VoIP for IPv6

This document describes VoIP in IPv6 (VoIPv6), a feature that adds IPv6 capability to existing VoIP features. This feature adds dual-stack (IPv4 and IPv6) support on voice gateways and media termination points (MTPs), IPv6 support for Session Initiation Protocol (SIP) trunks, and support for Skinny Client Control Protocol (SCCP)-controlled analog voice gateways. In addition, the Session Border Controller (SBC) functionality of connecting a SIP IPv4 or H.323 IPv4 network to a SIP IPv6 network is implemented on a Cisco UBE to facilitate migration from VoIPv4 to VoIPv6.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VoIP for IPv6

- Cisco Express Forwarding for IPv6 must be enabled.
- Virtual routing and forwarding (VRF) is not supported in IPv6 calls.

Cisco Unified Border Element

- Cisco IOS Release 12.4(22)T or a later release must be installed and running on your Cisco UBE.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.3S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for Implementing VoIP for IPv6

The following are the restrictions for Cisco UBE features:

Media Flow–Through

- Video call flows with Alternative Network Address Types (ANAT) are not supported.
- WebEx call flow with ANAT are not supported (Cisco UBE does not support ANAT on Video and Application media types).

SDP Pass-Through

- Supports only Early Offer (EO)–Early Offer (EO) and Delayed Offer (DO)–Delayed Offer (DO) call flows.
- Delayed Offer–Early Offer call flow falls back to Delayed Offer–Delayed Offer call flow.
- Supplementary services are not supported on SDP Pass-Through.
- Transcoding and DTMF interworking are not supported.

Note The above SDP Pass–Through restrictions are applicable for both IPv4 and IPv6.

- SDP Pass–Through does not support the dual-stack functionality.
- ANAT call flows does not support IPv4-to-IPv6 and IPv6-to-IPv4 Media interworking.

UDP Checksum

- CEF and process options are not supported on ASR1000 series routers.
- None option is partially supported on ISR–G2.

Media Anti–Trombone

- Media Anti–Trombone is not enabled if the initial call before tromboning is in Flow–Around (FA) mode.
- Media Anti–Trombone supports only symmetric media address type interworking (IPv4-IPv4 or IPv6-IPv6 media) with or without ANAT.
- Does not provide support for IPv4-IPv6 interworking cases with or without ANAT because Cisco UBE cannot operate in FA mode post tromboning.

Information About VoIP for IPv6

SIP Features Supported on IPv6

The Session Initiation Protocol (SIP) is an alternative protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP.

The Cisco SIP functionality enables Cisco access platforms to signal the setup of voice and multimedia calls over IP networks. SIP features also provide advantages in the following areas:

- Protocol extensibility
- System scalability
- Personal mobility services
- Interoperability with different vendors

A SIP User Agent (UA) operates in one of the following three modes:

- IPv4-only: Communication with only IPv6 UA is unavailable.
- IPv6-only: Communication with only IPv4 UA is unavailable.
- Dual-stack: Communication with only IPv4, only IPv6 and dual-stack UAs are available.

Dual-stack SIP UAs use Alternative Network Address Transport (ANAT) grouping semantics:

- Includes both IPv4 and IPv6 addresses in the Session Description Protocol (SDP).
- Is automatically enabled in dual-stack mode (can be disabled if required).
- Requires media to be bound to an interface that have both IPv4 and IPv6 addresses.
- Described in RFC 4091 and RFC 4092 (RFC 5888 describes general SDP grouping framework).

SIP UAs use “sdp-anat” option tag in the Required and Supported SIP header fields:

- Early Offer (EO) INVITE using ANAT semantics places “sdp-anat” in the Require header.
- Delayed Offer (DO) INVITE places “sdp-anat” in the Supported header.

SIP Signaling and Media Address Selection:

- Source address for SIP signaling is selected based on the destination signaling address type configured in the session-target of the outbound dial-peer:
  - If signaling bind is configured, source SIP signaling address is chosen from the bound interface.
  - If signaling bind is not configured, source SIP signaling address is chosen based on the best address in the UA to reach the destination signaling address.

SDP may or may not use ANAT semantics:

- When ANAT is used, media addresses in SDP are chosen from the interface media that is configured. When ANAT is not used, media addresses in SDP are chosen from the interface media that is configured

OR based on the best address to reach the destination signaling address (when no media bind is configured).

VoIPv6 Support on Cisco UBE

Cisco UBE in VoIPv6 adds IPv6 capability to VoIP features. This feature adds dual-stack support on voice gateways, IPv6 support for SIP trunks, support for SCCP-controlled analog voice gateways, support for real-time control protocol (RTCP) pass-through, and support for T.38 fax over IPv6.

For more information on these features, refer to the following:

- "Configuring Cisco IOS Gateways" section in the Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager
- "Trunks" section in Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager
- "SCCP-controlled analog voice gateways" section in the SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways
- "RTCP Pass-Through" section in Cisco UBE RTCP Voice Pass-Through for IPv6
- "T.38 fax over IPv6" section in Fax, Modem, and Text Support over IP Configuration Guide

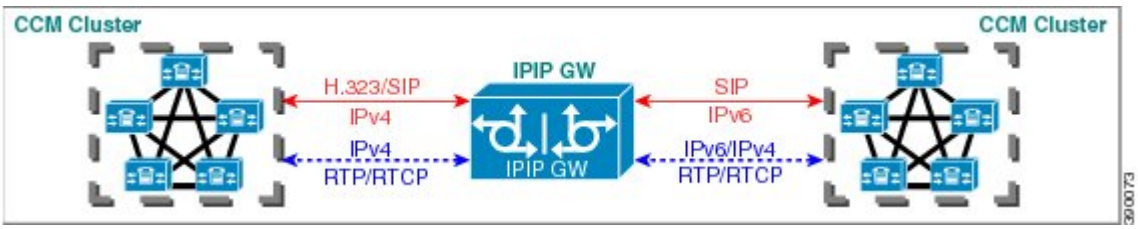
Support has been added for audio calls in media Flow–Through (FT) and Flow–Around (FA) modes, High Density (HD) transcoding, Local Transcoding Interface (LTI), along with Voice Class Codec (VCC) support, support for Hold/Resume, REFER, re-INVITE, 302 based services, and support for media anti-trombone have been added to Cisco UBE.

Cisco UBE being a signaling proxy processes all signaling messages for setting up media channels. This enables Cisco UBE to affect the flow of media packets using the media flow-through and the media flow-around modes.

- Media FT and Media FA modes support the following call flows:
  - EO–to–EO
  - DO–to–DO
  - DO–to–EO

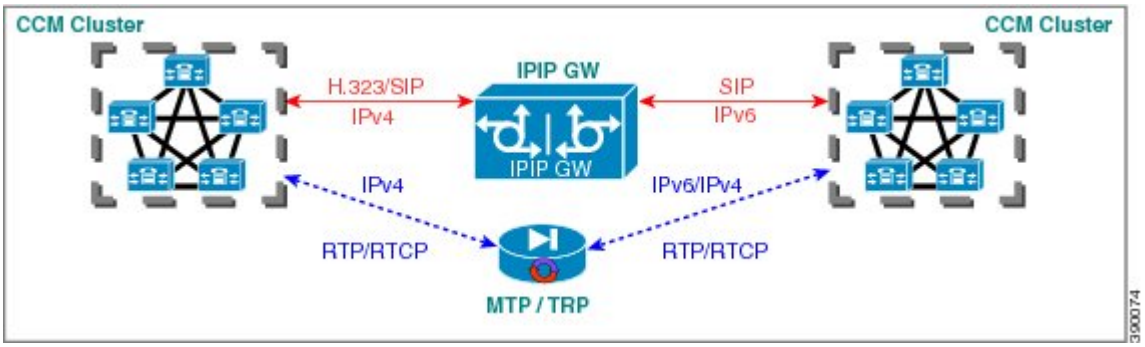
- **Media Flow-Through (FT)**: In a media flow–through mode, between two endpoints, both signaling and media flows through the IP-to-IP Gateway (IPIP GW). The IPIP GW performs both signaling and media interworking between H.323/SIP IPv4 and SIP IPv6 networks.

Figure 1: H.323/SIP IPv4 – SIP IPv6 interworking in media flow-through mode



- **Media Flow-Around (FA)**: Media flow–around provides the ability to have a SIP video call whereby signaling passes through Cisco UBE and media pass directly between endpoints bypassing the Cisco UBE.

Figure 2: H.323/SIP IPv4 - SIP IPv6 interworking in media flow-around mode



- **Assisted RTCP (RTCP Keepalive)**: Assisted Real-time Transport Control Protocol (RTCP) enables Cisco UBE to generate RTCP keepalive reports on behalf of endpoints; however, endpoints, such as second generation Cisco IP phones (7940/7960) and Nortel Media Gateways (MG 1000T) do not generate any RTCP keepalive reports. Assisted RTCPs enable customers to use Cisco UBE to interoperate between endpoints and call control agents, such as Microsoft OCS/Lync so that RTCP reports are generated to indicate session liveliness during periods of prolonged silence, such as call hold or call on mute.

  The assisted RTCP feature helps Cisco UBE to generate standard RTCP keepalive reports on behalf of endpoints. RTCP reports determine the liveliness of a media session during prolonged periods of silence, such as a call on hold or a call on mute.

- **SDP Pass–Through**: SDP is configured to pass through transparently at the Cisco UBE, so that both the remote ends can negotiate media independently of the Cisco UBE.

  SDP pass-through is addressed in two modes:

  - Flow-through—Cisco UBE plays no role in the media negotiation, it blindly terminates and re-originates the RTP packets irrespective of the content type negotiated by both the ends. This supports address hiding and NAT traversal.
  - Flow-around—Cisco UBE neither plays a part in media negotiation, nor does it terminate and re-originate media. Media negotiation and media exchange is completely end-to-end.

  For more information, refer to the "Configurable Pass-through of SIP INVITE Parameters" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **UDP Checksum for IPv6**: User Datagram Protocol (UDP) checksums provide data integrity for addressing different functions at the source and destination of the datagram, when a UDP packet originates from an IPv6 node.

- **IP Toll Fraud**:The IP Toll Fraud feature checks the source IP address of the call setup before routing the call. If the source IP address does not match an explicit entry in the configuration as a trusted VoIP source, the call is rejected.

  For more information, refer to the "Configuring Toll Fraud Prevention" section in the Cisco Unified Communications Manager Express System Administrator Guide.

- **RTP Port Range**: Provides the capability where the port range is managed per IP address range. This features solves the problem of limited number of rtp ports for more than 4000 calls. It enables combination of an IP address and a port as a unique identification for each call.
- **Hold/Resume**: Cisco UBE supports supplementary services such as Call Hold and Resume. An active call can be put in held state and later the call can be resumed.

  For more information, refer to the "Configuring Call Hold/Resume for Shared Lines for Analog Ports" section in Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide.

- **Call Transfer (re-INVITE, REFER)**: Call transfer is used for conference calling, where calls can transition smoothly between multiple point-to-point links and IP level multicasting.

  For more information, refer to the "Configurable Pass-through of SIP INVITE Parameters" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **Call Forward (302 based)**: SIP provides a mechanism for forwarding or redirecting incoming calls. A Universal Access Servers (UAS) can redirect an incoming INVITE by responding with a 302 message (moved temporarily).
  - Consumption of 302 at stack level is supported for EO-EO, DO-DO and DO-EO calls for all combination of IPv4/IPv6/ANAT.
  - Consumption of 302 at stack level is supported for both FT and FA calls.

  For more information, refer to the " Configuring Call Transfer and Forwarding" section in Cisco Unified Communications Manager Express System Administrator Guide.

- **Media Antitrombone**: Antitromboning is a media signaling service in SIP entity to overcome the media loops. Media Trombones are media loops in a SIP entity due to call transfer or call forward. Media loops in Cisco UBE are not detected because Cisco UBE looks at both call types as individual calls and not calls related to each other.

  Antitrombone service has to be enabled only when no media interworking is required in both legs. Media antitrombone is supported only when the initial call is in IPv4 to IPv4 or IPv6 to IPv6 mode only.

  For more information, refer to the "Configuring Media Antitrombone" section in the Cisco Unified Border Element Protocol-Independent Features and Setup Configuration Guide.

- **RE-INVITE Consumption**: The Re-INVITE/UPDATE consumption feature helps to avoid interoperability issues by consuming the mid-call Re-INVITEs/UPDATEs from Cisco UBE. As Cisco UBE blocks RE-INVITE / mid-call UPDATE, remote participant is not made aware of the SDP changes, such as Call Hold, Call Resume, and Call transfer.

  For more information, refer to the "Cisco UBE Mid-call Re-INVITE/UPDATE Consumption" section in the Cisco Unified Border Element Protocol-Independent Features and Setup Configuration Guide.

- **Address Hiding**: The address hiding feature ensures that the Cisco UBE is the only point of signaling and media entry/exit in all scenarios. When you configure address-hiding, signaling and media peer addresses are also hidden from the endpoints, especially for supplementary services when the Cisco UBE passes REFER/3xx messages from one leg to the other.

  For more information, refer to the "Configuring Address Hiding" section in the SIP-to-SIP Connections on a Cisco Unified Border Element.

- **Header Passing**: Header Pass through enables header passing for SIP INVITE, SUBSCRIBE and NOTIFY messages; disabling header passing affects only incoming INVITE messages. Enabling header passing results in a slight increase in memory and CPU utilization.

  For more information, refer to the "SIP-to-SIP Connections on a Cisco Unified Border Element" section in the SIP-to-SIPConnections on Cisco Unified Border Element.

- **Refer–To Passing**: The Refer-to Passing feature is enabled when you configure refer-to-passing in Refer Pass through mode and the supplementary service SIP Refer is already configured. This enables the received refer-to header in Refer Pass through mode to move to the outbound leg without any modification. However, when refer-to-passing is configured in Refer Consumption mode without configuring the supplementary-service SIP Refer, the received Refer-to URI is used in the request-URI of the triggered invite.

  For more information, refer to the "Configuring Support for Dynamic REFER Handling on Cisco UBE" section in the Cisco Unified Border Element SIP Configuration Guide.

- **Error Pass-through**: The SIP error message pass through feature allows a received error response from one SIP leg to pass transparently over to another SIP leg. This functionality will pass SIP error responses that are not yet supported on the Cisco UBE or will preserve the Q.850 cause code across two sip call-legs.

  For more information, refer to the "Configuring SIP Error Message Passthrough" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **SIP UPDATE Interworking**: The SIP UPDATE feature allows a client to update parameters of a session (such as, a set of media streams and their codecs) but has no impact on the state of a dialog. UPDATE with SDP will support SDP Pass through, media flow around and media flow through. UPDATE with SDP support for SIP to SIP call flows is supported in the following scenarios:

  - Early Dialog SIP to SIP media changes.
  - Mid Dialog SIP to SIP media changes.

  For more information, refer to the "SIP UPDATE Message per RFC 3311" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **SIP OPTIONS Ping**: The OPTIONS ping mechanism monitors the status of a remote Session Initiation Protocol (SIP) server, proxy or endpoints. Cisco UBE monitors these endpoints periodically.

  For more information, refer to the "Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints" section in the Configuration of SIP Trunking for PSTN Access (SIP-to-SIP) Configuration Guide.

- **Configurable Error Response Code in OPTIONS Ping**: Cisco UBE provides an option to configure the error response code when a dial peer is busied out because of an Out-of-Dialog OPTIONS ping failure.

  For more information, refer to the "Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **SIP Profiles**: SIP profiles create a set of provisioning properties that you can apply to SIP trunk.

- **Dynamic Payload Type Interworking (DTMF and Codec Packets)**: The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature provides dynamic payload type interworking for dual tone multifrequency (DTMF) and codec packets for Session Initiation Protocol (SIP) to SIP calls. The Cisco UBE interworks between different dynamic payload type values across the call legs for the same codec. Also, Cisco UBE supports any payload type value for audio, video,

named signaling events (NSEs), and named telephone events (NTEs) in the dynamic payload type range 96 to 127.

For more information, refer to the "Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls" section in the Cisco Unified Border Element (Enterprise) Protocol-Independent Features and Setup Configuration Guide.

- **Audio Transcoding using Local Transcoding Interface (LTI)**: Local Transcoding Interface (LTI) is an interface created to remove the requirement of SCCP client for Cisco UBE transcoding.

  For information, refer to Cisco Unified Border Element 9.0 Local Transcoding Interface (LTI).

- **Voice Class Codec (VCC) with or without Transcoding**: The Voice Class Codec feature supports basic and all Re-Invite based supplementary services like call-hold/resume, call forward, call transfer, where if any mid-call codec changes, Cisco UBE inserts/removes/modifies the transcoder as needed.

  Support for negotiation of an Audio Codec on each leg of a SIP–SIP call on the Cisco UBE feature supports negotiation of an audio codec using the Voice Class Codec (VCC) infrastructure on Cisco UBE.

  VCC supports SIP-SIP calls on Cisco UBE and allows mid-call codec change for supplementary services.

SIP Voice Gateways in VoIPv6

Session Initiation Protocol (SIP) is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints.

In addition to the already existing features that are supported on IPv4 and IPv6, the SIP Voice Gateways support the following features:

- **History–Info**: The SIP History–info Header Support feature provides support for the history-info header in SIP INVITE messages only. The SIP gateway generates history information in the INVITE message for all forwarded and transferred calls. The history-info header records the call or dialog history. The receiving application uses the history-info header information to determine how and why the call has reached it.

  For more information, refer to the "SIP History INFO" section in the Cisco Unified Border Element (Enterprise) SIP Support Configuration Guide.

- **Handling 181/183 Responses with/without SDP**: The Handling 181/183 Responses with/without SDP feature provides support for SIP 181 (Call is Being Forwarded) and SIP 183 (Session Progress) messages either globally or on a specific dial-peer. Also, you can control when the specified SIP message is dropped based on either the absence or presence of SDP information.

  For more information, refer to "SIP–Enhanced 180 Provisional Response Handling" section in the Cisco Unified Border Element Configuration Guide.

- **Limiting the Rate of Incoming SIP Calls per Dial-Peer (Call Spike)**: The call rate-limiting feature for incoming SIP calls starts working after a switch over in a SIP call. The rate–limiting is done for new calls received on the new Active. The IOS timers that track the call rate limits runs on active and standby mode and does not require any checkpoint. However, some statistics for calls rejected requires to be checked for the show commands to be consistent before and after the switchover.

- **PPI/PAI/Privacy and RPID Passing**: For incoming SIP requests or response messages, when the PAI or PPI privacy header is set, the SIP gateway builds the PAI or PPI header into the common SIP stack, thereby providing support to handle the call data present in the PAI or PPI header. For outgoing SIP

requests or response messages, when the PAI or PPI privacy header is set, privacy information is sent using the PAI or PPI header.

For more information, refer to the "Support for PAID PPID Privacy PCPID and PAURI Headers on Cisco UBE" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **SIP VMWI for FXS phones**: SIP provides visible message waiting indication (VMWI) on FXS phones. This feature provides users with the option to enable one message waiting indication (MWI): audible, visible, or both. The VMWI mechanism uses SIP Subscribe or Notify to get MWI updates from a virtual machine (VM) system, and then forwards updates to the FXS phone on the port.

  For more information, refer to the "Configuring SIP MWI Features" section in the SIP Configuration Guide.

- **SIP Session timer (RFC 4028)**: This feature allows for a periodic refresh of SIP sessions through a re-INVITE or UPDATE request. The refresh allows both user agents and proxies to determine whether the SIP session is still active. Two header fields can be defined: Session-Expires, which conveys the lifetime of the session, and Min-SE, which conveys the minimum allowed value for the session timer.

  For more information, refer to the "SIP Session Timer Support" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **SIP Media Inactivity Detection**: The SIP Media Inactivity Detection Timer feature enables Cisco gateways to monitor and disconnect VoIP calls if no Real-Time Control Protocol (RTCP) packets are received within a configurable time period.

  For more information, refer to the SIP Media Inactivity Timer section.

The SIP Voice Gateways feature is supported for analog endpoints that are connected to Foreign Exchange Station (FXS) ports or a Cisco VG224 Analog Phone Gateway and controlled by a Cisco call-control system, such as a Cisco Unified Communications Manager (Cisco Unified CM) or a Cisco Unified Communications Manager Express (Cisco Unified CME).

For more information on SIP Gateway features and information about configuring the SIP voice gateway for VoIPv6, see the Configuring VoIP for IPv6.

SIP Voice Gateways in VoIPv6

SIP is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints.

For further information about this feature and information about configuring the SIP voice gateway for VoIPv6, see the Configuring VoIP for IPv6, on page 9.

How to Configure VoIP for IPv6

Configuring VoIP for IPv6

SIP is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints.

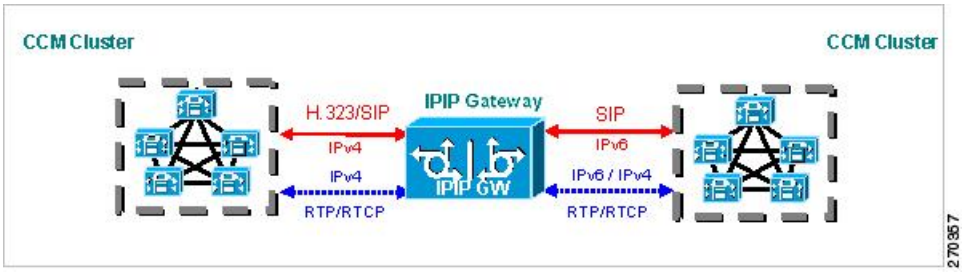
Users in a SIP network are identified by unique SIP addresses. A SIP address is similar to an e-mail address and is in the format of sip:userID@gateway.com. The user ID can be either a username or an E.164 address. The gateway can be either a domain (with or without a hostname) or a specific Internet IPv4 or IPv6 address.

A SIP trunk can operate in one of three modes: SIP trunk in IPv4-only mode, SIP trunk in IPv6-only mode, and SIP trunk in dual-stack mode, which supports both IPv4 and IPv6.

A SIP trunk uses the Alternative Network Address Transport (ANAT) mechanism to exchange multiple IPv4 and IPv6 media addresses for the endpoints in a session. ANAT is automatically enabled on SIP trunks in dual-stack mode. The ANAT Session Description Protocol (SDP) grouping framework allows user agents (UAs) to include both IPv4 and IPv6 addresses in their SDP session descriptions. The UA is then able to use any of its media addresses to establish a media session with a remote UA.

A Cisco Unified Border Element can interoperate between H.323/SIP IPv4 and SIP IPv6 networks in media flow-through mode. In media flow-through mode, both signaling and media flows through the Cisco Unified Border Element, and the Cisco Unified Border Element performs both signaling and media interoperation between H.323/SIP IPv4 and SIP IPv6 networks (see the figure below).

Figure 3: H.323/SIP IPv4--SIP IPv6 Interoperating in Media Flow-Through Mode



Shutting Down or Enabling VoIPv6 Service on Cisco Gateways

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **shutdown** [**forced**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
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 VoIP configuration mode.
Step 4	**shutdown** [**forced**] **Example:** `Device(config-voi-serv)# shutdown forced`	Shuts down or enables VoIP call services.

Shutting Down or Enabling VoIPv6 Submodes on Cisco Gateways

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **call service stop** [**forced**]

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.

	Command or Action	Purpose
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**call service stop** [**forced**] **Example:** `Device(config-serv-sip)# call service stop`	Shuts down or enables VoIPv6 for the selected submode.

Configuring the Protocol Mode of the SIP Stack

Before You Begin

SIP service should be shut down before configuring the protocol mode. After configuring the protocol mode as IPv6, IPv4, or dual-stack, SIP service should be reenabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **protocol mode ipv4** | **ipv6** | **dual-stack** [**preference** {**ipv4** | **ipv6**}]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters SIP user agent configuration mode.
Step 4	**protocol mode ipv4 | ipv6 | dual-stack [preference {ipv4 | ipv6}]}** **Example:** `Device(config-sip-ua)# protocol mode dual-stack`	Configures the Cisco IOS SIP stack in dual-stack mode.

Example: Configuring the SIP Trunk

This example shows how to configure the SIP trunk to use dual-stack mode, with IPv6 as the preferred mode. The SIP service must be shut down before any changes are made to protocol mode configuration.

```
Device(config)# sip-ua
Device(config-sip-ua)# protocol mode dual-stack preference ipv6
```

Disabling ANAT Mode

ANAT is automatically enabled on SIP trunks in dual-stack mode. Perform this task to disable ANAT in order to use a single-stack mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **no anat**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• 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 VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**no anat** **Example:** `Device(conf-serv-sip)# no anat`	Disables ANAT on a SIP trunk.

Configuring the Source IPv6 Address of Signaling and Media Packets

Users can configure the source IPv4 or IPv6 address of signaling and media packets to a specific interface's IPv4 or IPv6 address. Thus, the address that goes out on the packet is bound to the IPv4 or IPv6 address of the interface specified with the **bind** command.

The **bind** command also can be configured with one IPv6 address to force the gateway to use the configured address when the bind interface has multiple IPv6 addresses. The bind interface should have both IPv4 and IPv6 addresses to send out ANAT.

When you do not specify a bind address or if the interface is down, the IP layer still provides the best local address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **bind** {**control** | **media** | **all**} **source interface** *interface-id* [**ipv6-address** *ipv6-address*]

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 VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**bind** {**control** | **media** | **all**} **source interface** *interface-id* [**ipv6-address** *ipv6-address*] **Example:** `Device(config-serv-sip)# bind control source-interface FastEthernet 0/0`	Binds the source address for signaling and media packets to the IPv6 address of a specific interface.

Example: Configuring the Source IPv6 Address of Signaling and Media Packets

```
Device(config)# voice service voip
Device(config-voi-serv)# sip
Device(config-serv-sip)# bind control source-interface fastEthernet 0/0
```

Configuring the SIP Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. sip-server {**dns:** *host-name*] | **ipv4:** *ipv4–address* | **ipv6:** [**ipv6-address**] **:**[*port-nums*]}
5. **keepalive target** {{**ipv4 :** *address* | **ipv6 :** *address*}[**:** *port*] | **dns :** *hostname*} [**tcp** [**tls**]] | **udp**] [**secondary**]

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	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters SIP user agent configuration mode.
Step 4	sip-server {**dns:** *host-name*] | **ipv4:** *ipv4–address* | **ipv6:** [**ipv6-address**] **:**[*port-nums*]} **Example:** `Device(config-sip-ua)# sip-server ipv6: 2001:DB8:0:0:8:800:200C:417A`	Configures a network address for the SIP server interface.
Step 5	**keepalive target** {{**ipv4 :** *address* | **ipv6 :** *address*}[**:** *port*] | **dns :** *hostname*} [**tcp** [**tls**]] | **udp**] [**secondary**] **Example:** `Device(config-sip-ua)# keepalive target ipv6: 2001:DB8:0:0:8:800:200C:417A`	Identifies SIP servers that will receive keepalive packets from the SIP gateway.

Example: Configuring the SIP Server

```
Device(config)# sip-ua
Device(config-sip-ua)# sip-server ipv6: 2001:DB8:0:0:8:800:200C:417A
```

Configuring the Session Target

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* {**mmoip** | **pots** | **vofr** | **voip**}
4. **destination pattern** [+ *string* **T**
5. **session target** {**ipv4:** *destination-address*| **ipv6: [** *destination-address* **]**| **dns : s.** | **d.** | **e.** | **u.**] *host-name* | **enum:***table -num* | **loopback:rtp** | **ras**| **sip-server**} [**:** *port*

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	**dial-peer voice** *tag* {**mmoip** | **pots** | **vofr** | **voip**} **Example:** `Device(config)# dial-peer voice 29 voip`	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.
Step 4	**destination pattern** [+ *string* **T** **Example:** `Device(config-dial-peer)# destination-pattern 7777`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.
Step 5	**session target** {**ipv4:** *destination-address*| **ipv6: [** *destination-address* **]**| **dns : s.** | **d.** | **e.** | **u.**] *host-name* | **enum:***table -num* | **loopback:rtp** | **ras**| **sip-server**} [**:** *port*	Designates a network-specific address to receive calls from a VoIP or VoIPv6 dial peer.

	Command or Action	Purpose
	Example: `Device(config-dial-peer)# session target ipv6:2001:DB8:0:0:8:800:200C:417A`	

Example: Configuring the Session Target

```
Device(config)# dial-peer voice 29 voip
Device(config-dial-peer)# destination-pattern 7777
Device(config-dial-peer)# session target ipv6:2001:DB8:0:0:8:800:200C:417A
```

Configuring SIP Register Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **registrar** {**dns:** *address* | **ipv4:** *destination-address* [**:** *port*] | **ipv6:** *destination-address* **:** *port*] } **aor-domain expires** *seconds* [**tcp tls**]] **type** [**secondary**] [**scheme** *string*]
5. **retry register** *retries*
6. **timers register** *milliseconds*

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	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters SIP user agent configuration mode.

	Command or Action	Purpose
Step 4	**registrar** {**dns:** *address* | **ipv4:** *destination-address* [**:** *port*] | **ipv6:** *destination-address* **:** *port*] } **aor-domain expires** *seconds* [**tcp tls**]] **type** [**secondary**] [**scheme** *string*] **Example:** `Device(config-sip-ua)# registrar ipv6: 2001:DB8::1:20F:F7FF:FE0B:2972 expires 3600 secondary`	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports, IP phone virtual voice ports, and SCCP phones with an external SIP proxy or SIP registrar.
Step 5	**retry register** *retries* **Example:** `Device(config-sip-ua)# retry register 10`	Configures the total number of SIP register messages that the gateway should send.
Step 6	**timers register** *milliseconds* **Example:** `Device(config-sip-ua)# timers register 500`	Configures how long the SIP UA waits before sending register requests.

Example: Configuring SIP Register Support

```
Device(config)# sip-ua
Device(config-sip-ua)# registrar ipv6: 2001:DB8:0:0:8:800:200C:417A expires 3600 secondary
Device(config-sip-ua)# retry register 10
Device((config-sip-ua)# timers register 500
```

Configuring Outbound Proxy Server Globally on a SIP Gateway

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **outbound-proxy** {**ipv4:** *ipv4-address* | **ipv6:** *ipv6-address* | **dns:** *host* **:** *domain*} [**:** *port-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• 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 VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters sip configuration mode.
Step 5	**outbound-proxy** {**ipv4:** *ipv4-address* | **ipv6:** *ipv6-address* | **dns:** *host* **:** *domain*} [**:** *port-number*] **Example:** `Device(config-serv-sip)#outbound-proxy ipv6: 2001:DB8:0:0:8:800:200C:417A`	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway using an IPv6 address.

Verifying SIP Gateway Status

Before You Begin

To verify the status of SIP Gateway, use the following commands

SUMMARY STEPS

1. **show sip-ua calls**
2. **show sip-ua connections**
3. **show sip-ua status**

DETAILED STEPS

Step 1 **show sip-ua calls**

The **show sip-ua calls** command displays active user agent client (UAC) and user agent server (UAS) information on SIP calls:

```
Device# show sip-ua calls
SIP UAC CALL INFO
 Call 1
 SIP Call ID : 8368ED08-1C2A11DD-80078908-BA2972D0@2001::21B:D4FF:FED7:B000
  State of the call       : STATE_ACTIVE (7)
  Substate of the call    : SUBSTATE_NONE (0)
  Calling Number          : 2000
  Called Number           : 1000
  Bit Flags               : 0xC04018 0x100 0x0
CC Call ID              : 2
   Source IP Address (Sig ): 2001:DB8:0:ABCD::1
   Destn SIP Req Addr:Port : 2001:DB8:0:0:FFFF:5060
   Destn SIP Resp Addr:Port: 2001:DB8:0:1:FFFF:5060
   Destination Name        : 2001::21B:D5FF:FE1D:6C00
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 2
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1709707780
     Negotiated Codec         :  (20 bytes)
     Codec Payload Type       : 18
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     Media Source IP Addr:Port: [2001::21B:D4FF:FED7:B000]:16504
     Media Dest IP Addr:Port  : [2001::21B:D5FF:FE1D:6C00]:19548
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1
SIP UAS CALL INFO
   Number of SIP User Agent Server(UAS) calls: 0
```

Step 2 **show sip-ua connections**

Use the **show sip-ua connections** command to display SIP UA transport connection tables:

Example:

```
Device# show sip-ua connections udp brief
Total active connections      : 1
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Router# show sip-ua connections udp detail

Total active connections      : 1
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
---------Printing Detailed Connection Report---------
Note:
```

```
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition
Remote-Agent:2001::21B:D5FF:FE1D:6C00, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size
  =========== ======= =========== ===========
        5060       2 Established           0
```

Step 3 **show sip-ua status**

Use the **show sip-ua status** command to display the status of the SIP UA:

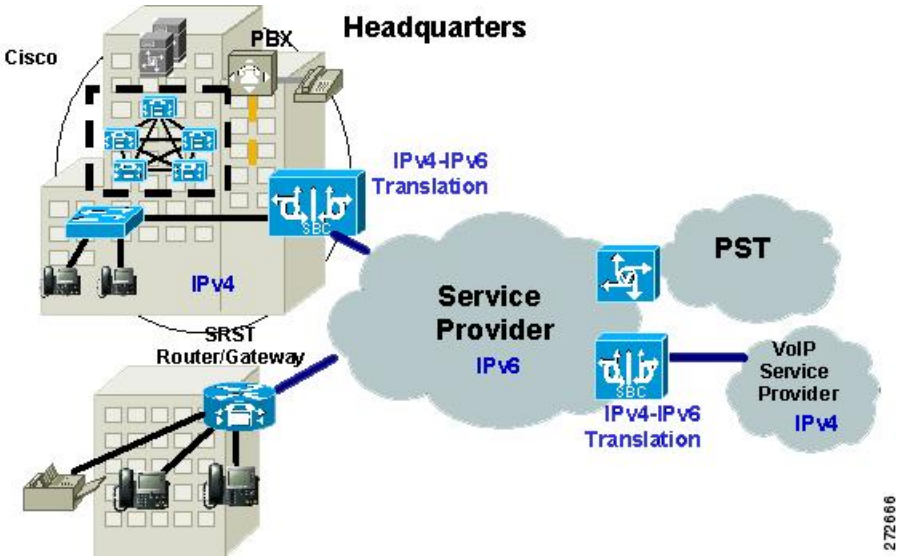
Example:

```
Device# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv6
SDP application configuration:
 Version line (v=) required
 Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

Configuring H.323 IPv4-to-SIPv6 Connections in a Cisco UBE

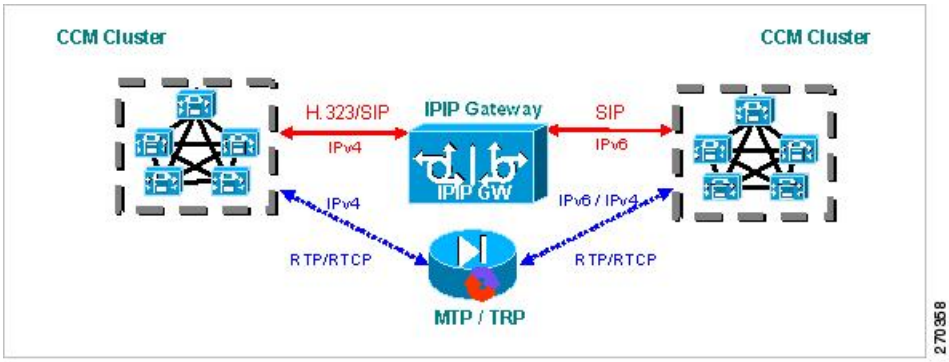
An organization with an IPv4 network can deploy a Cisco UBE on the boundary to connect with the service provider's IPv6 network (see the figure below).

Figure 4: Cisco UBE Interoperating IPv4 Networks with IPv6 Service Provider



A Cisco UBE can interoperate between H.323/SIP IPv4 and SIP IPv6 networks in media flow-through mode. In media flow-through mode, both signaling and media flows through the Cisco UBE, and the Cisco UBE performs both signaling and media interoperation between H.323/SIP IPv4 and SIP IPv6 networks (see the figure below).

Figure 5: IPv4 to IPv6 Media Interoperating Through Cisco IOS MTP



The Cisco UBE feature adds IPv6 capability to existing VoIP features. This feature adds dual-stack support on voice gateways and MTP, IPv6 support for SIP trunks, and SCCP-controlled analog voice gateways. In addition, the SBC functionality of connecting SIP IPv4 or H.323 IPv4 network to a SIP IPv6 network is implemented on an Cisco UBE to facilitate migration from VoIPv4 to VoIPv6.

Before You Begin

Cisco UBE must be configured in IPv6-only or dual-stack mode to support IPv6 calls.

Note A Cisco UBE interoperates between H.323/SIP IPv4 and SIP IPv6 networks only in media flow-through mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections** *from type* **to** *to type*

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 VoIP configuration mode.
Step 4	**allow-connections** *from type* **to** *to type* **Example:** `Device(config-voi-serv)# allow-connections h323 to sip`	Allows connections between specific types of endpoints in a VoIPv6 network. Arguments are as follows: • *from-type* --Type of connection. Valid values: **h323**, **sip**. • *to-type* --Type of connection. Valid values: **h323**, **sip**.

Example: Configuring H.323 IPv4-to-SIPv6 Connections in a Cisco UBE

```
Device(config)# voice service voip
Device(config-voi-serv)# allow-connections h323 to sip
```

Troubleshooting Tips for VoIP for IPv6

Media Flow-Through

To enable all Session Initiation Protocol (SIP)-related debugging, use the **debug ccsip all** command in privileged EXEC mode.

To trace the execution path through the call control application programming interface (CCAPI), use the **debug voip ccapi inout** command.

Media Flow-Around

To enable all Session Initiation Protocol (SIP)-related debugging, use the **debug ccsip all** command.

To trace the execution path through the call control application programming interface (CCAPI), use the **debug voip ccapi inout** command.

SDP Pass-Through

To enable all Session Initiation Protocol (SIP)-related debugging (when the call is active in Pass through mode), use the **debug ccsip all** command.

RTP Port Range

To enable all Session Initiation Protocol (SIP)-related debugging, use the **debug ccsip all** command.

To enable debugging for Real-Time Transport Protocol (RTP) named event packets, use the **debug voip rtp** command.

VMWI SIP

To collect debug information only for signaling events, use the **debug vpm signal** command.

To show all Session Initiation Protocol (SIP) Service Provider Interface (SPI) message tracing, use the **debug ccsip messages** command.

Verifying Cisco UBE ANAT Call Flows

To verify that media settings are enabled in the media flowthrough and media flow-around feature, use the following commands:

SUMMARY STEPS

1. **show call active voice brief**
2. **show call active voice compact**
3. **show voip rtp connections**

DETAILED STEPS

Step 1 **show call active voice brief**

Example:

```
Device# show call active voice brief

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> media:<packets
violation> audio tos:<audio tos value> video tos:<video tos value>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
 LostPacketRate:<%> OutOfOrderRate:<%>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
         speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
0    : 987 361904110ms.1 (16:01:10.557 IST Tue May 14 2013) +530 pid:1 Answer 1005 connected
 dur 00:00:56 tx:1082/173120 rx:1141/182560 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 2001:1111:2222:3333:4444:5555:6666:1012:38356 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms
 g711ulaw TextRelay: off Transcoded: No
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00

0    : 988 361904120ms.1 (16:01:10.567 IST Tue May 14 2013) +510 pid:2 Originate 2005 connected
 dur 00:00:56 tx:1141/182560 rx:1082/173120 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 2001:1111:2222:3333:4444:5555:6666:1012:26827 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms
 g711ulaw TextRelay: off Transcoded: No
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

----------------------------------------------------------------------------
```

Step 2 **show call active voice compact**

Example:

```
Device# show call active voice compact

 <callID>  A/O FAX T<sec> Codec       type        Peer Address       IP R<ip>:<udp>
Total call-legs: 2
       987 ANS     T61    g711ulaw    VOIP        P1005 2001:......:1012:38356
       988 ORG     T61    g711ulaw    VOIP        P2005 2001:......:1012:26827
```

Step 3 **show voip rtp connections**

Example:

```
Device# show voip rtp connections

VoIP RTP Port Usage Information:
Max Ports Available: 24273, Ports Reserved: 303, Ports in Use: 2
Port range not configured, Min: 16384, Max: 32767
                                                  Ports       Ports       Ports
Media-Address Range                               Available   Reserved    In-use

Default Address-Range                             8091        101         0
2001::
2002::                                            8091        101         1
9.0.0.0             10.0.0.0                      8091        101         1
Found 2 active RTP connections
```

Feature Information for VoIP for IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 1: Feature Information for VoIP for IPv6

Feature Name	Releases	Feature Information
IPv6 Dual Stack	Cisco IOS XE Release 3.3S Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.9S	Adds IPv6 capability to existing VoIP features on the Cisco Unified Border Element (Enterprise). Additionally, the SBC functionality of connecting SIP IPv4 or H.323 IPv4 network to SIP IPv6 network is implemented on a Cisco Unified Border Element to facilitate migration from VoIPv4 to VoIPv6. The following commands were introduced or modified: None

Feature Name	Releases	Feature Information
DSCP-Based QoS Support	Cisco IOS XE Release 3.9S	IPv6 supports this feature.
RTP/RTCP over IPv6	Cisco IOS Release XE 3.9S	RTP stack supports the ability to create IPv6 connections using IPv6 unicast and multicast addresses as well as IPV4 connections.