Cisco Unified Border Element (Enterprise) Fundamentals and Basic Setup Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 1000)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Cisco Unified Border Element Enterprise Fundamentals and Basic Setup

This Cisco Unified Border Element (Enterprise) is a special Cisco IOS XE software image that runs on Cisco ASR1000. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking. This chapter describes basic gateway functionality, software images, topology, and summarizes supported features.

Cisco Product Authorization Key (PAK)--A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license .

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 at the end of this module.

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 Cisco Unified Border Element Enterprise

Cisco Unified Border Element (Enterprise) Hardware

- Install the routers that will serve as session border controllers in your VoIP network.

Cisco Unified Border Element (Enterprise) Software

- Obtain the appropriate feature license for each router on which you will install an image that supports the Unified Border Element feature. Additional information on obtaining a feature license can be found at: http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_data_sheet09186a00801da698.html

- Cisco Product Authorization Key (PAK)--A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license .
- Install the appropriate Cisco IOS XE image on each router and configure a working VoIP network.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Restrictions for Cisco Unified Border Element Enterprise

- Cisco Unified Border Elements that require the Registration, Admission, and Status (RAS) protocol must have a via-zone-enabled gatekeeper or equivalent.
- Cisco fax relay is reported as a voice call on an Cisco Unified Border Element. Fax relay is enabled by default for all systems. No further configuration is needed.
- Cisco Unified Border Element supports T.38 fax relay (H.323 Annex D). However, endpoints configured with Named Signaling Events (NSE) may result in reduced fax transmission quality and are not supported.
- Codec filtering must be based on codec types; filtering based on byte size is not supported.
- When a Tcl script is running on an Cisco Unified Border Element, the Cisco Unified Border Element does not support ringback tone generation.
- Transcoding is not supported.

Information About Cisco Unified Border Element Enterprise

When you configure SIP on a router, the ports on all its interfaces are open by default. This makes the router vulnerable to malicious attackers who can execute toll fraud across the gateway if the router has a public IP address and a public switched telephone network (PSTN) connection. To eliminate the threat, you should bind an interface to private IP address that is not accessible by untrusted hosts. In addition, you should protect any public or untrusted interface by configuring a firewall or an access control list (ACL) to prevent unwanted traffic from traversing the router.A Cisco Unified Border Element (Enterprise) facilitates connectivity between independent VoIP networks by enabling SIP and H.323 VoIP and videoconferencing calls from one IP network to another. This gateway performs most of the same functions of a PSTN-to-IP gateway, but typically joins two IP call legs, rather than a PSTN and an IP call leg. Media packets can flow either through the gateway (thus hiding the networks from each other) or around the border element, if so configured.

Cisco Unified Border Element (Enterprise) is a special Cisco IOS software image that runs on the Cisco AS1000 platform. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

Cisco UBE (Enterprise) is designed to meet the interconnection needs of Internet telephony service providers (ITSPs) and of enterprises. One set of images provides basic interconnection and a second set provides interconnection through an Open Settlement Protocol (OSP) provider, enabling ITSPs to gain the benefits of the Cisco Unified Border Element while making use of the routing, billing, and settlement capabilities offered by OSP-based clearinghouses.

Feature benefits include the following:

- Capacity control and improved call routing control using carrier-based routing with the Cisco Unified Border Element feature and routing traffic through the gateways.
- Improved billing and settlement capabilities.
- Provides key services at the edge of the network for scalability.

To configure any Cisco UBE (Enterprise) Feature, you should understand the following concepts:

- Gateway Functionality, page 3
- Cisco Unified Border Element Network Topology, page 3

Gateway Functionality

Gateways are responsible for the following tasks.

- Media stream handling and speech path integrity
- DTMF relay
- Fax relay and passthrough
- Digit translation and call processing
- Dial peers and codec filtering
- Carrier ID handling
- Gateway-based billing
- Termination and re-origination of signaling and media

Cisco Unified Border Element Network Topology

In the current VoIP market, ITSPs who provide wholesale VoIP services use their own IP-to-TDM gateways to exchange calls with the PSTN. Problems occur when a wholesaler receives a call from an originating ITSP and decides to terminate the call to another ITSP. Because it does not own the PSTN gateways, the wholesaler does not receive call setup or release information and therefore cannot bill for the call. Wholesalers are forced either to forbid these connections, thereby foregoing a potential revenue source, or to set up the call through a combination of back-to-back IP-to-TDM gateways. This solution results in reduced quality due to double media coding and decoding, and it wastes TDM port resources.

Cisco Unified Border Element allows the wholesaler to terminate the call from the originating ITSP and then reoriginate it, thereby providing a point at which accurate call detail records (CDRs) can be collected for billing.

The superior interconnect capability provided by the Cisco Unified Border Element enables service providers to conceal their internal network and business relationships while improving call admission control, flexible routing, and protocol interworking capabilities.

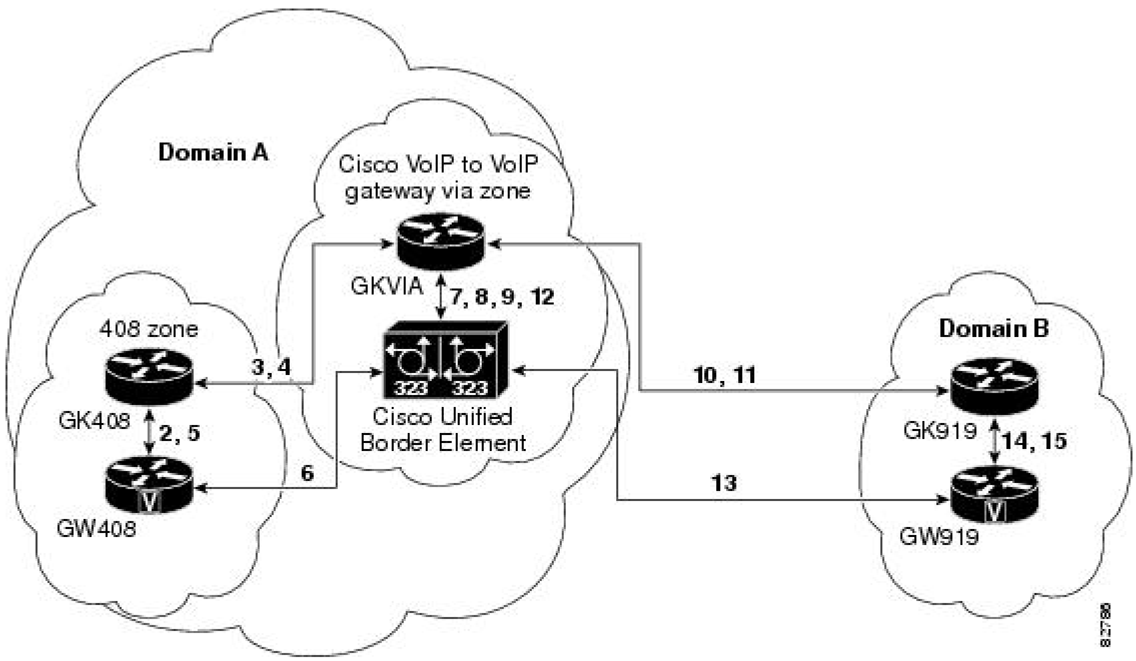
The Cisco Unified Border Element includes the following changes to gateways and gatekeepers to allow Cisco UBE call legs:

- Support for H.323-to-H.323, H.323-to-SIP, and SIP-to-SIP connection types
- Support for transparent codec on H.323-to-H.323 connection types
- Support for H.323 call capacities
- Introduction of gatekeeper via-zones. *Via-zone* is a Cisco term for a zone that contains Cisco Unified Border Elements and via-zone-enabled gatekeepers. A via-zone-enabled gatekeeper is capable of recognizing via-zones and sending traffic to via-zone gateways. Cisco via-zone-enabled gatekeepers include a via-zone command-line interface (CLI) command.

Via-zones are usually located on the edge of an ITSP network and are like a VoIP transfer point, or tandem zone, where traffic passes through on the way to the remote zone destination. Gateways in this zone terminate requested calls and reoriginate traffic to its final destination. Via-zone gatekeepers operate as usual for applications that are not Cisco UBE gatekeepers in via-zones support resource management (for example, gateway selection and load balancing) using the Capacities field in the H.323 Version 4 RAS messages.

The figure below shows a simple topology example of the Cisco Unified Border Element using via-zone gatekeepers.

Figure 1 *Cisco Unified Border Element Feature Sample Topology*



The gatekeeper in Domain A and the gatekeeper in Domain B are connected to the via-zone gatekeeper. GK408 and the via-zone gatekeeper exchange Registration, Admission, and Status (RAS) messages for the originating side. Then the connection is made between the originating gateway and the Cisco Unified Border Element. The via-zone gatekeeper exchanges RAS messages with GK919 for the terminating side. If the call is accepted, the Cisco Unified Border Element completes the connection from GW408 to GW919, and the media flows through the Cisco Unified Border Element.

In a basic call scenario, on receiving a location request (LRQ) message from the originating gatekeeper (GK408), the via-zone-enabled gatekeeper (GKVIA) processes the message and determines that the call should be set up using the Cisco Unified Border Element. After the originating gateway receives its admission confirmation (ACF) message, it sets up the call.

With the Cisco Unified Border Element feature, instead of the originating gateway signaling the terminating gateway directly, the Cisco Unified Border Element controls the call set-up both the signaling and media channel. The Cisco Unified Border Element is terminating the signaling and media channels, but the information associated with the media is propagated through to the opposite call leg. This process allows the endpoints to determine what media channel capabilities to use for the call. When the call is established, the audio stream flows through the Cisco Unified Border Element, meaning that the gateway terminates the audio channel on one call leg and then reorginates it to the other leg.

The following scenario illustrates a basic call from the originating gateway to the terminating gateway, using the Cisco Unified Border Element and gatekeepers.

1. GW408 (the originating gateway) calls someone in the 919 area code, which is serviced by GW919 (the terminating gateway).
2. GW408 sends an ARQ with the called number having the 919 area code to a gatekeeper in its zone (GK408).
3. GK408 resolves 919 to belong to a via-zone gatekeeper (GKVIA). GK408 then sends an LRQ to GKVIA.
4. GKVIA receives the LRQ for the 919 number. GKVIA resolves the 919 prefix to belong to the Cisco Unified Border Element. GKVIA is configured to route requests for 919 prefix calls through its Cisco Unified Border Element. GKVIA sends an LCF to GK408.
5. GK408 returns an ACF specifying Cisco Unified Border Element to GW408.
6. GW408 sends a SETUP message to Cisco Unified Border Element for the 919 number.
7. Cisco Unified Border Element consults GKVIA with an ARQ message with the answerCall=true parameter to admit the incoming call.
8. GKVIA responds with an ACF to admit the call. From the perspective of the gatekeeper, the first call leg has been established.
9. Cisco Unified Border Element has a dial peer specifying that RAS messages should be sent to GKVIA for all prefixes. Cisco Unified Border Element initiates the resending of the call by sending the ARQ message with the **answerCall** parameter set to, false to GKVIA for 919.
10. GKVIA knows that prefix 919 belongs to GK919, and since the source zone is the via-zone, the GKVIA sends an LRQ to GK919.
11. GK919 sees prefix 919 as a local zone and sends an LCF pointing to GW919.
12. GKVIA returns an ACF specifying GW919.
13. Cisco Unified Border Element sends a SETUP message to GW919 for the 919 call.
14. GW919 sends an ARQ to GK919 to request admission for the call.
15. GK919 sends an ACF with the answerCall=true parameter.

All other messages (for example, Proceeding, Alerting, and Connect) are created as two legs between GW408, and GW919, with the Cisco Unified Border Element acting as an intermediate gateway.

Basic SIP-to-SIP Set-up and Functionality Features

This chapter contains the following configuration topics:

SIP-to-SIP Set-up

- IP-to-IP Gateway: SIP-SIP Basic Functionality
- Transport Control Protocol (TCP) and User Datagram Protocol (UDP) — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr5/vcr-t3.html#GUID-90074126-D070-4532-8699-CC98C020DA08
- Cisco Unified Border Element and Cisco Unified Communications Manager Express Support for Universal Packaging — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr3/vcr-m3.html#GUID-F7169012-D016-4AE1-9AFA-4BAB1C6B4182

IP Addressing

- SIP—Gateway Support for the bind Command
- Configuring an Inbound Dial-peer to Match the URI on SIP Calls

- Multiple Destination pattern support on Voice Dialpeer
- Configuring Media Flow Through and Flow Around

Basic Dial Plan Management

- Dial Peer Configuration on Voice Gateway Routers - See also the "Dial Peer Configuration on Voice Gateway Routers, Cisco IOS Release 15.1M&T" guide.

Basic Protocol and DTMF Interworking

- Supported Protocol Interworking

Lawful Intercept Support

Lawful Intercept (LI) is the term used to describe the process by which law enforcement agencies conduct electronic surveillance of circuit communications as authorized by judicial or administrative order. Cisco Service Independent Intercept (SII) supports voice and data intercept and intercept requests are initiated by MD using SNMPv3.

IP-to-IP Gateway SIP-to-SIP Basic Functionality

SIP-to-SIP Basic Functionality for Cisco Unified Border Element (Cisco UBE) and Cisco Unified Border Element (Enterprise) (Cisco UBE (Enterprise)) provides termination and reorigination of both signaling and media between VoIP and video networks using SIP signaling in conformance with RFC3261. The SIP-to-SIP protocol interworking capabilities support the following:

- Basic voice calls (Supported audio codecs include: G.711, G.729, G.728, G.726, G.723, G.722, gsmamr nb, AAC_LD, iLBC. Video codecs: H.263, and H.264)
- Calling/called name and number
- DTMF relay interworking
    - SIP RFC 2833 <-> SIP RFC 2833
    - SIP Notify <-> SIP Notify
- Interworking between SIP early-media and SIP early-media signaling
- Interworking between SIP delayed-media and SIP delayed-media signaling
- RADIUS call-accounting records
- RSVP synchronized with call signaling
- SIP-to-SIP Video calls
- TCL IVR 2.0 for SIP, including media playout and digit collection (RFC 2833 DTMF relay)
- T.38 fax relay and Cisco fax relay
- UDP and TCP transport

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 at the end of this module.

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 IP-to-IP Gateway SIP-to-SIP Basic Functionality

Cisco Unified Border Element

- Cisco IOS Release 12.2(13)T3 or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for IP-to-IP Gateway SIP-to-SIP Basic Functionality

- Connections are disabled by default in Cisco IOS images that support the Cisco UBE (Enterprise).

How to Configure SIP-to-SIP Connections in a Cisco Unified Border Element Enterprise

To configure SIP-to-SIP connection types, perform the steps in this section.

SUMMARY STEPS

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

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 VoIP voice-service configuration mode.
Step 4	**allow-connections** *from-type* **to** *to-type* **Example:** `Device(config-voi-serv)# allow-connections sip to sip`	Allows connections between specific types of endpoints in an Cisco UBE. Arguments are as follows: • *from-type* --Type of connection. Valid values: **h323**, **sip**. • *to-type* --Type of connection. Valid values: **h323**, **sip**. **Note** H.323-to-H.323: By default, H.323-to-H.323 connections are disabled and POTS-to-any and any-to-POTS connections are enabled.
Step 5	**exit** **Example:** `Device(config-voi-serv)# exit`	Exits the current mode.

Feature Information for IP-to-IP Gateway SIP-to-SIP Basic Functionality

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 IP-to-IP Gateway: SIP-to-SIP Basic Functionality

Feature Name	Releases	Feature Information
SIP-to-SIP Basic Functionality	12.2(13)T3 12.3(7)T	This feature provides termination and reorigination of both signaling and media between VoIP and video networks using SIP signaling in conformance with RFC3261. In Cisco IOS Release 12.2(13)T3, this feature was implemented on the Cisco Unified Border Element. The following commands were introduced or modified: **allow-connections**
SIP-to-SIP Basic Functionality	Cisco IOS XE Release 2.5	This feature provides termination and reorigination of both signaling and media between VoIP and video networks using SIP signaling in conformance with RFC3261. In Cisco IOS Release 12.2(13)T3, this feature was implemented on the Cisco Unified Border Element (Enterprise). The following commands were introduced or modified: **allow-connections**

SIP-to-SIP Extended Feature Functionality for Session Border Controllers

The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:

- Call Admission Control (based on CPU, memory, and total calls)
- Delayed Media Call
- ENUM support
- Configuring SIP Error Message Pass Through
- Interoperability with Cisco Unified Communications Manager 5.0 and BroadSoft
- Lawful Intercept
- Media Inactivity
- Modem Passthrough over VoIP, page 12
- TCP and UDP interworking
- Tcl scripts with SIP NOTIFY VoiceXML with SIP-to-SIP
- Transport Layer Security (TLS)

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 at the end of this module.

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 SIP-to-SIP Extended Feature Functionality for Session Border Controllers

Cisco Unified Border Element

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Modem Passthrough over VoIP

The Modem Passthrough over VoIP feature provides the transport of modem signals through a packet network by using pulse code modulation (PCM) encoded packets.

Prerequisites for the Modem Passthrough over VoIP Feature

- VoIP enabled network.
- Cisco IOS Release 12.1(3)T must run on the gateways for the Modem Passthrough over VoIP feature to work.
- Network suitability to pass modem traffic. The key attributes are packet loss, delay, and jitter. These characteristics of the network can be determined by using the Cisco IOS feature Service Assurance Agent.

Cisco Unified Border Element

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

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 the Modem Passthrough over VoIP Feature

Cisco Unified Border Element (Enterprise)

- If call started as g729, upon modem tone (2100Hz) detection both the outgoing gateway (OGW) and the trunking gateway (TGW) will genearate NSE packets towards peer side and up speed to g711 as Cisco UBE(Enterprise) passes these packets to the peer side.

Note That OGW and TGW display the new codec, but the Cisco UBE (Enterprise) continues to show the original codec g729 in the show commands.

Information about Configuring Modem Passthrough over VoIP

The Modem Passthrough over VoIP feature performs the following functions:

- Represses processing functions like compression, echo cancellation, high-pass filter, and voice activity detection (VAD).
- Issues redundant packets to protect against random packet drops.
- Provides static jitter buffers of 200 milliseconds to protect against clock skew.
- Discriminates modem signals from voice and fax signals, indicating the detection of the modem signal across the connection, and placing the connection in a state that transports the signal across the network with the least amount of distortion.
- Reliably maintains a modem connection across the packet network for a long duration under *normal* network conditions.

For further details, the functions of the Modem Passthrough over VoIP feature are described in the following sections.

Modem Tone Detection

The gateway is able to detect modems at speeds up to V.90.

Passthrough Switchover

When the gateway detects a data modem, both the originating gateway and the terminating gateway roll over to G.711. The roll over to G.711 disables the high-pass filter, disables echo cancellation, and disables VAD. At the end of the modem call, the voice ports revert to the prior configuration and the digital signal processor (DSP) goes back to the state before switchover. You can configure the codec by selecting the **g711alaw** or **g711ulaw** option of the **codec** command.

See also the How to Configure Modem Passthrough over VoIP, page 14 section in this document.

Controlled Redundancy

You can enable payload redundancy so that the Modem Passthrough over VoIP switchover causes the gateway to emit redundant packets.

Packet Size

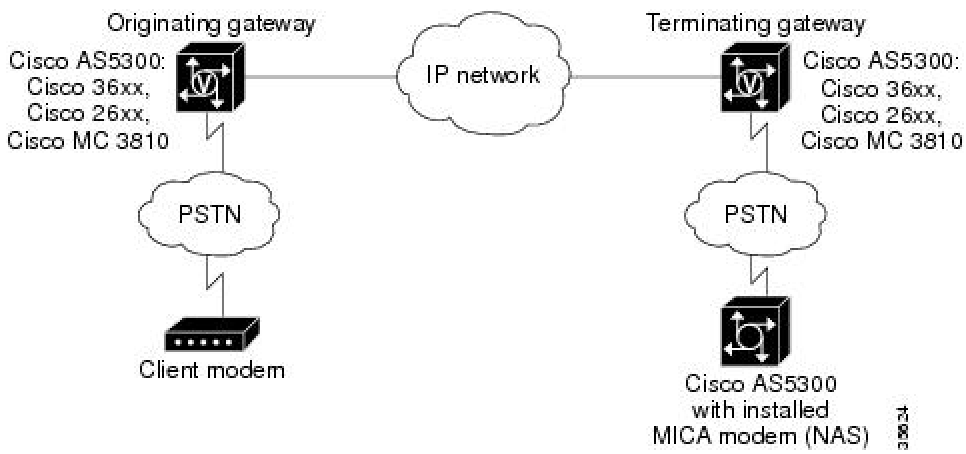
When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

Clock Slip Buffer Management

When the gateway detects a data modem, both the originating gateway and the terminating gateway switch from dynamic jitter buffers to static jitter buffers of 200-ms depth. The switch from dynamic to static is to compensate for Public Switched Telephone Network (PSTN) clocking differences at the originating gateway and the terminating gateway. At the conclusion of the modem call, the voice ports revert to dynamic jitter buffers.

The figure below illustrates the connection from the client modem to a MICA technologies modem network access server (NAS).

Figure 2 Modem Passthrough Connection



How to Configure Modem Passthrough over VoIP

You can configure the Modem Passthrough over VoIP feature on a specific dial peer in two ways, as follows:

- Globally in the voice-service configuration mode
- Individually in the dial-peer configuration mode on a specific dial peer

By default, modem passthrough over VoIP capability and redundancy are disabled.

Tip You need to configure modem passthrough in both the originating gateway and the terminating gateway for the Modem Passthrough over VoIP feature to operate. If you configure only one of the gateways in a pair, the modem call will not connect successfully.

Redundancy can be enabled in one or both of the gateways. When only a single gateway is configured for redundancy, the other gateway receives the packets correctly, but does not produce redundant packets.

See the following sections for the Modem Passthrough over VoIP feature. The two configuration tasks can configure separately or together. If both are configured, the dial-peer configuration takes precedence over the global configuration. Consequently, a call matching a particular dial-peer will first try to apply the modem passthrough configuration on the dial-peer. Then, if a specific dial-peer is not configured, the router will use the global configuration:

- Configuring Modem Passthrough over VoIP Globally, page 15
- Configuring Modem Passthrough over VoIP for a Specific Dial Peer, page 16
- Troubleshooting Tips, page 18

Configuring Modem Passthrough over VoIP Globally

For the Modem Passthrough over VoIP feature to operate, you need to configure modem passthrough in both the originating gateway and the terminating gateway so that the modem call matches a voip dial-peer on the gateway.

The default behavior for the voice-service configuration mode is **no modem passthrough**. This default behavior implies that modem passthrough is disabled for all dial peers on the gateway by default.

When using the **voice service voip** and **modem passthrough nse** commands on a terminating gateway to globally set up fax or modem passthrough with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match.

To configure the Modem Passthrough over VoIP feature for all the connections of a gateway, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **voice service voip**
3. **modem passthrough nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**] [**maximum-sessions** *value*]
4. **exit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice-service configuration mode. Configures voice service for all the connections for the gateways.

	Command or Action	Purpose
Step 3	**modem passthrough nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**] [**maximum-sessions** *value*] **Example:** `Device(config)# Router(conf-voi-serv)# modem passthrough nse payload-type 97 codec g711alaw redundancy maximum-sessions 3`	Configures the Modem Passthrough over VoIP feature The default behavior is **no modem passthrough**. The payload type is an optional parameter for the **nse** keyword. Use the same **payload-type** *number* for both the originating gateway and the terminating gateway. The **payload-type** *number*can be set from 96 to 119. If you do not specify the **payload-type** *number*, the *number*defaults to 100. When the **payload-type** is 100, and you use the **show running-config**command, the **payload-type** parameter does not appear. Use the same codec type for both the originating gateway and the terminating gateway. **g711ulaw** codec is required for T1, and **g711alaw** codec is required for E1. The **redundancy** keyword is an optional parameter for sending redundant packets for modem traffic. The **maximum-sessions** keyword is an optional parameter for the **redundancy**keyword. This parameter determines the maximum simultaneous modem passthrough sessions with **redundancy**.
Step 4	**exit** **Example:** `Device(conf-voi-serv)# exit`	Exits voice-service configuration mode.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuring Modem Passthrough over VoIP for a Specific Dial Peer

To enable Modem Passthrough on the VoIP dial peers on both the originating and terminating gateway, configure modem passthrough globally or explicitly on the dial peer.

For modem passthrough to operate, you must define VoIP dial peers on both gateways to match the call, for example, by using a destination pattern or an incoming called number. The modem passthrough parameters associated with those dial peers then will apply to the call.

Note When modem passthrough is configured individually for a specific dial peer, that configuration for the specific dial peer takes precedence over the global configuration.

To configure the Modem Passthrough over VoIP feature for a specific dial peer, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **dial-peer voice** *number* **voip**
3. **modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**]}
4. **exit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**dial-peer voice** *number* **voip** **Example:** `Device(config)# dial-peer voice 5 voip`	Enters dial-peer configuration mode. Configures a specific dial peer in dial-peer configuration mode.
Step 3	**modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**}[**redundancy**]} **Example:** `Device(config-dial-peer)# modem passthrough nse payload-type 97 codec g711alaw redundancy`	Configures the Modem Passthrough over VoIP feature for a specific dial peer. The default behavior for the Modem Passthrough for VoIP feature in dial-peer configuration mode is **modem passthrough system**. As required, the gateway defaults to **no modem passthrough**. When the **system** keyword is enabled, the following parameters are not available: **nse**, **payload-type**, **codec**, and **redundancy**. Instead the values from the global configuration are used. The payload type is an optional parameter for the **nse** keyword. Use the same **payload-type** *number* for both the originating gateway and the terminating gateway. The **payload-type** *number*can be set from 96 to 119. If you do not specify the **payload-type** *number*, the *number*defaults to 100. When the **payload-type** is 100, and you use the **show running-config**command, the **payload-type** parameter does not appear. Use the same codec type for both the originating gateway and the terminating gateway. **g711ulaw** codec is required for T1, and **g711alaw** codec is required for E1. The **redundancy** keyword is an optional parameter for sending redundant packets for modem traffic.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits dial-peer configuration mode and returns to the global configuration mode.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Troubleshooting Tips

To troubleshoot the Modem Passthrough over VoIP feature, perform the following steps:

- Make sure that you can make a voice call.
- Make sure that Modem Passthrough over VoIP is configured on both the originating gateway and the terminating gateway.
- Make sure that both the originating gateway and the terminating gateway have the same named signaling event (NSE) **payload-type** *number*.
- Make sure that both the originating gateway and the terminating gateway have the same **maximum-sessions** *value* when the two gateways are configured in the voice-service configuration mode.
- Use the **debug vtsp dsp** and **debug vtsp session** commands to debug a problem.

Verifying Modem Passthrough over VoIP

To verify that the Modem Passthrough over VoIP feature is enabled, perform the following steps:

SUMMARY STEPS

1. Enter the **show run** command to verify the configuration.
2. Enter the **show dial-peer voice** command to verify that Modem Passthrough over VoIP is enabled.

DETAILED STEPS

Step 1 Enter the **show run** command to verify the configuration.

Step 2 Enter the **show dial-peer voice** command to verify that Modem Passthrough over VoIP is enabled.

Monitoring and Maintaining Modem Passthrough over VoIP

To monitor and maintain the Modem Passthrough over VoIP feature, use the following commands in privileged EXEC mode:

Command	Purpose
Device# **show call active voice brief**	Displays information for the active call table or displays the voice call history table. The brief option displays a truncated version of either option.
Device# **show dial-peer voice 15 summary**	Displays configuration information for dial peers. The *number* argument specifies a specific dial peer from 1 to 32767. The summary option displays a summary of all dial peers.

Configuration Examples

The following is sample configuration for the Modem Passthrough over VoIP feature:

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
voice service voip
     modem passthrough nse codec g711ulaw redundancy maximum-session 5
!
!
resource-pool disable
!
!
!
!
!
ip subnet-zero
ip ftp source-interface Ethernet0
ip ftp username lab
ip ftp password lab
no ip domain-lookup
!
isdn switch-type primary-5ess
cns event-service server
!
!
!
!
!
mta receive maximum-recipients 0
!
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 shutdown
 clock source line secondary 1
!
controller T1 2
 shutdown
!
controller T1 3
 shutdown
!
!
!
interface Ethernet0
 ip address 1.1.2.2 255.0.0.0
```

```
 no ip route-cache
 no ip mroute-cache
!
interface Serial0:23
 no ip address
 encapsulation ppp
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no peer default ip address
 no fair-queue
 no cdp enable
 no ppp lcp fast-start
!
interface FastEthernet0
 ip address 26.0.0.1 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 duplex full
 speed auto
 no cdp enable
!
ip classless
ip route 17.18.0.0 255.255.0.0 1.1.1.1
no ip http server
!
!
!
!
voice-port 0:D
!
dial-peer voice 1 pots
 incoming called-number 55511..
 destination-pattern 020..
 direct-inward-dial
 port 0:D
 prefix 020
!
dial-peer voice 2 voip
 incoming called-number 020..
 destination-pattern 55511..
 modem passthrough nse codec g711ulaw redundancy
 session target ipv4:26.0.0.2
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
!
end
```

Feature Information for SIP-to-SIP Extended Feature Functionality for Session Border Controllers

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 2 Feature Information for Configuring SIP-to-SIP Extended Feature Functionality for Session Border Controllers

Feature Name	Releases	Feature Information
SIP-to-SIP Extended Feature Functionality for Session Border Controllers	12.4(6)T	The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). In Cisco IOS Release 12.4(6)S, this feature was implemented on the Cisco Unified Border Element The following commands were introduced or modified: **modem passthrough (dial-peer)**; **modem passthrough (voice-service)**; **show call active voice voice**; **show call history voice voice**; **show dial-peer voice**; **voice service**.
SIP-to-SIP Extended Feature Functionality for Session Border Controllers	Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.3S	The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). In Cisco IOS Release 12.4(6)S, this feature was implemented on the Cisco Unified Border Element (Enterprise). The following commands were introduced or modified: **modem passthrough (dial-peer)**; **modem passthrough (voice-service)**; **show call active voice voice**; **show call history voice voice**; **show dial-peer voice**; **voice service**.

SIP Gateway Support for the bind Command

The Gateway Support for the bind Command feature introduces the **bind** command, which allows you to configure the source IP address of signaling packets or both signaling and media packets. Befor this feature was introduced the source address of a packet going out of a Cisco IOS gateway is not deterministic. The session protocols and VoIP layers depended on the IP layer to give the best local address and then used the address for the source address in signaling or media or both, even if multiple interfaces can support a route to the destination address.

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 at the end of this module.

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 SIP Gateway Support for the bind Command

- Ensure that the gateway has voice functionality that is configurable for SIP.
- Establish a working IP network.
- Configure VoIP.

Cisco Unified Border Element

- Cisco IOS Release 12.2(8)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information About SIP Gateway Support for the bind Command

Prior to the Gateway Support for the bind Command feature the source address of a packet going out of the gateway was never deterministic. That is, the session protocols and VoIP layers always depended on the IP layer to give the *best local address* . The best local address was then used as the source address (the address showing where the SIP request came from) for signaling and media packets. Using this nondeterministic address occasionally caused confusion for firewall applications, because a firewall could not be configured with an exact address and would take action on several different source address packets.

The **bind** interface command allows you to configure a specific interface's IP address as the source IP address of signaling and media packets. The address that goes out on the packet is bound to the IP address of the interface specified with the **bind** command. Packets that are not destined to the bound address are discarded.

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

With the **bind** command, SIP signaling and media paths can advertise the same source IP address on the gateway for certain applications, even if the paths use different addresses to reach the source. This eliminates confusion for firewall applications that, Without the binding, may have taken action on several different source address packets.

The table below lists the results of the bind command based on the state of the interface.

Table 3 ***Command functions for the bind command based on the state of the interface***

Interface State	Result Using Bind Command
A **bind interface is shut down**, or its **IP Address is changed**, or the **physical cable is pulled** while SIP calls are active	The call becomes a one-way call with media flowing in only one direction. It flows from the gateway where the change or shutdown took place to the gateway where no change occurred. Thus, the gateway with the status change no longer receives media. The call is then disconnected, but the disconnected message is not understood by the gateway with the status change, and the call is still assumed to be active.
No Shutdown— With no active calls.	The TCP and UDP socket listeners are initially closed. (Socket listeners receive datagrams addressed to the socket.) Then the sockets are opened and bound to the IP address set by the **bind** command. The sockets accept packets destined for the bound address only.

Interface State	Result Using Bind Command
No Shutdown— With active calls.	The TCP and UDP socket listeners are initially closed. Then the sockets are opened to listen to any IP address.
Shutdown— With or without active calls.	The TCP and User Datagram Protocol (UDP) socket listeners are initially closed. (Socket listeners receive datagrams addressed to the socket.) Then the sockets are opened to listen to any IP address. If the outgoing gateway has the **bind** command enabled and has an active call, the call becomes a one-way call with media flowing from the outgoing gateway to the terminating gateway.
The Bound interface's IP address is **removed**	The TCP and UDP socket listeners are initially closed. Then the sockets are opened to listen to any address, because the IP address has been removed. A message stating that the IP address has been deleted from SIP bound interface is displayed. If the outgoing gateway has the **bind**command enabled and has an active call, the call becomes a one-way call with media flowing from the outgoing gateway to the terminating gateway.
The **physical cable is pulled** on the bound port, or the **Interface layer goes down**	The TCP and UDP socket listeners are initially closed. Then the sockets are opened and bound to listen to any address. When the pulled cable is replaced, the result is as documented for **no shutdown**interfaces.

Note If there are active calls, the **bind** command will not take effect if it is issued for the first time or if it is issued while another **bind** command is in effect. A message is displayed reminding you that there are active calls and that the **bind** command change cannot take effect.

How to Configure SIP Gateway Support for the bind Command

- Setting the Bind Address, page 25
- Setting a Source IP Address for Signaling and Media Packets, page 26

Setting the Bind Address

To set the bind address, complete the task in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **voip**
4. **session target ipv4:** *destination-address*
5. **exit**

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** *number* **voip** **Example:** `Device(config)# dial-peer voice 2 voip`	Enters dial peer configuration mode to configure a VoIP dial-peer.
Step 4	**session target ipv4:** *destination-address* **Example:** `Device(config-dial-peer)# session target ipv4: 172.16.43.3`	Specifies a network-specific address for a dial peer. • This command must be set to the bind address of the receiving gateway before using the **bind** command. • **ipv4** :*destination-address*: Sets the IP address of the dial peer. A valid IP address is in this format: *xxx.xxx.xxx.xxx*.
Step 5	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits dial peer voice configuration mode.

Setting a Source IP Address for Signaling and Media Packets

SIP configuration mode starts from voice-service VoIP configuration mode. When the router is in SIP configuration mode, several options are available, including the **bind** command. To enable this feature, review the prerequisites to make sure your network is compliant, and then complete the task in this section.

Set the bind address prior to using the **bind** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **session transport** {**udp** | **tcp**}
6. **bind** {**control** | **all**} **source-interface** *interface-id*
7. **default** {**bind**|**rel1xx**|**session-transport**|**url**}
8. **exit**

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	**sip** **Example:** `Device(config-voi-srv)# sip`	Enters the SIP configuration mode.
Step 5	**session transport** {**udp** | **tcp**} **Example:** `Device(conf-serv-sip)# session transport udp`	(Optional) Sets the session transport type for the SIP user agent. • The default is UDP. • The transport protocol (**udp** or **tcp**) specified with the **session transport**command, and the protocol specified with the **transport** command, must be identical.

	Command or Action	Purpose
Step 6	**bind** {**control** | **all**} **source-interface** *interface-id* **Example:** `Device(conf-serv-sip)# bind all source- interface fastethernet`	Sets a source address for signaling and media packets. • **control** : Binds SIP signaling packets. • **all** : Binds SIP signaling packets and media packets. • **source-interface** : Specifies an interface as the source address of SIP packets. • *interface-id* argument specifies the type of interface: ◦ Async ◦ BVI ◦ CTunnel ◦ Dialer ◦ Ethernet ◦ FastEthernet ◦ Lex ◦ Loopback ◦ Multilink ◦ Null ◦ Serial ◦ Tunnel ◦ Vif ◦ Virtual-Template ◦ Virtual-TokenRing
Step 7	**default** {**bind**|**rel1xx**|**session-transport**|**url**} **Example:** `Device(conf-serv-sip)# bind`	(Optional) Resets the default value of a SIP command. • **bind--** Configures the source address of signaling and media packets to a specific interface's IP address • **rel1xx** --Enables all SIP provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint • **session-transport** --Configures the underlying transport layer protocol for SIP messages to TCP or UDP • **url** --Configures URLs to either the SIP or TEL format for your voip sip calls
Step 8	**exit** **Example:** `Device(conf-serv-sip)# exit`	Exits the current configuration mode.

Verifying and Troubleshooting Tips

Two **show** commands verify the correct settings for the **bind** command. The first enables you to verify a bound IP address. The second indicates the status of bind (enabled or disabled):

Verifying a Bound IP Address

The following examples show output for the **show ip socket**command, indicating that the bind address of the receiving gateway is set:

```
Device# show ip socket
```

Proto Remote Port Local Port In Out Stat TTY OutputIF

17 0.0.0.0 0 --any-- 2517 0 0 9 0

17 --listen-- 172.18.192.204 1698 0 0 1 0

17 0.0.0.0 0 172.18.192.204 67 0 0 489 0

17 0.0.0.0 0 172.18.192.204 5060 0 0 A1 0

Verifying Bind Status

The following example shows output for the **show sip-ua status**command, indicating that bind is enabled.

```
Device# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): ENABLED 172.18.192.204
SIP User Agent bind status(media): ENABLED 172.18.192.204
SIP max-forwards : 6
```

SIP DNS SRV version: 1 (rfc 2052)

To troubleshoot this feature, perform the following:

- Use the **debug ccsip all** command to enable all SIP debugging capabilities, or use one of the following SIP debug commands:
  - **debug ccsip calls**
  - **debug ccsip error**
  - **debug ccsip events**
  - **debug ccsip messages**
  - **debug ccsip states**
- Use the **show ip socket**command to display IP socket information.
- Use the **show sip-ua status**command to verify if binding is enabled. See the **show sip-ua status**command for details.

Configuration Examples for SIP Gateway Support for the bind Command

SIP Gateway Support for the bind Command Example

This section shows partial output from the **show running-config** command, indicating that bind is functional on receiving router 172.18.192.204.

```
ip subnet-zero
ip ftp source-interface Ethernet0
!
voice service voip
 sip
  bind all source-interface FastEthernet0
!
interface FastEthernet0
 ip address 172.18.192.204 255.255.255.0
 duplex auto
 speed auto
 fair-queue 64 256 1000
 ip rsvp bandwidth 75000 100
!!
```

Feature Information for SIP Gateway Support for the bind Command

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 4 Feature Information for SIP: Gateway Support for the bind Command

Feature Name	Releases	Feature Information
SIP: Gateway Support for the bind Command	12.2(8)T 12.3(2)T 12.2(11)T 12.2(15)T	In Cisco IOS Release 12.2(8)T, This feature was introduced on the Cisco Unified Border Element. The following commands were introduced or modified: **bind**and **sip**.
SIP: Gateway Support for the bind Command	Cisco IOS XE Release 2.5	In Cisco IOS XE Release 2.5, This feature was introduced on the Cisco ASR 1000 Series Routers. The following commands were introduced or modified: **bind**and **sip**.

Configuring an Inbound Dial Peer to Match on a URI

To configure an inbound dial peer to match an URI on a remote IP Address on SIP Trunks, perform the following task.

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 at the end of this module.

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 Configuring an Inbound Dial Peer to Match on a URI

- Enable SIP header passing. For information, see the Cisco IOS SIP Configuration Guide, Release 15.1
- Write a Tcl IVR 2.0 script or VoiceXML document that accepts a SIP or TEL URI. For information, see the Tcl IVR API Version 2.0 Programmer's Guide or Cisco VoiceXML Programmer's Guide.

Cisco Unified Border Element

Cisco IOS Release 15.1(2)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

Cisco IOS XE Release 3.6S or a later release must be installed and running on your Cisco Unified Border Element (Enterprise).

Configuring an Inbound Dial-Peer to Match the URI on SIP Calls

This task describes how to configure an inbound dial-peer to match the URI in a SIP call.

SUMMARY STEPS

1. **enable**
2. **configureterminal**
3. **voice class uri***tag*
4. **host** *hostname-pattern* or **host** {**host** {**ipv4:** *ipv4-address* | **ipv6:***ipv6-address* |**dns:***dns-address* | *hostname-pattern* }
5. **exit**
6. **dial-peer voice** *tag***voip**
7. **sessionprotocol sipv2**
8. **incoming uri** { **from** | **request** | **to** | **via** *tag*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Device> configure terminal`	Enters global configuration mode.
Step 3	**voice class uri***tag* **Example:** `Device(config)# voice class uri ab200 sip`	Creates a voice class for matching dial peers to a SIP and enters voice URI class configuration mode.

	Command or Action	Purpose

Step 4	**host** *hostname-pattern* or **host** {**host** {**ipv4:** *ipv4-address* | **ipv6:***ipv6-address* |**dns:***dns-address* |*hostname-pattern* }
	
	Example:
	
	`Device(config-voice-uri-class)# host server1`
	`or`
	`Device(config-voice-uri-class)# host`
	`ipv4:10.0.0.0`
		(Optional) Specifies a regular expression pattern for matching the hostname field in the SIP URI.
		
		• This command can have a single instance only.
		• You can specify up to ten instances of this command.
		
		Note You can use either the **host hostname** or **host** {**host** {**ipv4:** *ipv4-address* | **ipv6:***ipv6-address* |**dns:***dns-address* |*hostname-pattern* } command.

Step 5	**exit** **Example:** `Device(config-voice-uri-class)# exit`	Enters global configuration mode.
Step 6	**dial-peer voice** *tag***voip** **Example:** `Device(config)# dial-peer voice 6000 voip`	Enters dial peer voice configuration mode.
Step 7	**sessionprotocol sipv2** **Example:** `Device(config-dial-peer)# session protocol sipv2`	Configures SIP as the session protocol type.
Step 8	**incoming uri** { **from** | **request** | **to** | **via** *tag* **Example:** `Device(config-dial-peer)# incoming uri via ab200`	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
Step 9	**end** **Example:** `Device(config-dial-peer)# end`	Exits dial peer voice configuration mode and enters privileged EXEC mode.

Feature Information for Inbound Dial-peer Match Based on Remote IP Address on SIP Trunks

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.

Feature Name	Releases	Feature Information
Inbound Dial-peer Match Based on Remote IP Address on SIP Trunks	15.1(2)T	The Support Inbound Dial-peer Match Based on Remote IP Address on SIP Trunks feature supports the expansion of inbound dial-peer matching logic to include matching based on the source IP address of inbound signaling on a SIP trunk. This feature enables enforcement of specific call-treatment, security, and routing policies on each SIP trunk. In Cisco IOS Release 15.1(2)T this feature was implemented on the Cisco Unified Border Element. The following commands were introduced or modified: **dial-peer voice**, **voice-class uri**.
SIP and TEL URL support	Cisco IOS XE Release 3.6S	The Support Inbound Dial-peer Match Based on Remote IP Address on SIP Trunks feature supports the expansion of inbound dial-peer matching logic to include matching based on the source IP address of inbound signaling on a SIP trunk. This feature enables enforcement of specific call-treatment, security, and routing policies on each SIP trunk. In Cisco IOS Release 15.1(2)T this feature was implemented on the Cisco Unified Border Element (Enterprise). The following commands were introduced or modified: **dial-peer voice**, **voice-class uri**.

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 at the end of this module.

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 Multiple Destination Pattern Support on a Voice Dial Peer

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.7S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for Multiple Destination Pattern Support on a Voice Dial Peer

- The Multiple Destination Pattern Support on Voice Dial Peer feature is supported only on a VoIP dial peer.
- An E.164 pattern map is not supported on an inbound dial peer.
- An E.164 pattern map may not be supported on a local file system depending on the Cisco software version that you are using.
- Duplicate destination patterns cannot be added to a pattern map.

Information About Multiple Destination Pattern Support on a Voice Dial Peer

Overview of Multiple Destination Pattern Support on a Voice Dial Peer

On Cisco Unified Border Element (Enterprise) and Session Initiation Protocol (SIP) Gateway, one VoIP dial peer can have only one destination pattern. To support multiple destination patterns on a VoIP dial peer, which involve massive dial peer configuration, use an E.164 destination pattern map. You can create a destination E.164 pattern map and then link it to one or more dial peers. A destination pattern, which is associated with a dialed string on a specific telephony device, is configured on a VoIP dial peer by using the **destination e164-pattern map** command. When a dialed string on a telephony device matches the destination pattern, calls are routed on to the VoIP dial peer; otherwise the call fails. You must configure an E.164 destination pattern map for each VoIP dial peer that is defined on a device. Configuring an E.164 destination pattern map on multiple dial peers requires several configurations as compared to configuring a destination pattern map on a single dial peer.

When a destination pattern is the only source to enable a dial peer, a valid E.164 destination pattern map enables linked dial peers, whereas an invalid E.164 destination pattern map disables the linked dial peers. Additionally, whenever an E.164 destination pattern map is created or reloaded, one or more dial peers linked with an E.164 destination pattern map is enabled or disabled based on the validation of a pattern map.

When a dial peer has multiple destination patterns, select the longest prefix matching criteria to count as the pattern matched for the dial peer. For example, if dial peer A has two destination patterns matched where one destination pattern is matched with five digits and the other destination pattern is matched with four digits, then dial peer A is counted as matched with five digits.

How to Configure Multiple Destination Pattern Support on a Voice Dial Peer

Configuring Multiple Destination Pattern Support on a Voice Dial Peer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class e164-pattern-map** *tag*
4. **url** *url*
5. **e164** *pattern*
6. **description** *string*
7. **exit**
8. **dial-peer voice** *tag***voip system**
9. **destination e164-pattern-map** *tag*
10. **end**
11. **voice class e164-pattern-map load***tag*
12. **show dial-peer voice**
13. **show voice class e164-pattern-map** [**summary** | *tag*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters 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 class e164-pattern-map** *tag* **Example:** `Device(config)# voice class e164-pattern-map 11`	Creates an E.164 pattern map to configure multiple destination E.164 patterns on a dial peer and enters voice class E.164 pattern map configuration mode.
Step 4	**url** *url* **Example:** `Device(config-voice class e164-pattern-map)# url http://http-host/config-files/destination-pattern-map.cfg`	Defines the URL of an internally or an externally stored text file used in the E.164 pattern map. **Note** If you are using the **url** command, skip Step 5 and proceed to Step 6.
Step 5	**e164** *pattern* **Example:** `Device(config-voice class e164-pattern-map)# e164 5557123`	Defines a complete E.164 telephone number prefix.
Step 6	**description** *string* **Example:** `Device(config-voice class e164-pattern-map)# description It has 3 entries`	Provides a description for a specific E.164 pattern map.
Step 7	**exit** **Example:** `Device(config-voice class e164-pattern-map)# exit`	Exits voice class E.164 pattern map configuration mode and enters global configuration mode.
Step 8	**dial-peer voice** *tag***voip system** **Example:** `Device(config)# dial-peer voice 123 voip system`	Defines a local dial peer and enters dial peer configuration mode.

	Command or Action	Purpose
Step 9	**destination e164-pattern-map** *tag* **Example:** `Device(config-dial-peer)# **destination e164-pattern-map 1111**`	Links an E.164 pattern map to one or more dial peers. • Identifies a destination E.164 pattern map associated with a dial peer with a number assigned to the destination E.164 pattern map. The range is from 1 to 10000. **Note** Repeat the Steps 1 to 9 to add multiple destination E.164 patterns to a pattern map.
Step 10	**end** **Example:** `Device(config-dial-peer)# **end**`	Exits dial peer configuration mode and enters privileged EXEC mode.
Step 11	**voice class e164-pattern-map load***tag* **Example:** `Device# **voice class e164-pattern-map load 2543**`	Loads a destination E.164 pattern map that is specified by a text file.
Step 12	**show dial-peer voice** **Example:** `Device# **show dial-peer voice**`	Displays the status of an E.164 pattern map when the pattern map is associated with a dial peer.
Step 13	**show voice class e164-pattern-map** [**summary** | *tag*] **Example:** `Device# **show voice class e164-pattern-map 11**`	Displays the status of the configured E.164 pattern maps and the status of the text file. • Also displays the status and the content of a particular E.164 pattern map.

Configuration Examples for Multiple Destination Pattern Support on a Voice Dial Peer

Example: Multiple Destination Pattern Support on a Voice Dial Peer

```
voice class e164-pattern-map 11
  url http://http-host/config-files/destination-pattern-map.cfg
  e164 5557456
description it has 5 entries
!
dial-peer voice tag voip system
destination e164-pattern-map 1131
!
voice class e164-pattern-map load 2543
!
```

Information About Multiple Destination Pattern Support on a Voice Dial Peer

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 5 Feature Information for Multiple Destination Pattern Support on a Voice Dial Peer

Feature Name	Releases	Feature Information
Multiple Destination Pattern Support on a Voice Dial Peer	15.2(4)M	The Multiple Destination Pattern Support on a Voice Dial Peer feature is used for handling calls that have noncontiguous dial patterns. This feature allows you to create an E.164 pattern map with multiple destination E.164 pattern, which helps to define and configure destination patterns on an individual dial peer or multiple dial peers. The following commands were introduced or modified: **destination e164-pattern-map**, **e164**, **show voice class e164-pattern-map**, **url**, **voice class e164-pattern-map load**, **voice class e164-pattern-map**.

Feature Name	Releases	Feature Information
Multiple Destination Pattern Support on a Voice Dial Peer	Cisco IOS XE Release 3.7S	The Multiple Destination Pattern Support on a Voice Dial Peer feature is used for handling calls that have noncontiguous dial patterns. This feature allows you to create an E.164 pattern map with multiple destination E.164 pattern, which helps to define and configure destination patterns on an individual dial peer or multiple dial peers. The following commands were introduced or modified: **destination e164-pattern-map**, **e164**, **show voice class e164-pattern-map**, **url**, **voice class e164-pattern-map load**, **voice class e164-pattern-map**.

SIP Video Calls with Flow Around Media

The SIP Video Calls with Flow Around Media feature provides the ability to have a SIP video call where the media flows around the Cisco Unified Border Element (Cisco UBE) and the Cisco Unified Border Element (Enterprise) platform. Previous support was only for call scenarios where the media flowed through the Cisco UBE.

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 at the end of this module.

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 SIP Video Calls with Flow Around Media

Cisco Unified Border Element

- Cisco IOS Release 12.4(15)XZ or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for SIP Video Calls with Flow Around Media

- Media flow-around for Delayed-Offer to Early-Offer audio and video calls is not supported.

How to Configure Support for SIP Video Calls with Flow Around Media

To enable this feature use the **media** command in dial peer, voice class, or voice service configuration mode. For detailed information on the use of this command, see the *Cisco IOS Voice Command Reference* at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr3/vcr-m1.html#GUID-817A36E2-6AF5-498C-A815-4E97D32FDF1B

Feature Information for Support for SIP Video Calls with Flow Around Media

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.

Feature Name	Releases	Feature Information
SIP Video Calls with Flow Around Media	12.4(15)XZ 12.4(20)T	This feature provides the capability for media packets to pass directly between endpoints without the intervention of the Cisco UBE. In Cisco IOS Release 12.4(15)XZ this feature was implemented on the Cisco Unified Border Element. The following command was modified by this feature: **media**
SIP Video Calls with Flow Around Media	Cisco IOS XE Release 3.1S	This feature provides the capability for media packets to pass directly between endpoints without the intervention of the Cisco UBE. In Cisco IOS XE Release 3.1S this feature was implemented on the Cisco Unified Border Element (Enterprise). The following command was modified by this feature: **media**

Additional References

The following sections provide references related to the Cisco Unified Border Element (Enterprise) Configuration Guide.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS Voice commands	*Cisco IOS Voice Command Reference*
Cisco IOS Voice Configuration Library	For more information about Cisco IOS voice features, including feature documents, and troubleshooting information--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm
Cisco IOS Release 15.0	Cisco IOS Release 15.0 Configuration Guides
Cisco IOS Release 12.2	Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2

Related Topic	Document Title
internet Low Bitrate Codec (iLBC) Documents	• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/ dp_ovrvw.html • Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/ dp_confg.html
Related Application Guides	• *Cisco Unified Communications Manager and Cisco IOS Interoperability Guide* • *Cisco IOS SIP Configuration Guide* • Cisco Unified Communications Manager (CallManager) Programming Guides
Troubleshooting and Debugging guides	• Cisco IOS Debug Command Reference, Release 12.4 at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html • *Troubleshooting and Debugging VoIP Call Basics* at http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml • *VoIP Debug Commands* at http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html

Standards

Standard	Title
ITU-T G.711	--

MIBs

MIB	MIBs Link
• CISCO-PROCESS MIB • CISCO-MEMORY-POOL-MIB • CISCO-SIP-UA-MIB • DIAL-CONTROL-MIB • CISCO-VOICE-DIAL-CONTROL-MIB • CISCO-DSP-MGMT-MIB • IF-MIB • IP-TAP-MIB • TAP2-MIB • USER-CONNECTION-TAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1889	*RTP: A Transport Protocol for Real-Time Applications*
RFC 2131	*Dynamic Host Configuration Protocol*
RFC 2132	*DHCP Options and BOOTP Vendor Extensions*
RFC 2198	*RTP Payload for Redundant Audio Data*
RFC 2327	*SDP: Session Description Protocol*
RFC 2543	*SIP: Session Initiation Protocol*
RFC 2543-bis-04	*SIP: Session Initiation Protocol, draft-ietf-sip-rfc2543bis-04.txt*
RFC 2782	*A DNS RR for Specifying the Location of Services (DNS SRV)*
RFC 2833	*RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*
RFC 3203	*DHCP reconfigure extension*
RFC 3261	*SIP: Session Initiation Protocol*
RFC 3262	*Reliability of Provisional Responses in Session Initiation Protocol (SIP)*
RFC 3323	*A Privacy Mechanism for the Session Initiation Protocol (SIP)*

RFC	Title
RFC 3325	*Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*
RFC 3515	*The Session Initiation Protocol (SIP) Refer Method*
RFC 3361	*Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers*
RFC 3455	*Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)*
RFC 3608	*Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration*
RFC 3711	*The Secure Real-time Transport Protocol (SRTP)*
RFC 3925	Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Glossary

AMR-NB —Adaptive Multi Rate codec - Narrow Band.

Allow header —Lists the set of methods supported by the UA generating the message.

bind — In SIP, configuring the source address for signaling and media packets to the IP address of a specific interface.

call —In SIP, a call consists of all participants in a conference invited by a common source. A SIP call is identified by a globally unique call identifier. A point-to-point IP telephony conversation maps into a single SIP call.

call leg —A logical connection between the router and another endpoint.

CLI —command-line interface.

Content-Type header —Specifies the media type of the message body.

CSeq header —Serves as a way to identify and order transactions. It consists of a sequence number and a method. It uniquely identifies transactions and differentiates between new requests and request retransmissions.

delta —An incremental value. In this case, the delta is the difference between the current time and the time when the response occurred.

dial peer —An addressable call endpoint.

DNS -—Domain Name System. Used to translate H.323 IDs, URLs, or e-mail IDs to IP addresses. DNS is also used to assist in locating remote gatekeepers and to reverse-map raw IP addresses to host names of administrative domains.

DNS SRV —Domain Name System Server. Used to locate servers for a given service.

DSP —Digital Signal Processor.

DTMF —dual-tone multifrequency. Use of two simultaneous voice-band tones for dialing (such as touch-tone).

EFXS —IP phone virtual voice ports.

FQDN —fully qualified domain name. Complete domain name including the host portion; for example, *serverA.companyA.com* .

FXS —analog telephone voice ports.

gateway —A gateway allows SIP or H.323 terminals to communicate with terminals configured to other protocols by converting protocols. A gateway is the point where a circuit-switched call is encoded and repackaged into IP packets.

H.323 —An International Telecommunication Union (ITU-T) standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the conferencing system and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol.

iLBC —internet Low Bitrate Codec.

INVITE—A SIP message that initiates a SIP session. It indicates that a user is invited to participate, provides a session description, indicates the type of media, and provides insight regarding the capabilities of the called and calling parties.

IP—Internet Protocol. A connectionless protocol that operates at the network layer (Layer 3) of the OSI model. IP provides features for addressing, type-of-service specification, fragmentation and reassemble, and security. Defined in RFC 791. This protocol works with TCP and is usually identified as TCP/IP. See TCP/IP.

ISDN —Integrated Services Digital Network.

Minimum Timer —Configured minimum value for session interval accepted by SIP elements (proxy, UAC, UAS). This value helps minimize the processing load from numerous INVITE requests.

Min-SE —Minimum Session Expiration. The minimum value for session expiration.

multicast —A process of transmitting PDUs from one source to many destinations. The actual mechanism (that is, IP multicast, multi-unicast, and so forth) for this process might be different for LAN technologies.

originator —User agent that initiates the transfer or Refer request with the recipient.

PDU —protocol data units. Used by bridges to transfer connectivity information.

PER —Packed Encoding Rule.

proxy —A SIP UAC or UAS that forwards requests and responses on behalf of another SIP UAC or UAS.

proxy server —An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets and, if necessary, rewrites a request message before forwarding it.

recipient —User agent that receives the Refer request from the originator and is transferred to the final recipient.

redirect server —A server that accepts a SIP request, maps the address into zero or more new addresses, and returns these addresses to the client. It does not initiate its own SIP request or accept calls.

re-INVITE —An INVITE request sent during an active call leg.

Request URI —Request Uniform Resource Identifier. It can be a SIP or general URL and indicates the user or service to which the request is being addressed.

RFC —Request For Comments.

RTP —Real-Time Transport Protocol (RFC 1889)

SCCP —Skinny Client Control Protocol.

SDP—Session Description Protocol. Messages containing capabilities information that are exchanged between gateways.

session —A SIP session is a set of multimedia senders and receivers and the data streams flowing between the senders and receivers. A SIP multimedia conference is an example of a session. The called party can be invited several times by different calls to the same session.

session expiration —The time at which an element considers the call timed out if no successful INVITE transaction occurs first.

session interval —The largest amount of time that can occur between INVITE requests in a call before a call is timed out. The session interval is conveyed in the Session-Expires header. The UAS obtains this value from the Session-Expires header of a 2*xx* INVITE response that it sends. Proxies and UACs determine this value from the Session-Expires header in a 2*xx* INVITE response they receive.

SIP —Session Initiation Protocol. An application-layer protocol originally developed by the Multiparty Multimedia Session Control (MMUSIC) working group of the Internet Engineering Task Force (IETF). Their goal was to equip platforms to signal the setup of voice and multimedia calls over IP networks. SIP features are compliant with IETF RFC 2543, published in March 1999.

SIP URL —Session Initiation Protocol Uniform Resource Locator. Used in SIP messages to indicate the originator, recipient, and destination of the SIP request. Takes the basic form of *user@host* , where *user* is a name or telephone number, and *host* is a domain name or network address.

SPI —service provider interface.

socket listener —Software provided by a socket client to receives datagrams addressed to the socket.

stateful proxy —A proxy in keepalive mode that remembers incoming and outgoing requests.

TCP —Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmissions. TCP is part of the TCP/IP protocol stack. See also TCP/IP and IP.

TDM —time-division multiplexing.

UA —user agent. A combination of UAS and UAC that initiates and receives calls. See **UAS**and **UAC**.

UAC —user agent client. A client application that initiates a SIP request.

UAS —user agent server. A server application that contacts the user when a SIP request is received and then returns a response on behalf of the user. The response accepts, rejects, or redirects the request.

UDP —User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC-768.

URI —Uniform Resource Identifier. Takes a form similar to an e-mail address. It indicates the user’s SIP identity and is used for redirection of SIP messages.

URL —Universal Resource Locator. Standard address of any resource on the Internet that is part of the World Wide Web (WWW).

User Agent —A combination of UAS and UAC that initiates and receives calls. See **UAS and UAC.**

VFC —Voice Feature Card.

VoIP —Voice over IP. The ability to carry normal telephone-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term that generally refers to the Cisco standards-based approach (for example, H.323) to IP voice traffic.