Overview of Cisco Unified Border Element

Overview

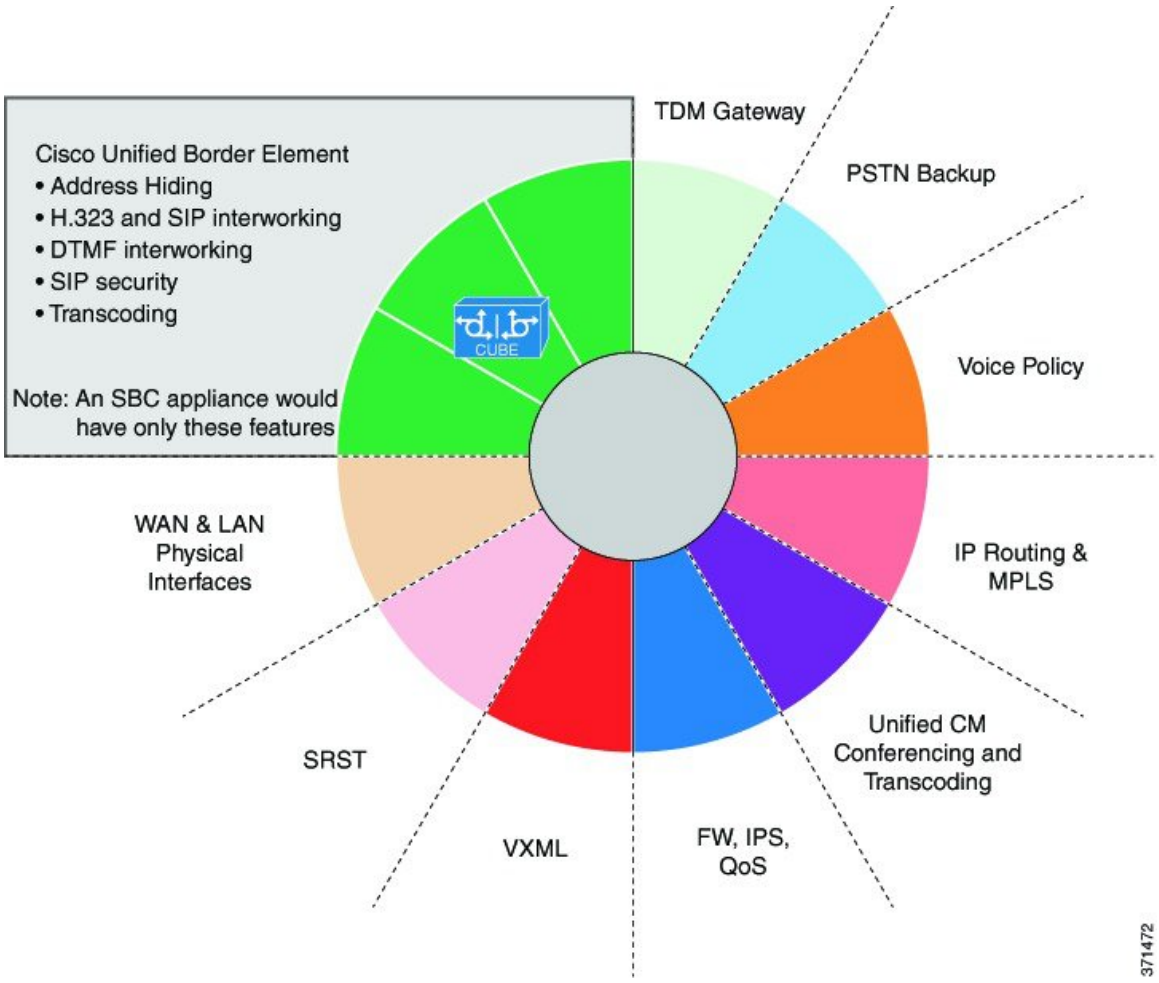
Cisco Unified Border Element (CUBE) bridges voice and video connectivity between two separate VoIP networks. It is similar to a traditional voice gateway, except for the replacement of physical voice trunks with IP-based voice trunks. Traditional gateways connect VoIP networks to telephone companies using a circuit-switched connection, such as PRI. The CUBE connects VoIP networks to other VoIP networks and enterprise networks to Internet telephony service providers (ITSPs).

CUBE terminates and originates signaling Session Initiation Protocol [SIP]) and media streams (Real-Time Transport Protocol [RTP] and RTP Control Protocol [RTCP]).

Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

CUBE offers a wide variety of enhanced features in addition to the conventional Session Border Controller (SBC) functions as shown in the chart below:

Figure 1: CUBE—More Than an SBC



The CUBE provides a network-to-network interface point for:

- Signaling interworking SIP.
- Media interworking—Dual-tone multifrequency (DTMF), fax, modem, and codec transcoding.
- Address and Port translations—Privacy and topology hiding.
- Billing and call detail record (CDR) normalization.
- Quality-of-service (QoS) and bandwidth management—QoS marking using differentiated services code point (DSCP) or type of service (ToS), audio quality monitoring bandwidth enforcement using Resource Reservation Protocol (RSVP), and codec filtering.
- Media Forking—Replicate media packets for advanced media services such as call recording, transcription, and customer assist service in contact center environments.
- Media Proxy—Proxy "forked media" session to multiple recipients for policy compliance, redundancy, and advanced media services.
- Security Demarcation—Unencrypted signaling or media to encrypted signaling or media interworking.

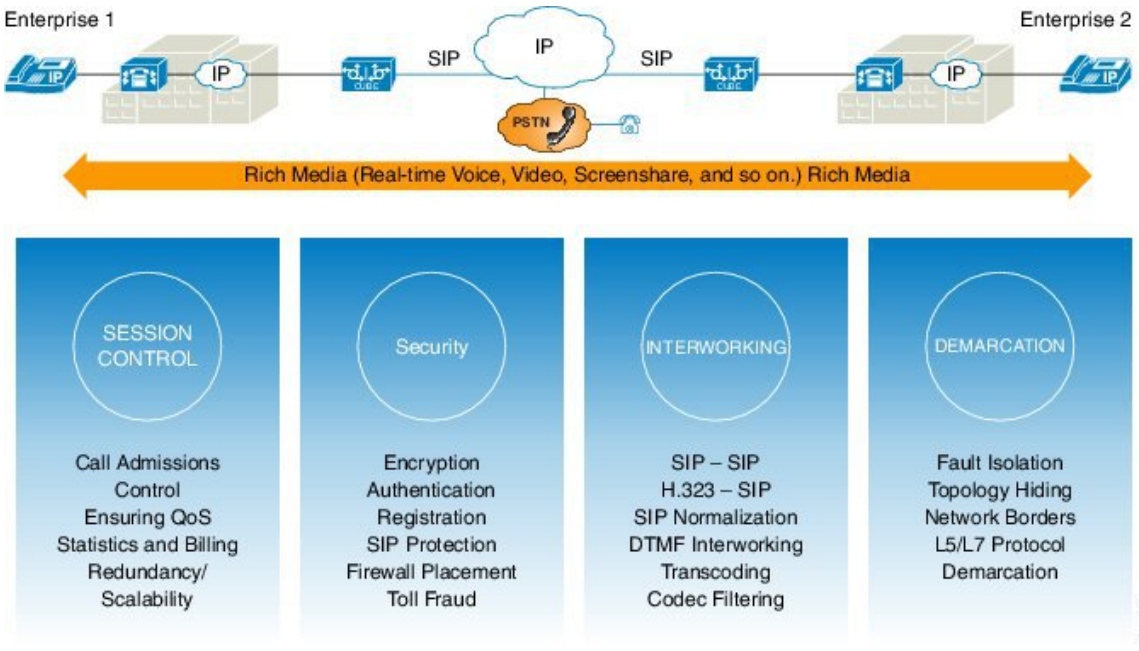
- Bridge enterprise and PSTN with cloud calling services such as Webex Calling, MS Teams Direct Routing and the like.

The CUBE provides a network-to-network demarcation interface for signaling interworking, media interworking, address and Port translations, billing, security, quality of service, call admission control, and bandwidth management.

The CUBE is used by enterprise and small and medium-sized organizations to interconnect SIP PSTN access with on-premise enterprise and hosted unified communications networks.

A CUBE interoperates with several different network elements including voice gateways, IP phones, and call-control servers in many different application environments, from advanced enterprise voice and video services with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, as well as simpler toll bypass and VoIP (VoIP) transport applications. The CUBE provides organizations with all the border controller functions integrated into the network layer to interconnect unified communications voice and video enterprise-to-service-provider architectures.

Figure 2: Why Does an Enterprise Need the CUBE



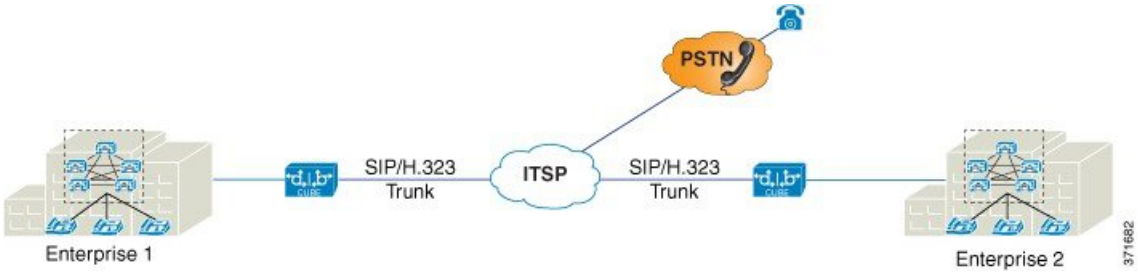
If enterprise subscribes to VoIP services offered by an ITSP, connecting the enterprise Cisco Unified Communications Manager through a CUBE provides network demarcation capabilities, such as security, topology hiding, transcoding, Call Admission Control, protocol normalization and SIP registration, none of which is possible if Cisco Unified Communications Manager connects directly to the ITSP. Another use case involves mergers or acquisitions in enterprise and the need to integrate voice equipment, such as CUCMs, IP PBXs, VM servers, and so on. If the networks in the two organizations have overlapping IP addresses, CUBE connects the two distinct networks until the acquired organization is migrated into the enterprise addressing plan.

SIP Trunking

The Session Initiation Protocol (SIP) is a signaling communications protocol, multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks. SIP trunking is the use of VoIP

to facilitate the connection of Private Branch Exchange (PBX) to other VoIP endpoints across the Internet. To use SIP trunking, an enterprise must have a PBX (internal VoIP system) that connects to all internal end users, an Internet Telephony Service Provider (ITSP), and a gateway that serves as the interface between the PBX and the ITSP. One of the most significant advantages of SIP trunking is the ability to combine data, voice, and video in a single line, eliminating the need for separate physical media for each mode.

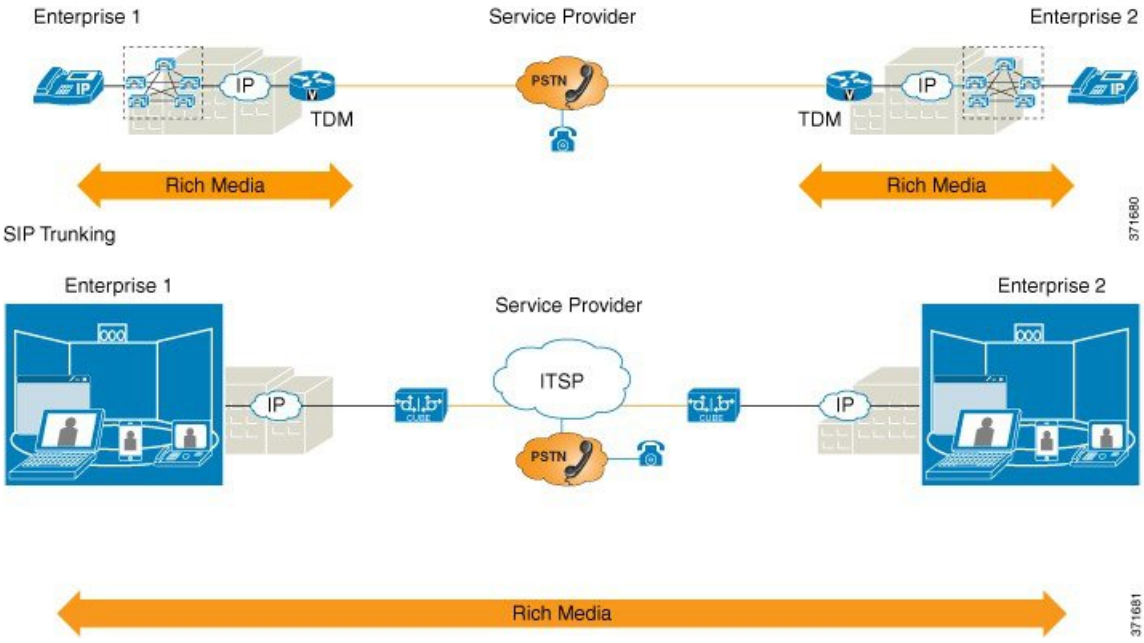
Figure 3: SIP Trunking



SIP trunking overcomes TDM barriers, in that it:

- Improves efficiency of interconnection between networks
- Simplifies PSTN interconnection with IP end-to-end
- Enables rich media services to employees, customers, and partners
- Carries converged voice, video, and data traffic

Figure 4: SIP Trunking Overcomes TDM Barriers



Note For Cisco IOS XE Gibraltar 16.11.1a and later releases, configure the either of the following CLIs to initiate the SIP processes:

- Voice dial-peer with **session protocol** as SIP.
- **voice register global**
- **sip-ua**

In the releases before Cisco IOS XE Gibraltar 16.11.1a, configure the following commands to initiate the SIP processes:

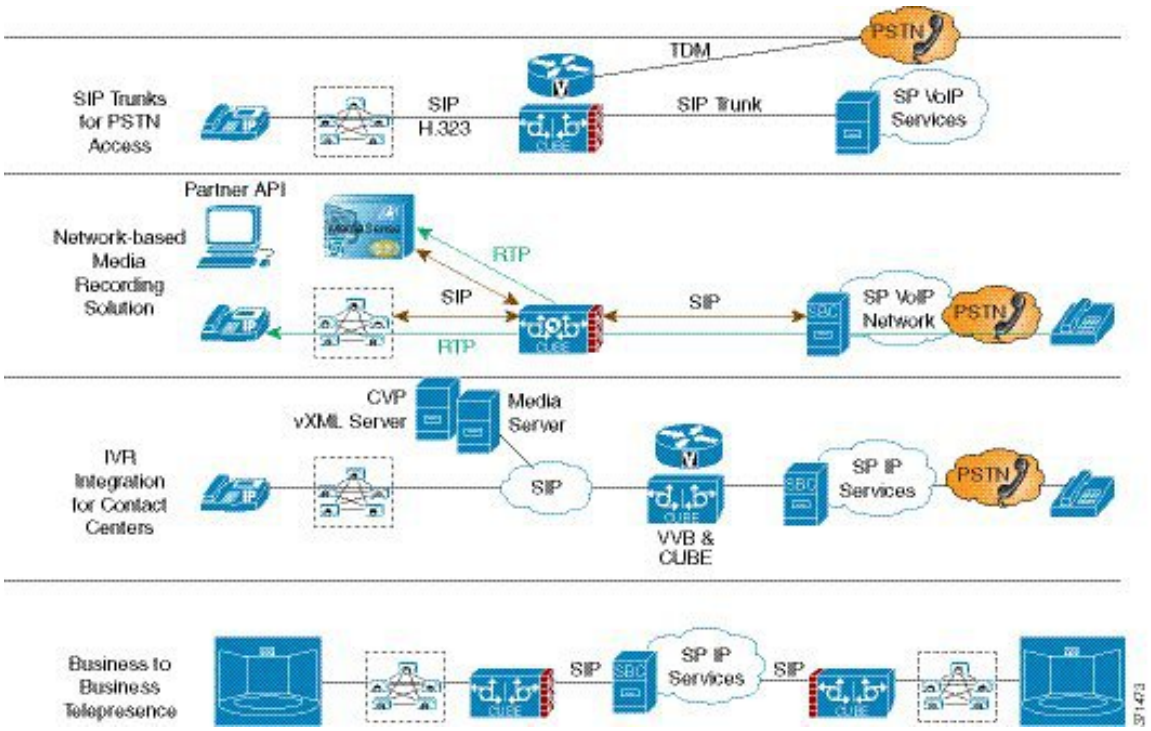
- **dial-peer voice** *(any)*
- **ephone-dn**
- **max-dn under call-manager-fallback**
- **ds0-group 0 timeslots 1 type e&m-wink-start**

Deployment Scenarios

CUBE in an enterprise environment that serves:

- PSTN Access: Connect on-prem enterprise voice and hosted UC network via SIP trunks for PSTN calling services
- Contact Center Integration: Integration with contact center software components to provide inbound calling, outbound dialing,call queuing, IVR streaming, agent transfer, and advanced media forking services.
- Webex Audio Edge: Connect on-prem enterprise/PSTN to Webex Meetings (audio dial-in/dial-out).
- Media Proxy/Forking
- Business-to-Business Telepresence
- Line side Registration Proxy

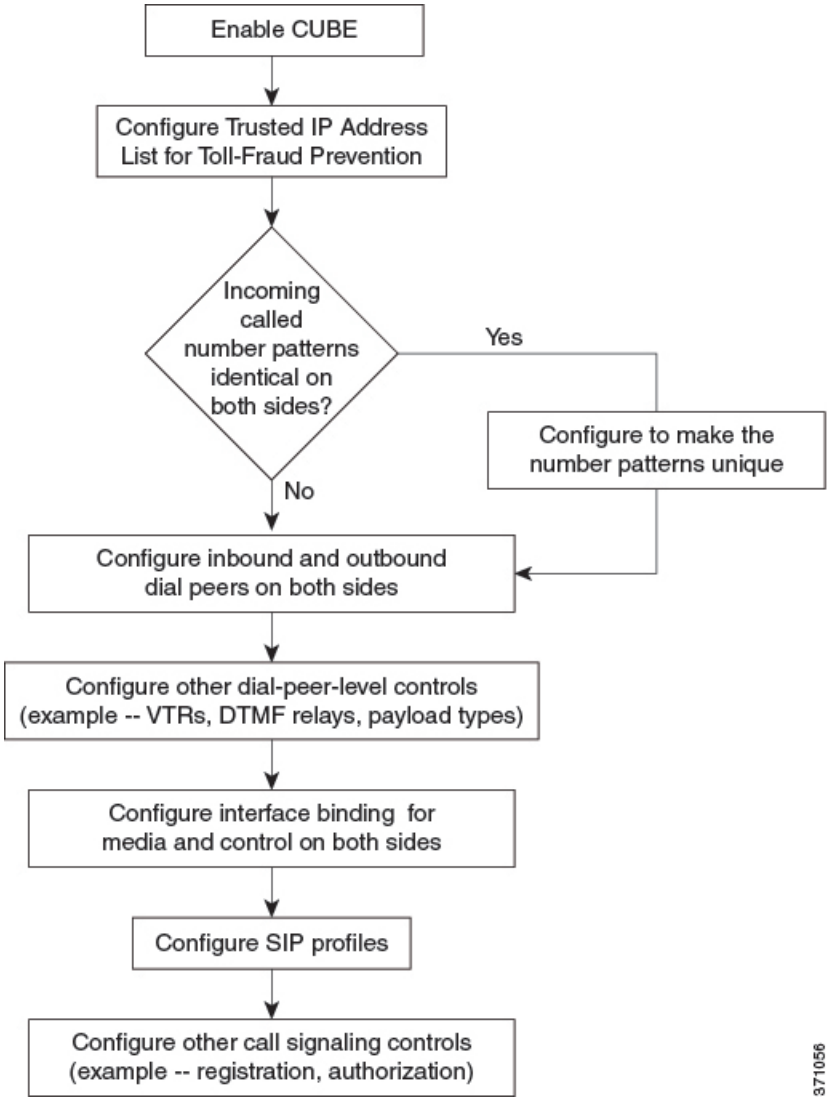
Figure 5: Typical Deployment Scenarios



Configure CUBE Features

Consider a scenario where XYZ corporation uses a VoIP network to provide phone services and uses a PRI connection for telecommunications services, and MGCP controls the PRI trunk. ITSP telecommunications provides migration from MGCP PRI to the SIP trunk. Cisco Unified Communications Manager (CUCM) sends the phone number, as 10 digits, to CUBE. CUCM sends only the extension (4 digits) to the CUBE. When the call is diverted (using call-forward), the requirement of the ITSP is that they need the full 10-digit number in the SIP Diversion field.

Figure 6: CUBE Configuration Workflow



The following sections describe the basic setup of CUBE through the steps that are involved in migrating the XYZ corporation to CUBE using a SIP trunk.

Enable the CUBE Application on a Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **mode border-element license** [**capacity** *sessions* | **periodicity** {**mins** *value* | **hours** *value* | **days** *value*}]
5. **allow-connections** *from-type* **to** *to-type*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters global VoIP configuration mode.

Step 4	**mode border-element license** [**capacity** *sessions* | **periodicity** {**mins** *value* | **hours** *value* | **days** *value*}]
	Example:
	`Device(conf-voi-serv)# mode border-element license capacity 200`
	`Device(conf-voi-serv)# mode border-element license periodicity days 15`
		Enables CUBE configuration and configures the number of licenses (capacity).
		• Effective from Cisco IOS XE Amsterdam 17.2.1r, the **capacity** keyword and *sessions* argument are deprecated. However, the keyword and argument are available in the Command Line Interface (CLI). If you try to configure license capacity using CLI, the following error message is displayed:
		`Error: CUBE SIP trunk licensing is now based on dynamic session counting. Static license capacity configuration has been deprecated.`
		• Effective from Cisco IOS XE Amsterdam 17.2.1r, the **periodicity** keyword and [**mins** | **hours**| **days**] argument are introduced. The **periodicity** keyword configures periodicity interval for license entitlement requests for CUBE. If you do not configure license periodicity, the default license period of 7 days is enabled.

	Command or Action	Purpose
		Note We recommend you to configure interval in days. Configuring interval in minutes or hours increases the frequency of entitlement requests and thereby increases the processing load on Cisco Smart Software Manager (CSSM). License periodicity configuration of minutes or hours is recommended to be used only with Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite) mode.
Step 5	**allow-connections** *from-type* **to** *to-type* **Example:** `Device(conf-voi-serv)# allow-connections sip to sip`	Allows connections between specific types of endpoints in a VoIP network. • The two protocols (endpoints) refer to the VoIP protocols (SIP) on the two call legs.
Step 6	**end** **Example:** `Device(conf-voi-serv)# end`	Returns to privileged EXEC mode.

Verify CUBE on the Device

SUMMARY STEPS

1. **enable**
2. **show cube status**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show cube status**

Displays the CUBE status, the software version, the license capacity, the image version, and the platform name of the device. In releases before , CUBE status display is enabled only if **mode border-element** command is configured with call license capacity. Effective from Cisco IOS XE Amsterdam 17.2.1r, this dependency is removed and Licensed-Capacity information is excluded from output.

Example:

Before Cisco IOS XE Amsterdam 17.2.1r:

```
Device# show cube status

CUBE-Version : 12.5.0
SW-Version : 16.11.1, Platform CSR1000V
HA-Type : none
Licensed-Capacity : 10
Calls blocked (Smart Licensing Not Configured) : 0
Calls blocked (Smart Licensing Eval Expired) : 0
```

Effective from Cisco IOS XE Amsterdam 17.2.1r:

```
Device# show cube status

CUBE-Version : 12.8.0
SW-Version : 17.2.1, Platform CSR1000V
HA-Type : none
```

Configure a Trusted IP Address List for Toll-Fraud Prevention

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **ip address trusted list**
5. **ipv4** *ipv4-address* [*network-mask*]
6. **ipv6** *ipv6-address*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters global VoIP configuration mode.
Step 4	**ip address trusted list** **Example:** `Device(conf-voi-serv)# ip address trusted list`	Enters IP address trusted list mode and enables the addition of valid IP addresses.

	Command or Action	Purpose
Step 5	**ipv4** *ipv4-address* [*network-mask*] **Example:** `Device(cfg-iptrust-list)# ipv4 192.0.2.1 255.255.255.0`	Allows you to add up to 100 IPv4 addresses in the IP address trusted list. Duplicate IP addresses are not allowed. • The *network-mask* argument allows you to define a subnet IP address.
Step 6	**ipv6** *ipv6-address* **Example:** `Device(cfg-iptrust-list)# ipv6 2001:DB8:0:ABCD::1/48`	Allows you to add IPv6 addresses to the trusted IP address list.
Step 7	**end** **Example:** `Device(cfg-iptrust-list)# end`	Returns to privileged EXEC mode.