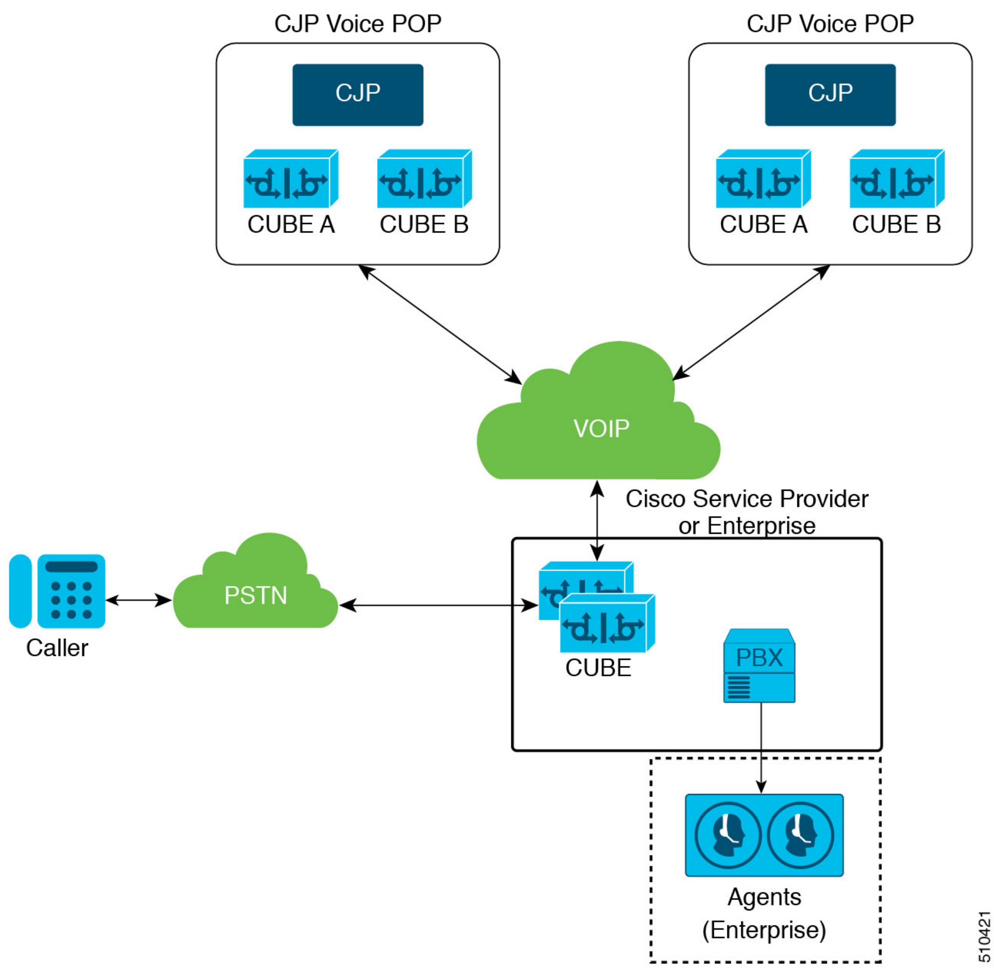
Voice Onboarding for Customer Journey Platform

Provision Voice for Customer Journey Platform

This document describes the setup of a Cisco Unified Border Element (CUBE) as the session border controller (SBC) at the customer enterprise or the Cisco service provider that connects to the Cisco Customer Journey Platform (CJP). Enterprise CUBE connects to a carrier for PSTN or VoIP connectivity on one side, and to CJP on the other side, to enable cloud contact center services. Both inbound and outbound calls to the CJP route through your enterprise CUBE. The customer provides TDM or SIP trunk, activated bidirectionally by both the service provider and CJP, to enable the call traffic between the platforms. For more information about CUBE, see Information About Cisco Unified Border Element.



Either the service provider or the customer enterprise can own and operate the CUBE and the PBX. In this case:

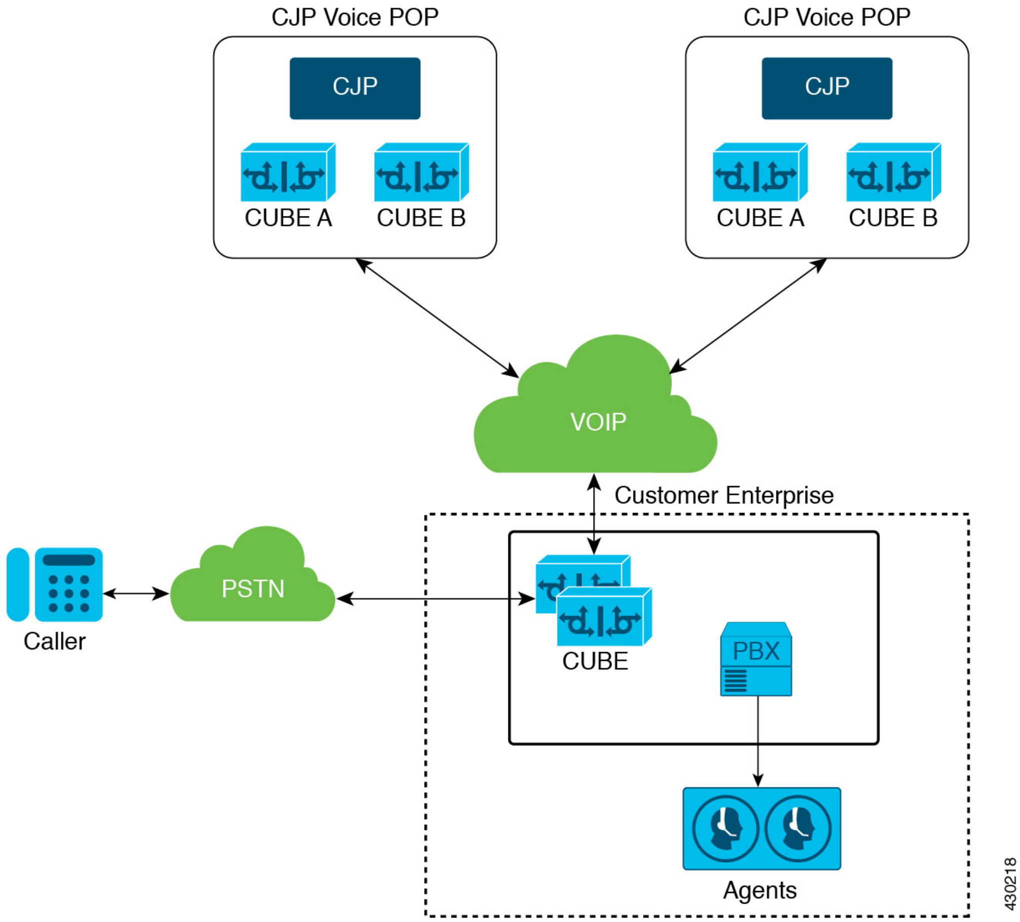
- All inbound calls to the CJP come through the carrier at the enterprise CUBE.
- CJP sends all outbound calls, whether to customers or agents, through the enterprise CUBE.
- CJP works with the service provider to bill the customer directly for PSTN usage, without going through CJP billing.

When the service provider owns the CUBE and the PBX, CJP provides a SIP header identifying the customer enterprise to the service provider. Service providers configure specific SIP header through the Application Service Provider dashboard.

CJP supports these SIP headers:

- Diversion
- PAI
- OTG
- DTG

In some cases, the customer enterprise owns and operates the CUBE and the PBX, which eliminates the need for a SIP header.



Related Topics

[Customer Journey Platform Call Flow]

[CUBE License and Sizing Requirements]

[CUBE Connectivity]

[Component Redundancy]

[Enterprise CUBE to Customer Journey Platform Configuration Example]

[Secure SIP Trunk Between CUBE and the Customer Journey Platform]

[Configure SIP Trunk for Your Tenant]

Customer Journey Platform Call Flow

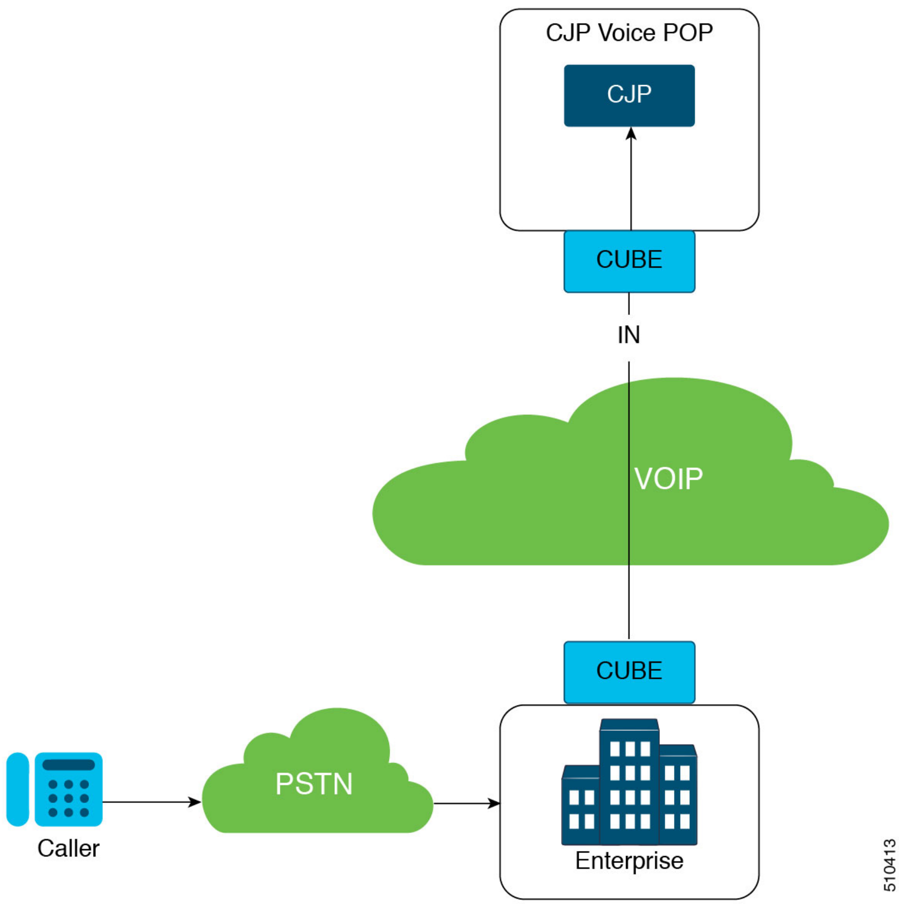
Inbound and outbound calls to CJP come through a carrier, which is routed through the Enterprise and CUBE.

Every call can include multiple sessions, depending on the call flow. Typical call flows include:

- Inbound call to an IVR
- Inbound call to an Agent
- Transfer and Conference
- Callback or Outbound call to a PSTN

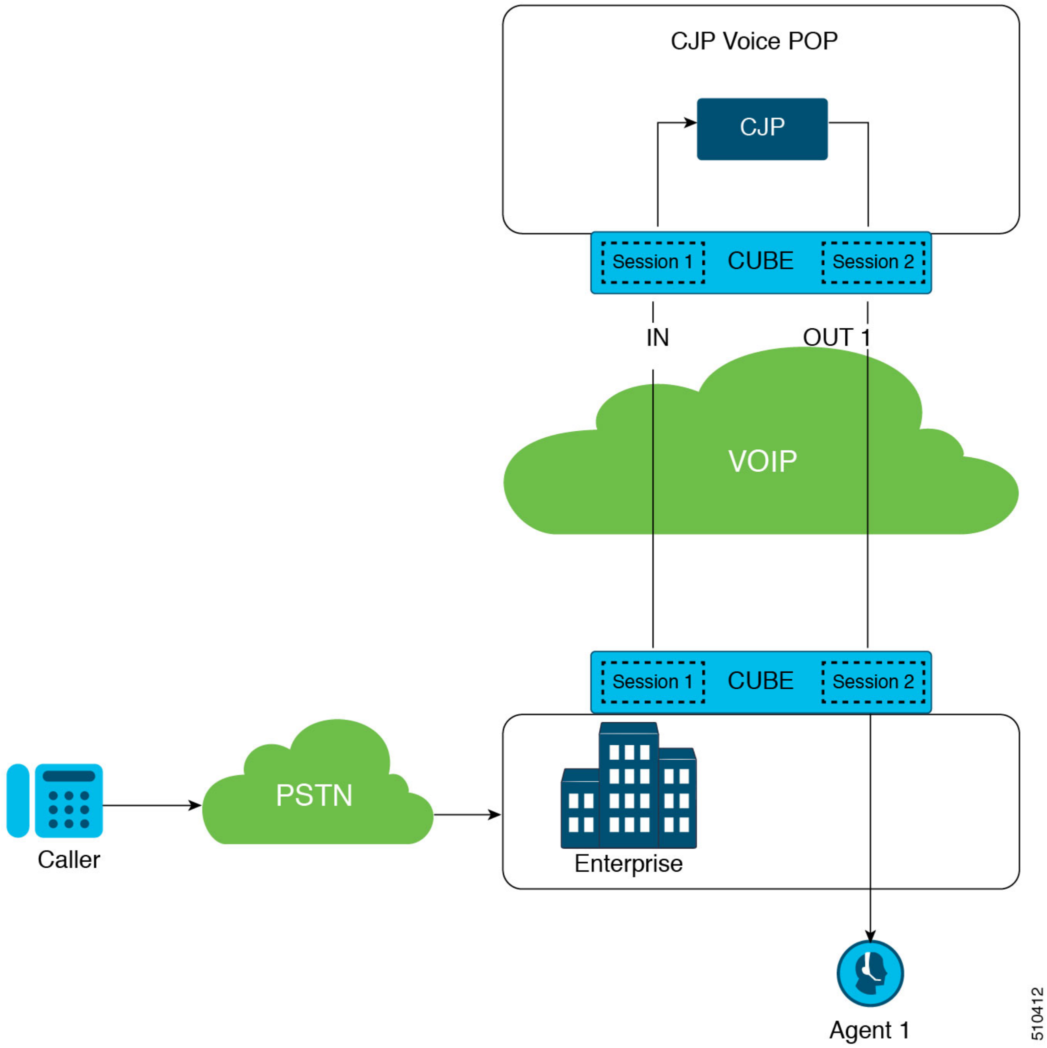
Inbound Call to an IVR

An inbound call from the caller to the CJP Voice POP creates a single session in the enterprise CUBE and a single session in the CJP CUBE.



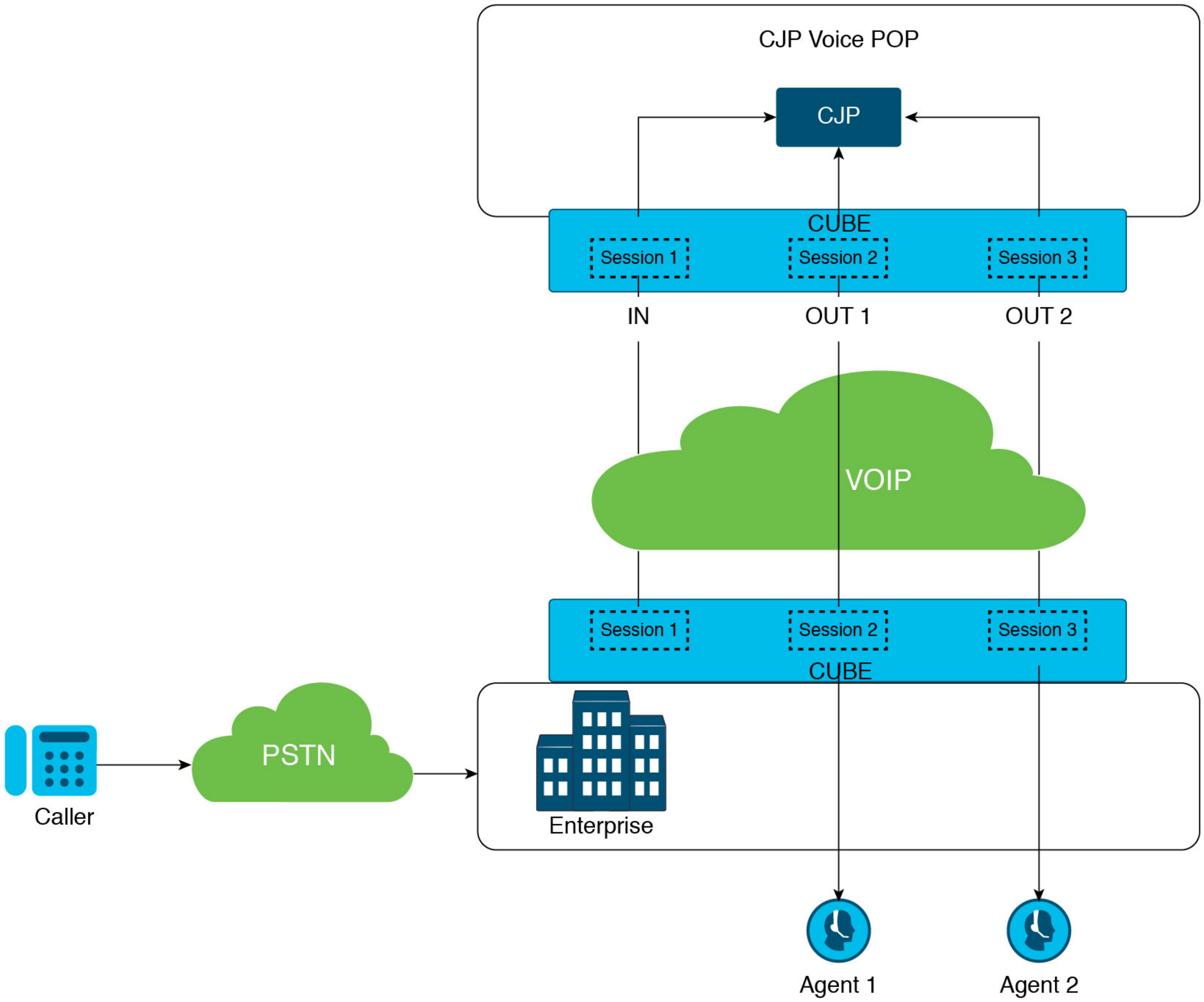
Inbound Call to an Agent

An inbound call to an agent adds an outbound session in the Customer Journey Portal CUBE and a single session in the enterprise CUBE.



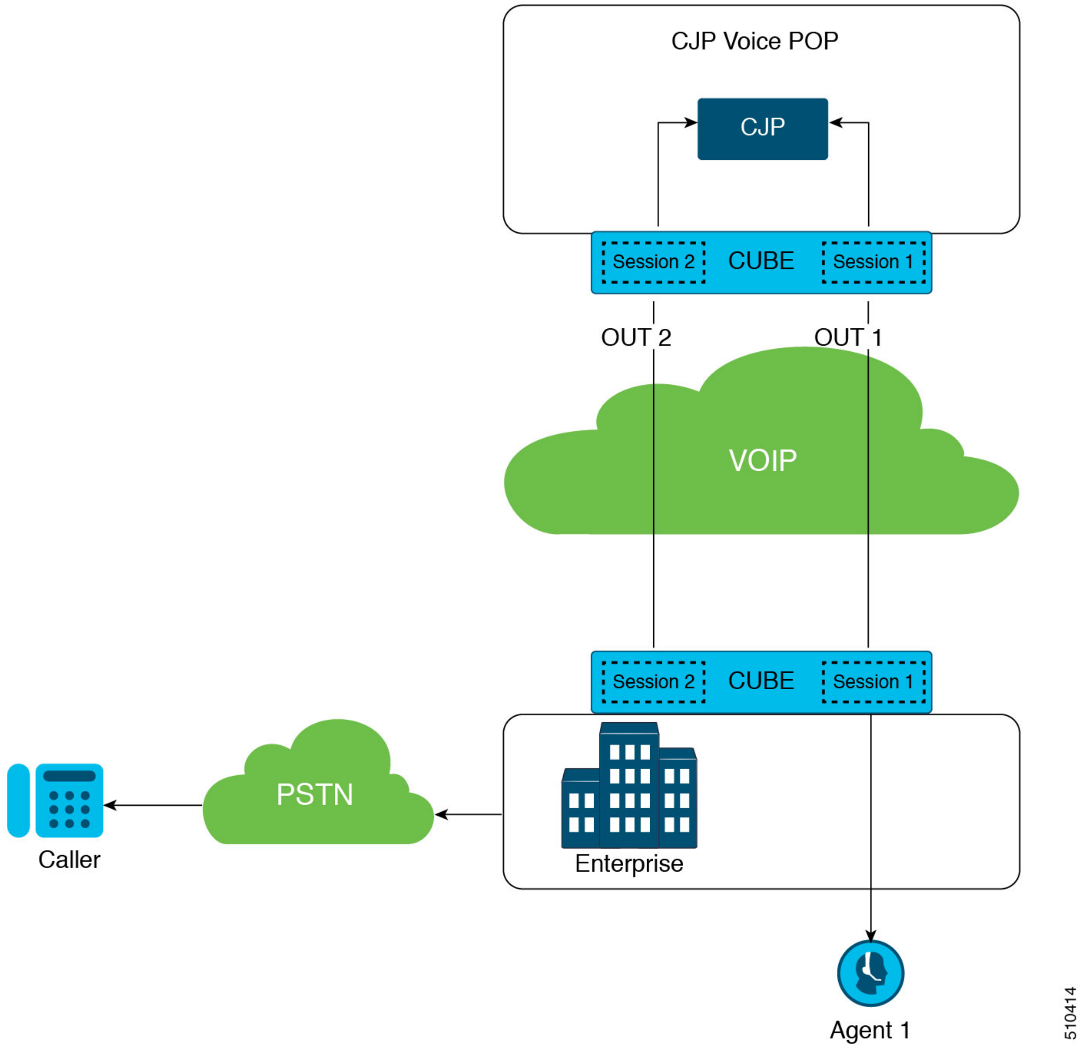
Conference and Consult Transfer

An agent to agent conference or consult transfer creates an additional outbound session in Customer Journey Portal and enterprise CUBE.



Callback or Outbound Call to PSTN

An outbound call creates two sessions, one from the Enterprise tenant to Customer Journey Portal and another from Customer Journey Portal to the Enterprise.



CUBE License and Sizing Requirements

CUBE Licensing

Cisco Unified Border Element (CUBE) is licensed per session and requires a two-way session. For more information, see Cisco Unified Border Element Data Sheet.

CUBE license sizing is the sum of the number of agent sessions and the number of calls at the Interactive Voice Response (IVR). Use the CUBE Data Sheet to determine the maximum number of sessions that your CUBE platform supports.

The number of licenses should be equal to the maximum capacity of the enterprise. Capacity is calculated as `(number of agents X 2) + (number of active sessions in queue).` For example:

- At peak time if you have 100 agents responding to customer calls, each call has two active sessions. The number of sessions is 200.

- The number of calls in queue in this instance is 100, which creates 100 sessions.
- Therefore, the total number of sessions equals 300 which is 300 licenses.

CUBE Session Sizing

A CUBE device can handle 1/3 of SIP sessions, if you have secured the calls using either TLS or SRTP. This is calculated as `((number of agents X 2) + (number of active sessions in queue)) X 3`. Using the example of 100 calls in queue with 100 agents responding to calls, the number of sessions is `((100 X 2)+ 100) X 3 = 900`.

You can size the CUBE for 300 sessions if you have provisioned a private WAN for the SIP Trunk.

Note If you are using SIP trunk over a public internet, you must secure it with SRTP/TLS.

To help determine the maximum number of agents, assume that:

- 50% of calls are queued and use IVR ports, while the remaining 50% of calls are active with agents.
- 10% of calls use the consult and conference supplementary services.
- 100% of calls are secured using either TLS or SRTP.

Based on these assumptions, CUBE platforms can support one agent for every 9.3 sessions.

CUBE Connectivity

You can connect to PSTN to allow local SIP trunk connectivity at enterprise and to CJP with appropriate CUBE IP addresses:

CJP Region	Voice POP CUBE IP Address
US	208.92.126.70 (LAX) 208.92.124.70 (JFK)
Europe	213.52.178.150 (AMS) 45.75.200.60 (LON)
Canada	149.97.158.70 (TOR) 173.205.108.170 (VAN)

Component Redundancy

Component redundancy allows the CJP to provide resilience when there is a service outage. You can configure both CJP cloud and enterprise CUBE to be redundant:

- Within a geographic region—You can set up more than one POP within an enterprise.
- Across enterprise data centers within a geographic region

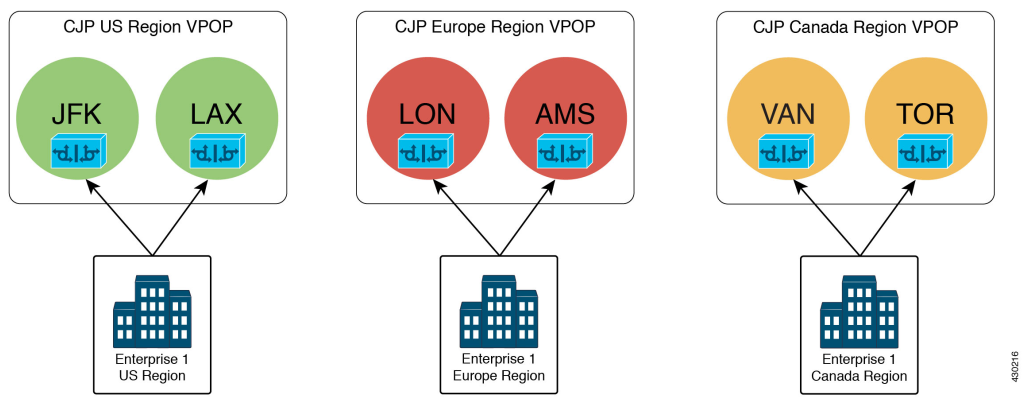
- Within enterprise networks—You can also set up CUBE in high availability (HA) mode. HA mode preserves oth signaling and media.

All signaling and media is sourced to and from the virtual IP address.

CJP uses two VPOPs to ensure high availability. For optimal performance, the service provider should also set up two POPs. This ensures that the hunting between the Customer Journey Platform VPOPs is an even round robin.

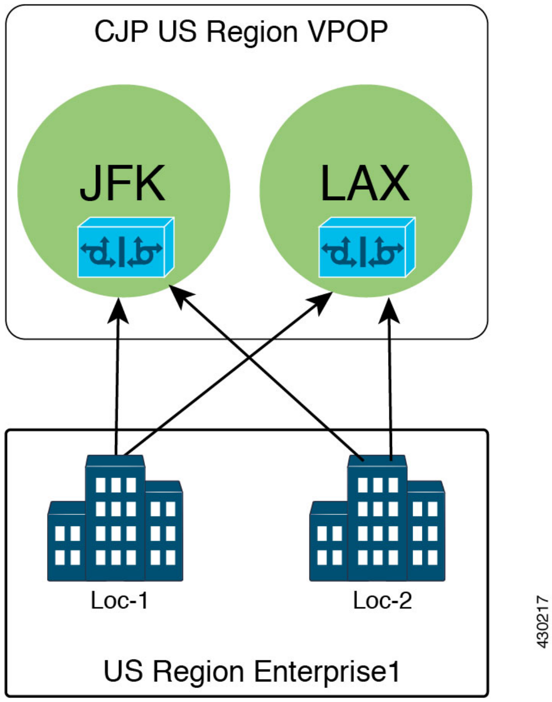
Redundancy Within a Geographic Region

Configure two VPOPs for each geographic region so that the enterprise CUBE can switch between VPOPs if a network failure occurs, with minimal call impact.

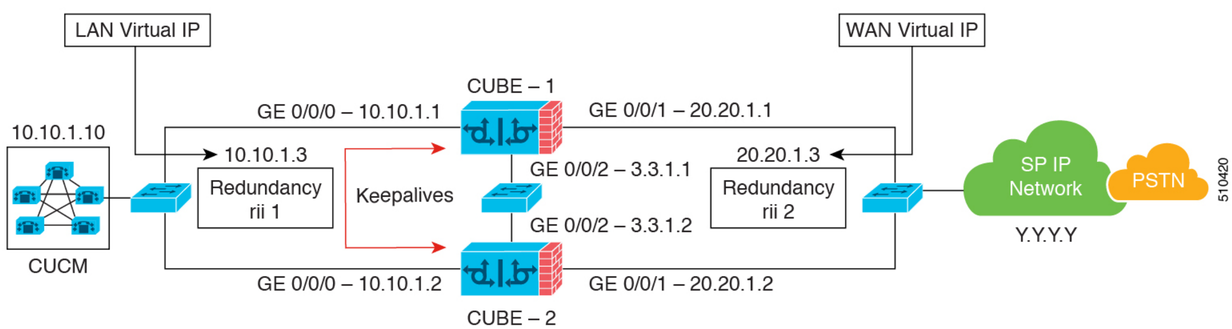


Redundancy Across Enterprise Data Centers Within a Geographic Region

Configure two data centers within the enterprise to connect to the same CJP VPOPs, within the same geographic region.



CUBE Redundancy Within the Enterprise Network



Using the CUBE High Availability (HA) feature with box-to-box redundancy ensures that the system preserves active calls when one of the CUBEs experiences an outage. Using the CUBE HA feature requires that all CUBEs:

- Use the same hardware configuration.
- Use the same software configuration.
- Use the same IOS version.
- Use the same type of platform.
- Use virtual IP addresses (VIP) for signaling and media.
- Are connected using a physical switch.

Note You can also use CUBEs as standalone SBCs. However, using standalone CUBEs does not provide redundancy within the enterprise network.

For more information on CUBE HA, see the CUBE Configuration Guide.

Example Configure Redundancy Groups and an Active-Standby Pairs

1. Configure the redundancy group and turn on CUBE redundancy:

```
redundancy
 application redundancy
  group 1
   name cubess-load-sbe-1
   priority 100 failover threshold 75
   timers delay 30 reload 60
   control GigabitEthernet2 protocol 1
   data GigabitEthernet2
   track 1 shutdown
   track 2 shutdown
  protocol 1
   name cubess-load-sbe-1
   authentication text sbe_1
!
voice service voip
redundancy-group 1
```

2. Track interfaces to trigger switchover:

```
track 1 interface GigabitEthernet1 line-protocol
track 2 interface GigabitEthernet2 line-protocol
!
redundancy
 application redundancy
  group 1
   track 1 shutdown
   track 2 shutdown
```

3. Redundancy interface identifier for inside and outside interface:

```
interface GigabitEthernet1
 ip address 10.1.20.10 255.255.255.0 #Example IP for illustration
 redundancy rii 15
 redundancy group 1 ip 10.1.20.115 exclusive
 hold-queue 10000 in
 hold-queue 10000 out
!
interface GigabitEthernet2
 ip address 10.2.20.10 255.255.255.0 #Example IP for illustration
!
```

4. Configuration on active and standby interface:

```
dial-peer voice 70021 voip
 description to-CUCM
 voice-class sip bind control source-interface GigabitEthernet1
 voice-class sip bind media source-interface GigabitEthernet1
dial-peer voice 70020 voip
 description to-SIP-SP
 voice-class sip bind control source-interface GigabitEthernet0
 voice-class sip bind media source-interface GigabitEthernet0
```

5. Configure media inactivity to clean up calls after failover that may not disconnect:

```
ip rtcp report interval 3000
!
gateway
 media-inactivity-criteria all
 timer receive-rtcp 5
 timer receive-rtp 86400
```

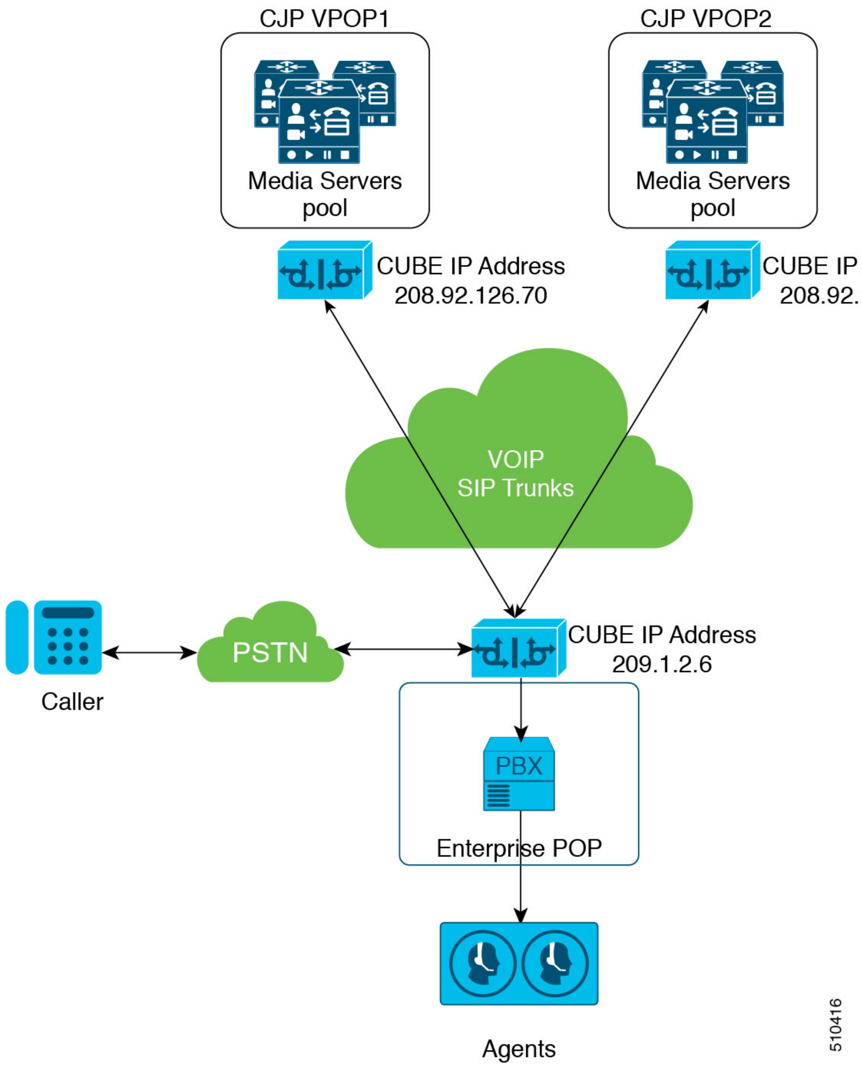
Enterprise CUBE to Customer Journey Platform Configuration Example

This configuration example applies to the Cisco IOS Voice Gateway and the Cisco UBE Voice gateway. For complete CUBE configuration instructions, see Cisco Unified Border Element Configuration Guide. All configurations in this example use global configuration mode. To enter global configuration mode:

1. Enter `enable` to enter privileged EXEC mode.
2. Enter `configuration terminal` to enter global configuration mode.

Common Configuration

This example shows CJP trunk provisioning in USA with this topology:



With these setup details:

- Configure server groups and SIP keepalive options.
- New dial peers with target destination IP address 208.92.126.70 for LAX, and 208.92.124.70 for JFK.
- Dial peer preference is equal to support 50/50% round robin.
- Codec and DTMF setup of G711 and RFC2833.
- Dial plan where the destination pattern matches CJP to agents through PBX and PSTN.
- More than one POP for high availability.

Basic Configuration

Set up NTP, DNS, and explicit trust list:

```
logging buffered 2000000 debugging
no logging console
service timestamps debug datetime msec localtime
ip routing
ip cef
ip source-route
ip name-server <DNS Server IP>

interface GigabitEthernet0/0
    ip route-cache same-interface
    ip address <ip address> <subnet mask>
    duplex auto
    speed auto
    no keepalive
    no cdp enable

voice service voip
    no ip address trusted authenticate
    media statistics
    media bulk-stats
    ip address trusted list
        ipv4 <0.0.0.0 0.0.0.0> # explicit Source IP Address Trust List
    allow-connections sip to sip
    signaling forward unconditional

ntp source GigabitEthernet0/0
ntp master 1
ntp server <NTP Server IP>
```

Configure Ingress Gateway

Step 1. Configure Global Settings.

Assume that the gateway licensed as a Cisco UBE:

```
voice service
mode border-element
sip
  rel1xx disable
  header-passing
error-passthru
 privacy-policy passthru
 pass-thru content unsupp
 options-ping 60
 midcall-signaling passthru
 pass-thru headers 1
voice class sip-hdr-passthrulist 1
 passthru-hdr CALL-Info
 passthru-hdr User-to-User
!
```

Step 2. Configure Voice Codec Preference Order.

CUBE uses codecs to reduce the call bandwidth usage by compressing digital voice samples. Setting the voice codec preference order allows you to select certain codecs over others depending on the geographic location of the caller. CJP supports the codecs:

- `g711ulaw`—For connections inside the United States.
- `g711alaw`—For connections outside the United States.

Configure your voice codec preference based on your region:

```
voice class codec 1
    codec preference 1 g711ulaw
```

For more information on CUBE video codecs, see Introduction to Codecs in the CUBE configuration guide.

Step 3. Configure Server Groups and SIP Keepalive Options.

This example demonstrates adding and setting the server selection mode to round robin.

Configure the server groups and SIP options keepalive using the US region CJP Voice Pop Mapping from the topology:

```
voice class server-group 100
 ipv4 208.92.124.70 preference 1 # JFK CUBE A
 ipv4 208.92.126.70 preference 1 # LAX CUBE A
 ipv4 208.92.124.70 preference 2 # JFK CUBE B
 ipv4 208.92.126.70 preference 2 # LAX CUBE B
 hunt-scheme round-robin
!
voice class server-group 101
 ipv4 209.1.2.6 preference 1 # PBX
 hunt-scheme round-robin
!
voice class sip-options-keepalive 200
 down-interval 10
 up-interval 10
 retry 2
 transport tcp
```

Step 4. Configure the Gateway and the SIP User Agent Timers.

```
gateway
 media-inactivity-criteria all
 timer receive-rtp 1200
sip-ua
 retry invite 2
 retry bye 1
 timers expires 60000
 timers connect 1000
 reason-header override
```

Step 5. Configure the POTS Dial-Peers for TDM Gateway.

If you are using a TDM gateway, configure the POTS dial-peers:

```
dial-peer voice 1 pots
    description TDM dial-peer
    incoming called-number .T
    direct-inward-dial
```

Step 6. Configure the Incoming PSTN SIP Trunk Dial Peer.

```
dial-peer voice 70000 voip
 description Incoming Call From SIP Trunk
 incoming called-number xxxx … #Customer specific pattern
 voice-class sip rel1xx disable
 dtmf-relay rtp-nte
 session protocol sipv2
 voice class codec 1
 no vad
```

Step 7. Configure the Switch Leg.

Use max-conn to prevent overloading of destination and options-keepalive to handle failover.

Note Configure switch dial-peers for every destination.

```
dial-peer voice 70021 voip
 description Used for Switch leg SIP Direct
 max-conn 225
 destination-pattern xxxx..... #Customer specific pattern
 session protocol sipv2
 session server-group 100
 session transport tcp
 voice-class codec 1
 voice-class sip options-keepalive profile 200
 dtmf-relay rtp-nte
 no vad
```

Step 8. Configure CUBE Hardware Resources (Optional).

Use this example to configure DSP resources. For gateways with physical DSP resources, configure Hardware resources using Unified Communications Manager. For more information, see the Cisco Unified Call Manager Configuration Guide.

1. Configure the voice-cards share the DSP resources located in Slot0:

```
voice-card 0
 dspfarm
 dsp services dspfarm
voice-card 1
 dspfarm
 dsp services dspfarm
voice-card 2
 dspfarm
 dsp services dspfarm
voice-card 3
 dspfarm
 dsp services dspfarm
voice-card 4
```

```
    dspfarm
    dsp services dspfarm
```

2. Reference the CallManager

```
sccp local GigabitEthernet0/0
sccp ccm ###.###.###.### identifier 1 priority 1 version 7.0 # Cisco Unified CM sub 1

sccp ccm ###.###.###.### identifier 2 priority 1 version 7.0 # Cisco Unified CM sub 2
```

3. Add an SCCP group for each of the hardware resource types:

```
sccp ccm group 1
    associate ccm 1 priority 1
    associate profile 2 register <gw70mtp>
    associate profile 1 register <gw70conf>
    associate profile 3 register <gw70xcode>
```

4. Configure DSPFarms for Conference, MTP, and Transcoder:

```
dspfarm profile 1 conference
    codec g711ulaw
    codec g711alaw
    codec g729r8
    maximum sessions 24
    associate application SCCP

dspfarm profile 2 mtp
    codec g711ulaw
    codec g711alaw
    codec g729r8
    maximum sessions software 500
    associate application SCCP

dspfarm profile 3 transcode universal
    codec g711ulaw
    codec g711alaw
    codec g729r8
    maximum sessions 52
    associate application SCCP
```

Note You only need the universal transcoder in certain cases.

5. Optionally, configure the SIP Trunk and Resource monitoring:

```
voice class resource-group 1
    resource cpu 1-min-avg threshold high 80 low 60
    resource ds0
    resource dsp
    resource mem total-mem
    periodic-report interval 30
```

6. Configure one rai target for each destination:

```
sip-ua
    rai target ipv4:###.###.###.### resource-group1 # UCM1A
    rai target ipv4:###.###.###.### resource-group1 # UCM2A
    rai target ipv4:###.###.###.### resource-group1 # UCM1B
    rai target ipv4:###.###.###.### resource-group1 # UCM2B
    permit hostname dns:%Requires manual replacement - ServerGroup Name defined in Server Groups%
```

Step 9. Configure the SIP Trunk and Resource Monitoring (Optional).

1. Configure the resources to be monitored

```
voice class resource-group 1
    resource cpu 1-min-avg threshold high 80 low 60
    resource ds0
    resource dsp
    resource mem total-mem
    periodic-report interval 30
```

2. Configure one rai target for each destination

```
sip-ua
    rai target ipv4:###.###.###.### resource-group1 # UCM1A
    rai target ipv4:###.###.###.### resource-group1 # UCM2A
    rai target ipv4:###.###.###.### resource-group1 # UCM1B
    rai target ipv4:###.###.###.### resource-group1 # UCM2B
    permit hostname dns:%Requires manual replacement - ServerGroup Name defined in Server Groups%
```

Configure the SIP trunk and resource monitoring:

Secure SIP Trunk Between CUBE and the Customer Journey Platform

This example demonstrates how to configure a SIP Transport Layer Security (TLS) connection between Cisco Unified Border Element (CUBE) and the Customer Journey Platform (CJP).

Before you Begin

Ensure that:

- The endpoints have the same date and time. You can synchronize endpoints by using a Network Time Protocol (NTP) server.

- You have TCP connectivity.
- The CUBE has the security and UCK9 licenses installed.

1. Create a trustpoint to hold the self-signed certificate of the CUBE:

```
crypto pki trustpoint CUBEtest(can be any name)
enrollment self-signed
serial-number none
fqdn none i
p-address none
subject-name cn= ISR4451-B.cisco.lab !(match the hostname of the router)
revocation-check none
rsakeypair ISR4451-B.cisco.lab !(match the hostname of the router)
```

2. Generate a self-signed certificate:

```
crypto pki enroll CUBEtest

% The fully-qualified domain name will not be included in the certificate

Generate Self Signed Router Certificate? [yes/no]: yes
```

3. Export the certificate:

```
crypto pki export CUBEtest pem terminal
```

4. Copy the self-signed certificate that you exported and save it as a text file with the `.pem` file extension.
5. Upload the self-signed CUBE certificate to CJP:
6. Copy the certificate from CJP:
7. Upload the CJP certificate to CUBE:

```
crypto pki trustpoint HOSTNAME
enrollment terminal
revocation-check none
crypto pku authenticate HOSTNAME

(PASTE THE CJP CERT HERE AND THEN PRESS ENTER TWICE)
```

   Enter `yes` when you are prompted to accept the certificate.

8. Configure SIP to use the self-signed certificate trustpoint that you created in step 1:

```
crypto signaling default trustpoint CUBEtest
```

9. Configure the dial peers with transport layer security:

```
dial-peer voice 9999 voip
answer-address 35..
destination-pattern 9999
```

```
session protocol sipv2
session target dns:cube-ent
session transport tcp tls
voice-class sip options-keepalive
srtp
```

Configure SIP Trunk for Your Tenant

Before You Configure

- Make sure you have the Gold partner tenant and access to the Service Provider Portal.
- Configure the enterprise session border controller. For more information, see Cisco Unified Border Element Configuration Guide.
- Obtain a destination address for your SIP Trunk. For more information, see SIP Binding for CUBE.

Provision Your Tenant

Cisco uses the provisioning information that you provide to configure the CJP session border controller for your tenant. Make sure that the information you provide matches your order, and is accurate. For instructions to provision your tenant, see the Cisco Customer Journey Platform Management Portal User Guide or the Cisco Customer Journey Platform Service Provider Portal User Guide.

- Configure a SIP trunk that connects your customer's IP address to the configured border controller. Make sure that you select **`CUBE`** for your **SIP Trunk Type**. Configure a SIP trunk for each CUBE you deploy.
- Create and provision a tenant.
- Assign SIP trunk to the tenant, add dial numbers and provision your new tenant.

Once the tenant is provisioned and the CJP CUBE is configured, you will receive an email that the tenant is ready for use.