Overview of Cisco Unified Border Element

Cisco Unified Border Element (CUBE) is a unified communications border element, providing voice and video connectivity between the enterprise IP network and service provider network. It is similar to a voice gateway, except for the replacement of physical voice trunks with an IP connection.

Information about Cisco Unified Border Element

Cisco Unified Border Element (CUBE) is network border element that can terminate and originate signaling (H.323 and Session Initiation Protocol [SIP]), media streams (Real-Time Transport Protocol [RTP] and RTP Control Protocol [RTCP]).

Session Border controller (SBC) was used by service providers (SP) to enable full billing capabilities within VoIP networks. CUBE provides the extended functionality of interconnecting VoIP networks, especially on the enterprise side.

CUBE functionality is implemented on devices using a special IOS feature set, which allows CUBE to route a call from one VoIP dial peer to another. As VoIP dial peers can be handled by either SIP or H.323, CUBE can be used to interconnect VoIP networks of different signaling protocols. VoIP internetworking is achieved by connecting an inbound dial peer with an outbound dial peer. A standard Cisco IOS gateway without CUBE functionality cannot allow VoIP-to-VoIP connections.

Protocol internetworking is possible for the following combinations:

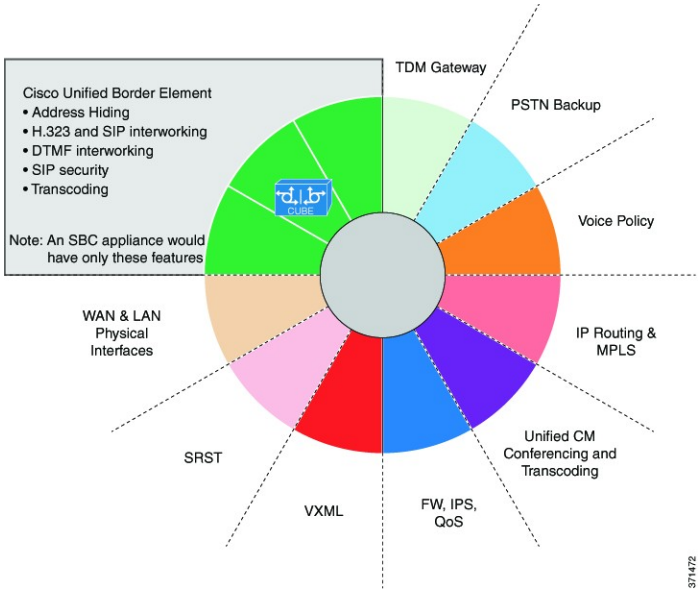
- H.323-to-SIP internetworking
- H.323-to-H.323 internetworking
- SIP-to-SIP internetworking

CUBE is used by enterprise and small and medium-sized organizations to interconnect SIP PSTN access with SIP and H.323 enterprise 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/or video services with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, as well as simpler toll bypass and voice over IP (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 1: Cisco Unified Border Element—More than an SBC

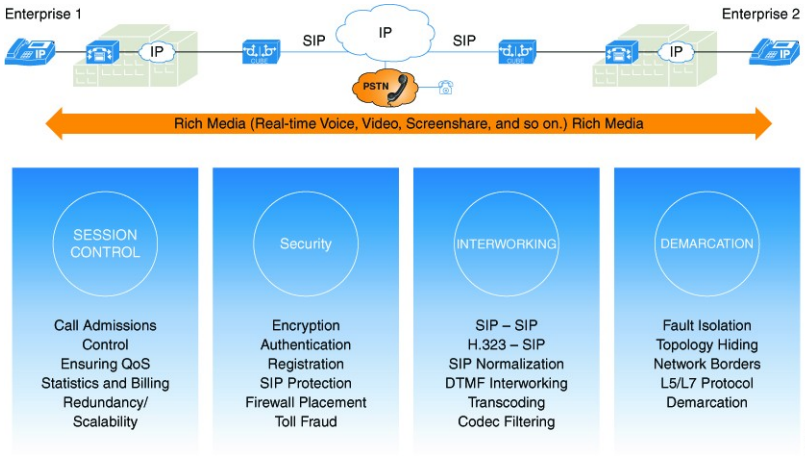


The CUBE provides a network-to-network interface point for:

- Signaling interworking—H.323 and 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), bandwidth enforcement using Resource Reservation Protocol (RSVP), and codec filtering.

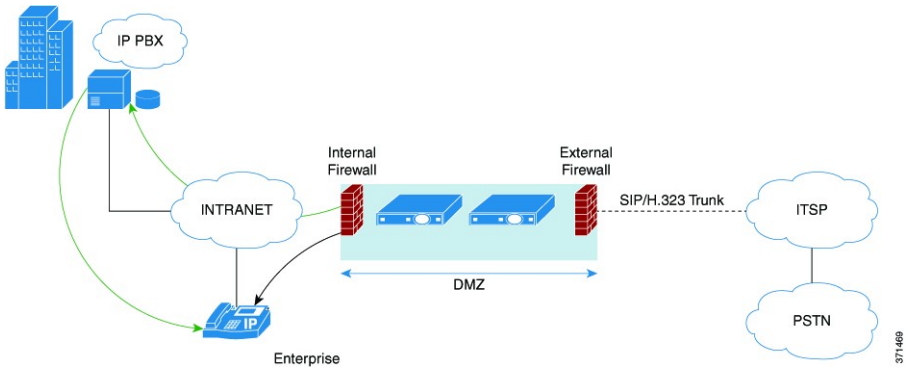
Figure 2: Why does an enterprise need the CUBE?



SIP/H.323 Trunking

The Session Initiation Protocol (SIP) is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks. SIP (or H.323) trunking is the use of VoIP to facilitate the connection of a private branch exchange (PBX) to the Internet. To use SIP trunking, an enterprise must have a PBX 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 its ability to combine data, voice, and video in a single line, eliminating the need for separate physical media for each mode.

Figure 3: SIP/H.323 Trunking

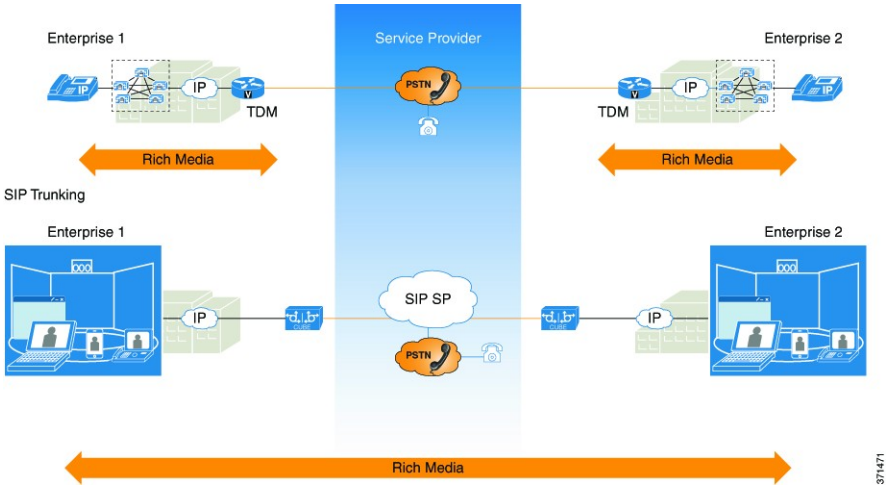


SIP trunking overcomes TDM barriers, in that it:

- 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



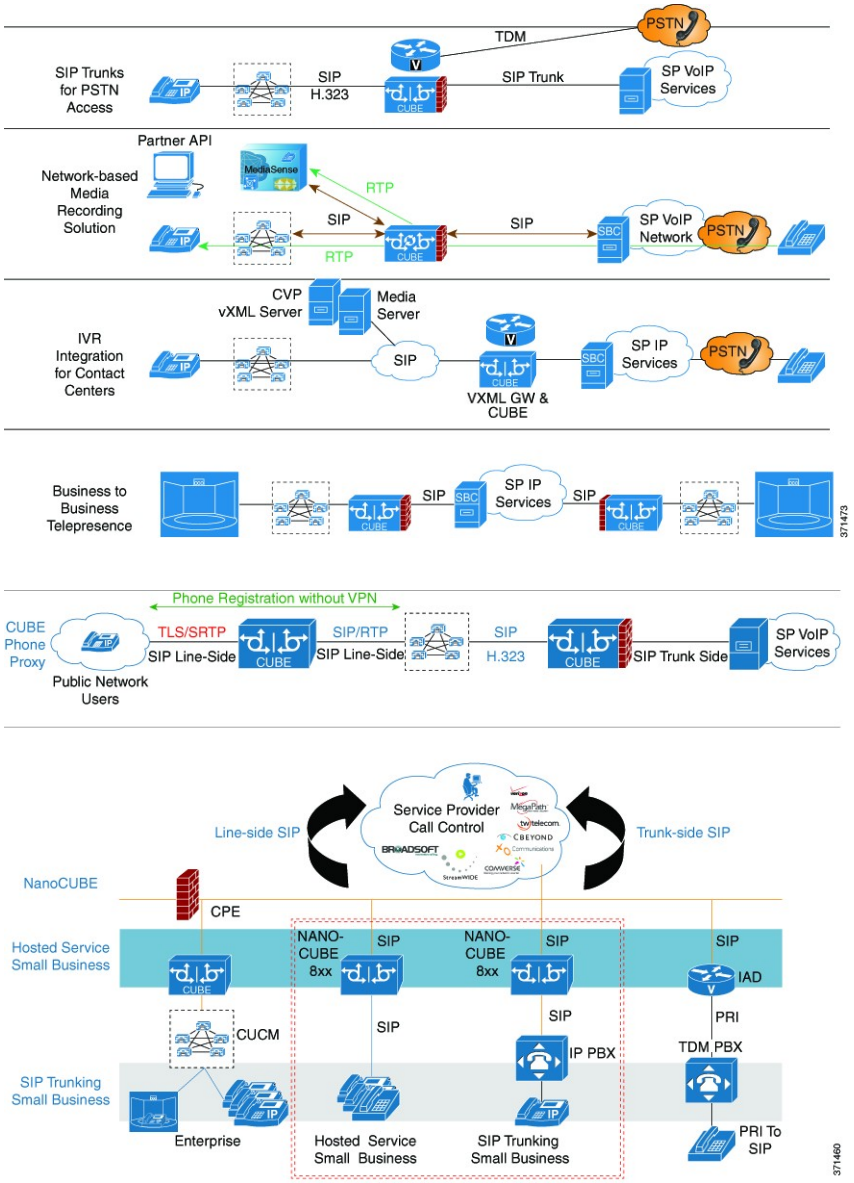
Typical Deployment Scenarios for CUBE

CUBE in an enterprise environments serve two main purposes:

- External Connections-CUBE is the demarcation point within a unified communications network and provides interconnectivity with external networks. This includes H.323 voice and video connections and SIP VoIP connections.

- Internal Connections-When used within a VoIP network, CUBE increases flexibility and interoperability between devices.

Figure 5: Typical Deployment Scenarios

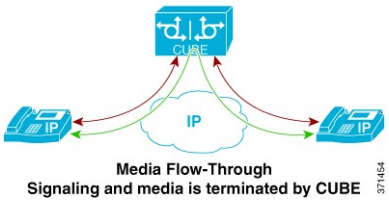


CUBE Deployment Modes

- Media flow-through—CUBE acts as a back-to-back user agent. In a media flow-through mode, between two endpoints, both signaling and media flows through the IP-to-IP Gateway (IPIP GW). The IPIP GW

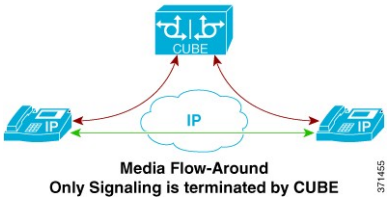
performs both signaling and media interworking between H.323/SIP IPv4 and SIP IPv6 networks. Media-flow-through mode is recommended when CUBE is used as an SBC for PSTN connectivity.

Figure 6: Media flow-through



- Media flow-around—Only signaling is terminated at CUBE. Media bypasses CUBE and flows directly between the endpoints. This mode is recommended to be used only if CUBE is deployed within an enterprise network.

Figure 7: Media flow-around



How to Configure Basic CUBE Tasks

Enabling the CUBE application on a Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **mode border-element license capacity** *sessions*
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* **Example:** `Device(conf-voi-serv)# mode border-element license capacity 200`	Enables the set of commands used in the CUBE. • You can configure the number of licenses (capacity) to be enabled for the CUBE.
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 on the two call legs.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(conf-voi-serv)# end`	Returns to privileged EXEC mode.

Configuring 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 voice service 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`	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.