com
  session transport tcp
  voice-class sip options-keepalive profile 1
```

---

# DNS SRV Based Option Ping : Status of Hosts

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

# Feature Operation



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



Feature will not work

NO

Is SIP OPTION keepalive profile configured?

YES

DNS SRV query for webex.com

Successful DNS response with host list

A Record resolution for the hosts

IP Address resolution

DNS lookup gets resolved to 3 hosts  
example1.webex.com  
example2.webex.com  
example3.webex.com  
IP Address Resolution of all hosts

Send OPTIONS to all hosts

YES

Dial-peer state Active

Is OPTIONS successful for ALL hosts?

NO

YES

Dial-peer state Partial

Is OPTIONS successful to ANY host?

NO

Dial-peer state Busyout

OPTIONS

200 OK

example1.webex.com  
**Active**

OPTIONS

200 OK

example2.webex.com  
**Active**

OPTIONS

example3.webex.com  
**Busyout**

One node is down

# 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        |
|------------|--------|---------------------------|------------|-----------|-----------|---------------|
| <b>786</b> | -      | dns:webex.com             |            |           |           | <b>active</b> |
|            |        | <b>example3.webex.com</b> | 46         | <b>10</b> | <b>50</b> | active        |
|            |        | ipv4:10.64.86.70:5880     |            |           |           |               |
|            |        | <b>example2.webex.com</b> | 45         | <b>10</b> | <b>50</b> | active        |
|            |        | ipv4:10.65.105.59:5060    |            |           |           |               |
|            |        | <b>example1.webex.com</b> | 44         | <b>10</b> | <b>50</b> | 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             |            |     |    | <b>partial</b> |
|     |        | <b>example3.webex.com</b> | 46         | 10  | 50 | busyout        |
|     |        | ipv4:10.64.86.70:5880     |            |     |    |                |
|     |        | <b>example2.webex.com</b> | 45         | 10  | 50 | active         |
|     |        | ipv4:10.65.105.59:5060    |            |     |    |                |
|     |        | <b>example1.webex.com</b> | 44         | 10  | 50 | active         |
|     |        | ipv4:10.65.105.58:5060    |            |     |    |                |

# Dial-peer show output - Busyout

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

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

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

# OPTIONS Keepalive profile show output

```
CUBE#show voice class sip-options-keepalive 1
```

```
Voice class sip-options-keepalive: 1 AdminStat: Up
```

```
Description: keepalive-webex
```

```
Transport: tcp Sip Profiles: 0
```

```
Interval(seconds) Up: 5 Down: 15
```

```
Retry: 1
```

| Peer Tag | Server Group | OOD SessID | OOD Stat | IfIndex |
|----------|--------------|------------|----------|---------|
| -----    | -----        | -----      | -----    | -----   |

|     |  |  |      |    |
|-----|--|--|------|----|
| 786 |  |  | None | 31 |
|-----|--|--|------|----|

|                |                |
|----------------|----------------|
| OOD SessID: 46 | OOD Stat: Busy |
|----------------|----------------|

```
Target: ipv4:10.64.86.70:5880
```

```
Transport: tcp Sip Profiles: 0
```

|                |                  |
|----------------|------------------|
| OOD SessID: 47 | OOD Stat: Active |
|----------------|------------------|

```
Target: ipv4:10.65.105.59:5060
```

```
Transport: tcp Sip Profiles: 0
```

|                |                  |
|----------------|------------------|
| OOD SessID: 48 | OOD Stat: Active |
|----------------|------------------|

```
Target: ipv4:10.65.105.58:5060
```

```
Transport: tcp Sip Profiles: 0
```

# Dial-peer voice summary show outout

```
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     |      |      | <b>partial</b> |

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



BRKCOL-2312

Hussain\_Cert-based Successfully Created.

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

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

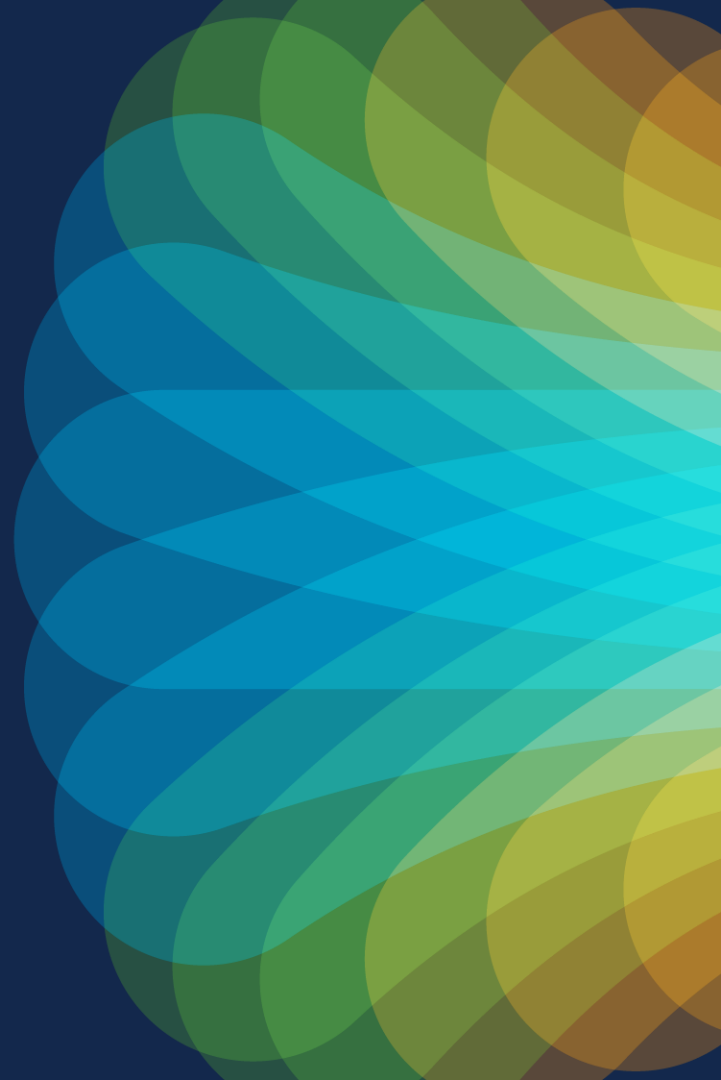
Visit [Dial Plans](#) page to use this trunk as the routing choice for a dial plan.

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

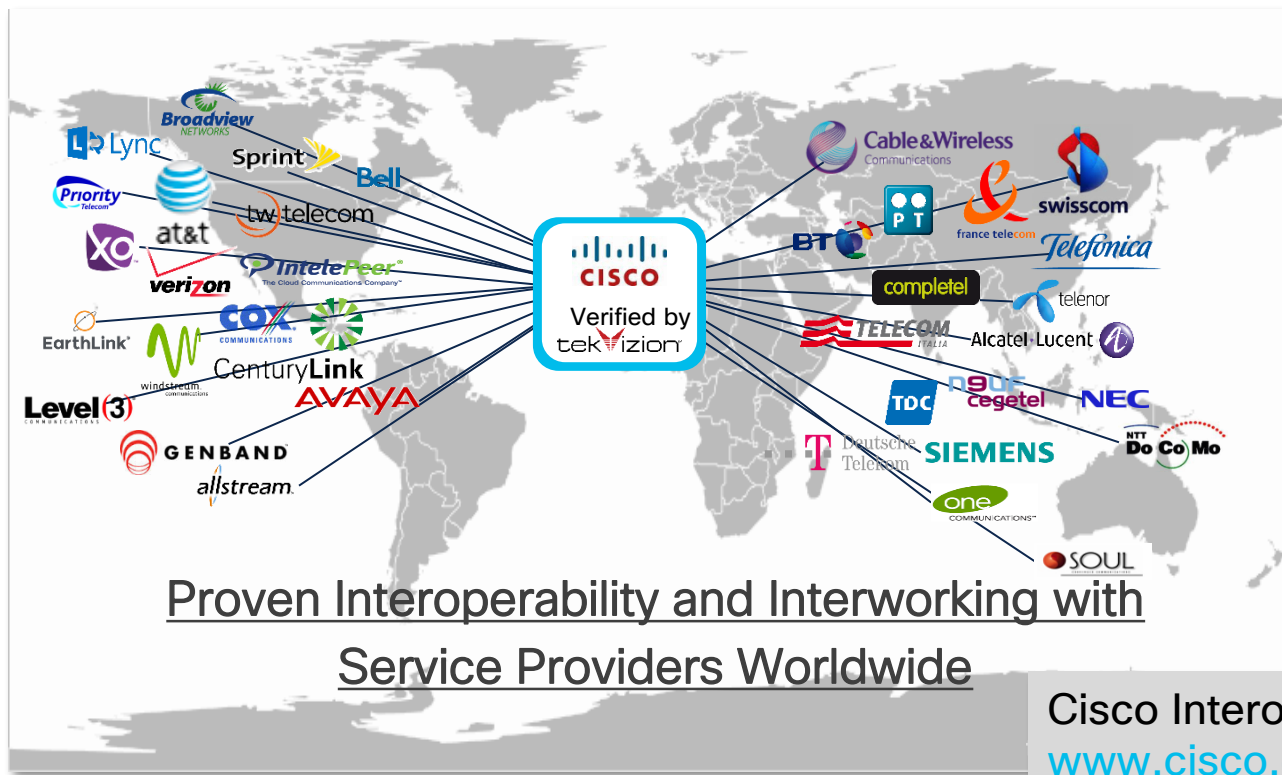
Webex Calling edge proxy address (FQDN)

peer1.us.sipconnect.bcld.webex.com:5062

# Enabling third-party Cloud Calling with CUBE



# CUBE Interoperability Portal for application notes



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

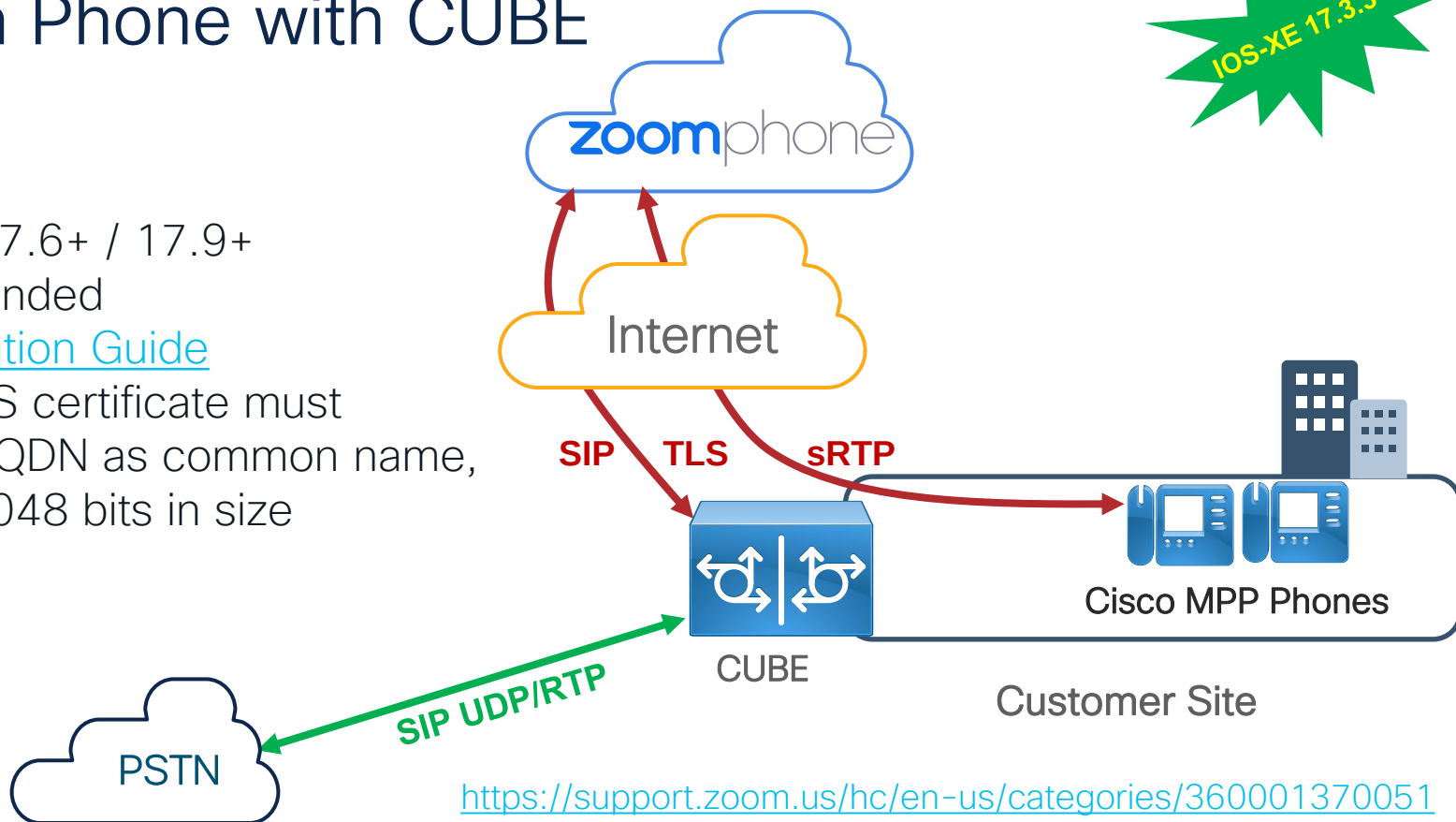
Cisco Interoperability Portal:

[www.cisco.com/go/interoperability](https://www.cisco.com/go/interoperability)

# Zoom Phone with CUBE



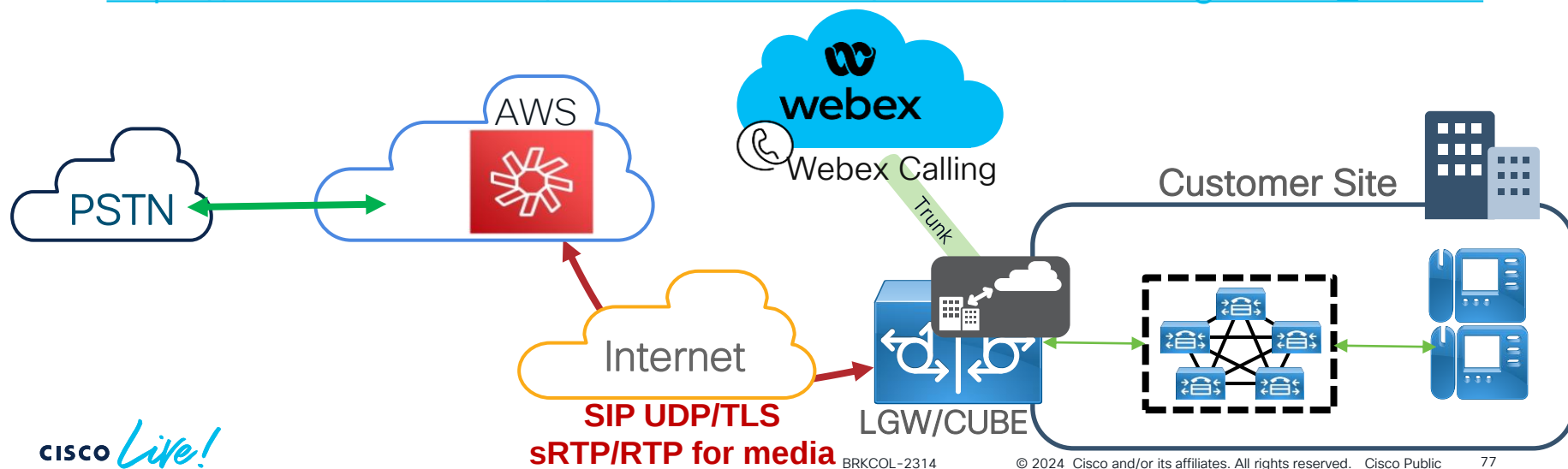
- IOS-XE 17.6+ / 17.9+ recommended
- [Configuration Guide](#)
- CUBE TLS certificate must contain FQDN as common name, and be 2048 bits in size



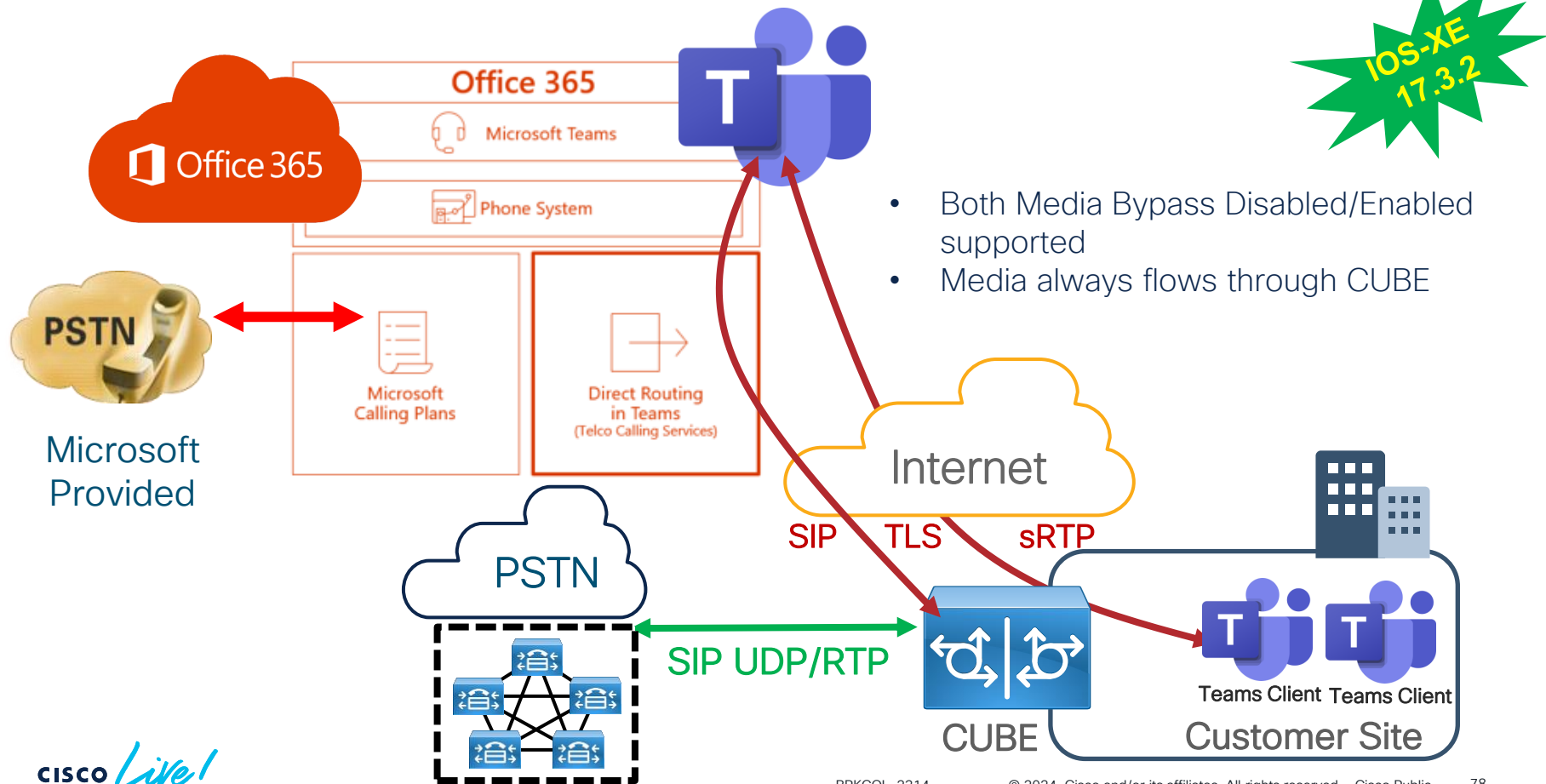
# Amazon Chime Voice Connector



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



# Microsoft Teams Direct Routing – Solution Overview



# Configuring Direct Routing for Microsoft Phone System

# Microsoft Admin Config

# Microsoft Domain Verification

Microsoft 365 admin center

Search

Home > Domains

## Domains

+ Add domain    Buy domain    Refresh

| Domain name ↑                                   | Status     |
|-------------------------------------------------|------------|
| <input type="checkbox"/> boldbetz.com (Default) | ⋮  Healthy |

Make sure your domain is verified and in Healthy state

# Configure Direct Routing

Provide the FQDN for  
your CUBE

**sbc2.cube-tme.com**

You must use the SBC's FQDN that has the host name registered in DNS. For example, if your good name for the SBC, but **sbc.contoso.onmicrosoft.com** isn't. [Learn more](#)

Add a description so you know why it was created

**SBC settings**

When you are adding this SBC, you can turn on or off the SBC and change settings

Enabled ☒ On

SIP signaling port 5061

Send SIP options ☒ On

Forward call history ☐ Off

Forward P-Asserted-Identity (PAI) header ☐ Off

Concurrent call capacity 24

Failover response codes 408, 503, 504

Failover time (seconds) 10

Port to connect to  
CUBE

Enable SIP Options to  
maintain trunk availability

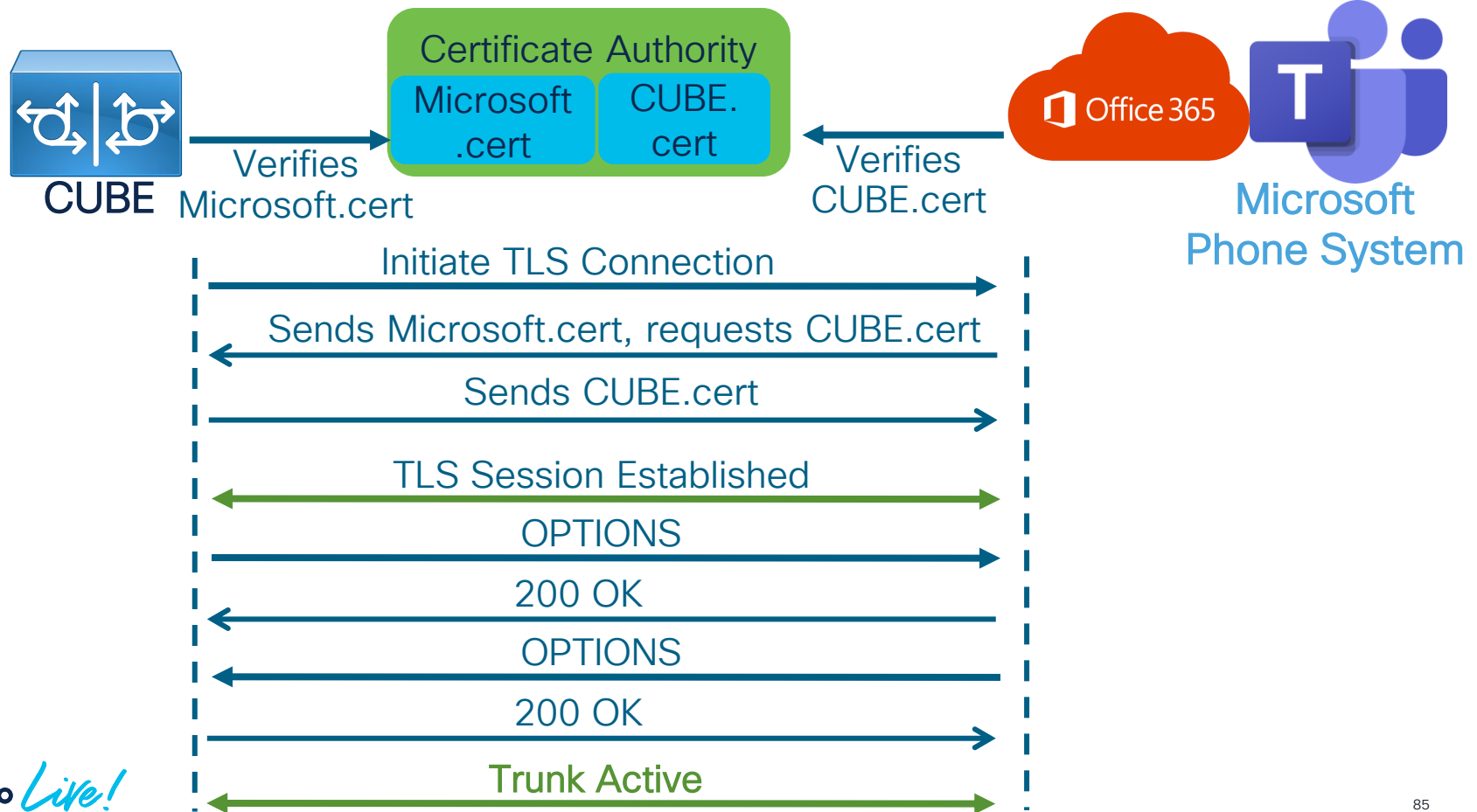
# CUBE Configuration for Direct Routing

# 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 between CUBE and Microsoft Teams



Microsoft Teams admin center

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 between CUBE and Microsoft Teams

```
graph LR
    CUBE[CUBE] -- "Verifies Microsoft.cert" --> CA[Certificate Authority]
    CA -- "Initiate TLS Connection" --> CUBE
    CUBE -- "Sends Microsoft.cert, requests CUBE.cert" --> CA
    CA -- "Sends CUBE.cert" --> CUBE
    CUBE -- "TLS Session Established" --> CA
    CUBE -- "OPTIONS" --> CA
    CA -- "200 OK" --> CUBE
    CUBE -- "OPTIONS" --> CA
    CA -- "200 OK" --> CUBE
    CUBE -- "Trunk Active" --> CA
```

BRKCOL-2314

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

86

# 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 recommended.

```
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-----
MIICpDCCAYwCAQAwPjEaMBgGA1UEAxMRc2JjMi5j
hkiG9w0BCQIWEXNlY3luY3ViZS10bWUuYz9tMIIlBjA
AQ8AMIIBCgKCAQEAjBuVXcBKtrPeAHQM1ips3Mxal
EtiQPWnFDjSXS2LTMx9FHnmdpEgYkGOzxVjdd0G+
yJT86Yre9M5uvsWEWiwYy/uaq3nz3CDFd5NpyUa3sH
2T12i3jMplMqjoDAnP2izd/zPqjBouRPAkx5LVVGATY
KbuoE0Hqaot89mkjxVYKdTHFKZGt1xtQy8QXNMzyi
vCOzcA3ecOWrjTsbd5hinLq654cyF1c2YVSTQIDAQ/
MRIwEDAQBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvc
DTCNQTOpzsCjql6f5l1z6/DGISwy2Lvm5j9SdTZ7M:
c8az2Ss6i0fWP5+jxF1ptbWy1ValsA4fxSgeSHNS2nVL
B1J5hdtqRzanCLR1lJgTKRFWqOM/NHqgTWX4LpDm
2b3kCUGYL324Ys1+9VfuouUeSKUj4lccwNaZmRimCC
JeuxjTJFdu1MZtXYMfXFCV99axLEgAuGl6Acp6LtpQfv
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

# 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-passthru list 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
- **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.

# 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"
```

- 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:svc2.cube-tme.com"
  rule 20 request OPTIONS sip-header Contact modify "<sip:198.135.2.118" "<sip:svc2.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, only for Media bypass enabled 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 simplify 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
```

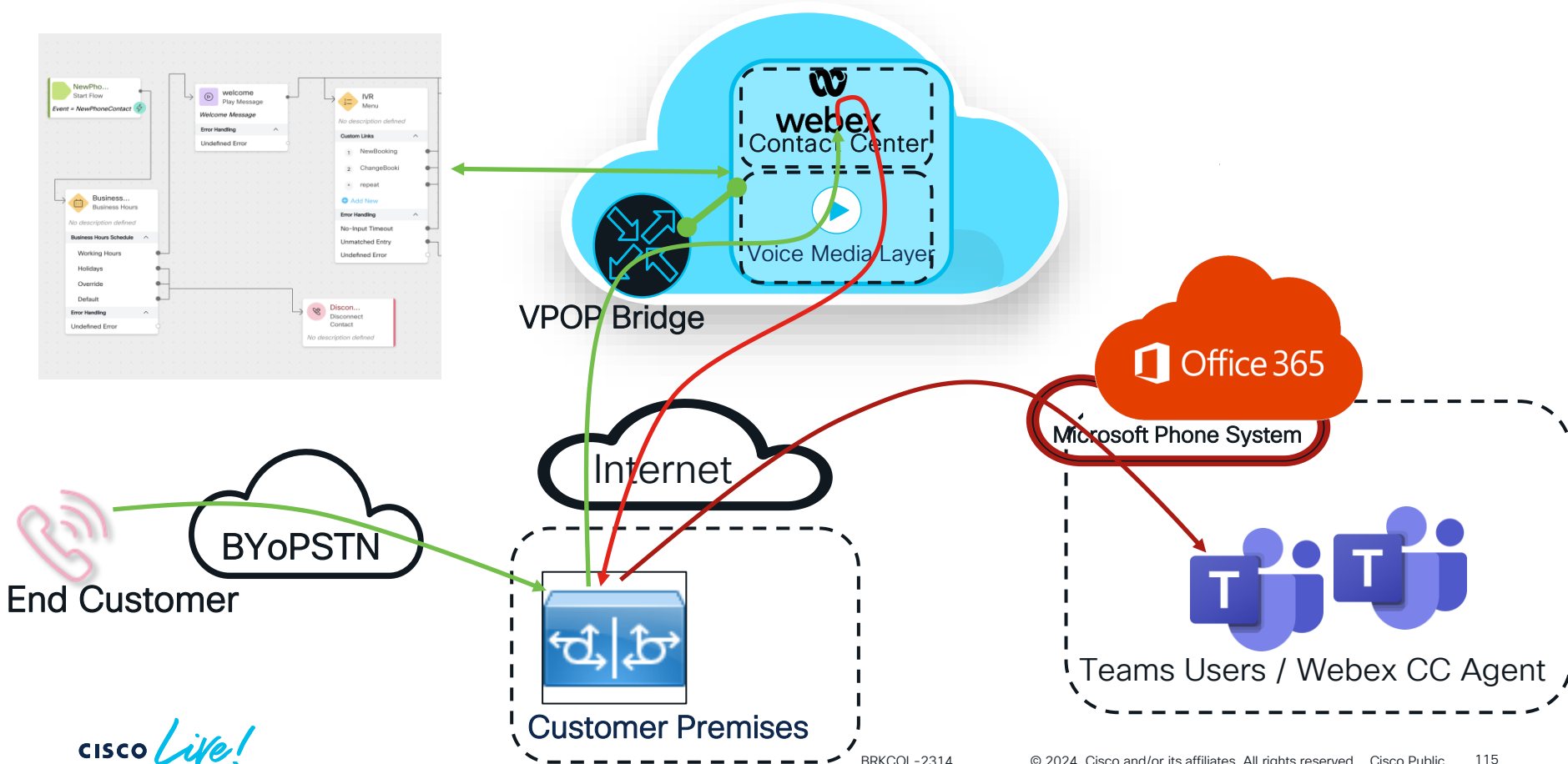
- The inbound dial-peer from Phone System is selected using the CUBE's FQDN as presented in the incoming TO: header. (dial-peer 290)
- NOTE : Inbound calls from the ITSP or UCM should use a different inbound dial-peer match criteria (e.g. VIA headers) and not CUBE's FQDN as shown above to ensure inbound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

# Webex Contact Center with MS teams



# References

# 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](#)
- [Deploying Cisco Catalyst 8000V Edge Software on Microsoft Azure](#)
- [Azure login](#)
- For VM image, search “Cisco Virtual CUBE Session Border Controller” in the Azure Marketplace
  - <https://azure.microsoft.com/en-us/partners/marketplace>

# Additional sessions on IOS-XE UC (CUBE, Local Gateway, Survivability Gateway)

- BROCOL-2314 CUBE v14 Updates
  - Session Room A4 – Tuesday 1:45PM – 2:45PM
- 
- BRKCOL-2312 High-Capacity Premises-based PSTN Option for Webex Calling
    - Session Room A1 – Wednesday 2:30PM – 3:30PM
  - Walk-in-Lab: LABCOL-2417 Certificate-based LGW for WxC
- 
- BRKCOL-2993 Enabling Site Survivability for Webex Calling
    - Session Room A9 – Thursday 10:30AM – 11:30AM
  - Walk-in-Lab: LABCOL-2416 Site Survivability for Webex Calling

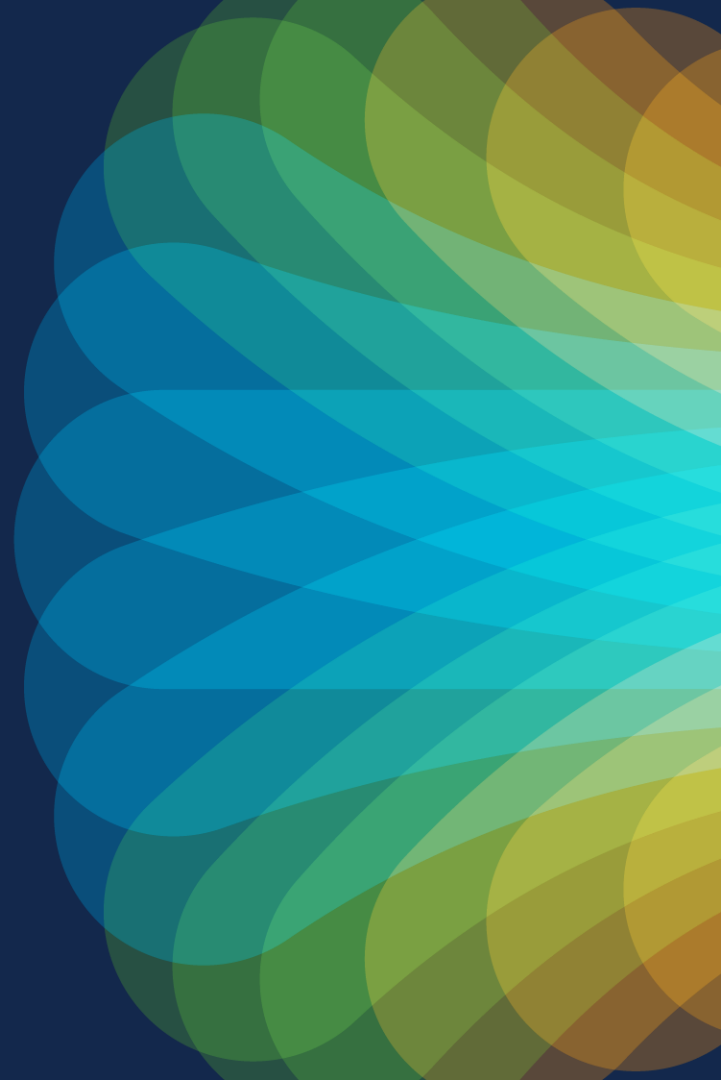




The bridge to possible

# Thank you

CISCO *Live!*



The background of the slide is a vibrant, abstract graphic. It features a large, stylized cloud shape on the left side, composed of overlapping, semi-transparent layers of orange, red, and yellow. To the right of the cloud, a bright, multi-colored sunburst or starburst pattern radiates outwards, transitioning through a spectrum of colors including yellow, green, blue, and purple. The overall effect is energetic and colorful.

cisco *Live!*

Let's go