VoIP for IPv6

- Overview, on page 1
- Prerequisites, on page 7
- Restrictions , on page 7
- Configure SIP for IPv6, on page 7

Overview

This document describes VoIP in IPv6, and dual-stack (IPv4 and IPv6) interworking.

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

Feature Information

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for VoIP for IPv6

Feature Name	Releases	Feature Information
CUBE support for IPv6	Baseline Functionality	The feature supports interworking for SIP IPv4-IPv6 dual stack and IPv4 and IPv6.

IPv6 SIP Features

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.

SIP Protocol Handling for VoIPv6

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 incoming calls that are 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 that are 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 CUBE" section in the Cisco Unified Border Element SIP Support 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 convey 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.

VoIPv6 Support

This feature adds dual-stack support IPv6 support for SIP trunks, 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 the Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager
- “RTCP Pass-Through” section in Cube RTCP Voice Pass-Through for IPv6
- “T.38 fax over IPv6” section in Fax, Modem, and Text Support over IP Configuration Guide
- The feature supports for audio calls in media Flow–Through (FT) and Flow–Around (FA) modes, 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 CUBE.

CUBE being a signaling proxy processes all signaling messages for setting up media channels. This enables CUBE 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.
- **Media Flow-Around (FA)**: Media flow–around provides the ability to have a SIP video call whereby signaling passes through CUBE and media pass directly between endpoints bypassing the CUBE.
- **SDP Pass–Through**: SDP is configured to pass through transparently at the CUBE, so that both the remote ends can negotiate media independently of the CUBE.

  SDP pass-through is addressed in two modes:

  - Flow-through—CUBE 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—CUBE 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**: CUBE 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 CUBE are not detected because CUBE 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 CUBE. As CUBE 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 “CUBE 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 CUBE 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 CUBE 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 CUBE” 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 CUBE 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. CUBE monitors these endpoints periodically.

  For more information, refer to the “CUBE 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**: CUBE 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 CUBE interworks between different dynamic payload type values across the call legs for the same codec. Also, CUBE 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 CUBE 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, CUBE inserts/removes/modifies the transcoder as needed.

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

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

- **DNS SRV call routing/ load balancing**: This feature may be used by configuring a dial-peer target with a fully qualified domain name (FQDN) that resolves to a set of DNS SRV records. You can monitor all the SRV hosts that are part of the DNS destination using the OPTIONS Keepalive mechanism. It is therefore possible to load balance calls across all active destinations. For information, refer to SIP Trunk Monitoring.

- **Multi-tenant based in listen-port**: This feature allows to configure specific global configurations for multiple tenants on SIP trunks. Listen ports are configured at the tenant level when there are no active calls on associated dial-peers. For information, refer to Configure Multiple Trunks Using Tenants.

- **High-Availability**: The High Availability (HA) feature allows you to benefit from the failover capability of CUBE on active and standby routers. IPv6 flows in HA is supported. For information, refer to Cisco Unified Border Element High Availability Configuration Guide.

- **SIP Binding**: The SIP Binding feature enables you to configure a source IP address for signaling packets and media packets. For more information, see SIP Bind.

- **Inbound Dial Peer Matching (by URI)**: The inbound dial peer matching by URI feature allows for the configuration of selecting inbound dial peers based on matching specific parts of the URI (Username, IP address, and DNS) received from a remote SIP entity. For more information, see Matching Inbound Dial Peers by URI of Incoming SIP Calls.

- **Server Groups**: This feature configures a server group (group of server addresses) that can be referenced from an outbound dial peer. Server groups allow you to create simpler configurations by specifying a list of destination SIP servers for a single dial peer. For more information, see Configuring Server Groups in Outbound Dial Peers.

- **Monitoring of Phantom Packets**: The Monitoring of Phantom Packets feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer. For more information, see Monitoring of Phantom Packets.

- **Call Admission Control**: The Call Admission Control feature enables you to control the audio quality and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link at the same time. For more information, see Call Admission Control.

Prerequisites

- Enable Cisco Express Forwarding for IPv6.
- IPv6 calls does not support virtual routing and forwarding (VRF).

Restrictions

The following are the restrictions for CUBE features:

- Media Anti–Trombone feature doesn't support for IPv4-IPv6 interworking cases.
- SIPREC IPv6-to-IPv6 or IPv6-to-IPv4 call recording is not supported, if the recording server is configured on the IPv6 call leg.
- WebSocket forking, multi-VRF, RTCP report generation, NAT traversal using media keepalive, Interactive Connectivity Establishment (ICE) over IPv6 are not supported.

Configure SIP for IPv6

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.

Configure 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.
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
```

RTCP Pass-Through

IPv4 and IPv6 addresses embedded within RTCP packets (for example, RTCP CNAME) are passed on toCUBE without being masked. These addresses are masked on the CUBE ASR 1000.

The CUBE ASR 1000 does not support printing of RTCP debugs.

Note RTCP is passed through by default. No configuration is required for RTCP pass-through.

Configure IPv6

In CUBE, IPv4-only and IPv6-only modes are not supported when endpoints are dual-stack. In this case, CUBE must also be configured in dual-stack mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **protocol mode** {**ipv4** | **ipv6** | **dual-stack** {**preference** {**ipv4** | **ipv6**}}
5. **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	**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 ipv6`
		Configures the Cisco IOS SIP stack.
		• **protocol mode dual-stack preference** {**ipv4** | **ipv6**} —Sets the IP preference when the ANAT command is configured.
		• **protocol mode** {**ipv4** | **ipv6**} —Passes the IPv4 or IPv6 address in the SIP invite.
		• **protocol mode dual-stack**} —Passes both the IPv4 addresses and the IPv6 addresses in the SIP invite and sets priority based on the far-end IP address.

Step 5	**end**
	Example:
	`Device(conf-voi-serv)# end`
		Exits SIP user-agent configuration mode.

Configure 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
```

Configure 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* **Example:** `Device(config-dial-peer)# session target ipv6:2001:DB8:0:0:8:800:200C:417A`	Designates a network-specific address to receive calls from a VoIP or VoIPv6 dial peer.

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
```

Configure 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.
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.

	Command or Action	Purpose
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
```

Configure IP Toll Fraud

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **ip address trusted list**
5. **ipv6** *X:X:X:X::X*
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 voice service VoIP configuration mode.

	Command or Action	Purpose
Step 4	**ip address trusted list** **Example:** `Device(config-voi-serv)# ip address trusted list`	Enters IP address trusted list configuration mode. You can add unique and multiple IP addresses for incoming VoIP (SIP) calls to a list of trusted IP addresses.
Step 5	**ipv6** *X:X:X:X::X* **Example:** `Device(cfg-iptrust-list)# ipv6 2001:DB8::/48`	Enters IPv6 addresses for toll fraud prevention.

Step 6	**end**
	Example:
	`Device(cfg-iptrust-list)# end`
		Exits trusted list configuration mode and returns to global configuration mode.