# Configuring SIP Bind Features

**First Published: October 24, 2001**
**Last Updated: July 21, 2010**

The SIP Gateway Support for the bind Command feature allows you to configure the source IP address of signaling packets and media packets.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for SIP Bind Features" section on page 19.

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

## Contents



**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Prerequisites for SIP Bind Features

The following are the prerequisites for this feature:

- Ensure the gateway has voice functionality that is configurable for Session Initiation Protocol (SIP).
- Establish a working IP network. For more information about configuring IP, refer to the *Cisco IOS IP Addressing Configuration Guide*.
- Configure VoIP. For more information about configuring VoIP, refer to the *Cisco IOS Voice Command Reference*.

# Restrictions for SIP Bind Features

Although the **bind all** command is an accepted configuration, it does not appear in **show running-config** command output. Because the **bind all** command is equivalent to issuing the commands **bind source** and **bind media**, those are the commands that appear in the **show running-config** command output.

# Information About SIP Bind Features

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 an IP address so that only those ports are open to the outside world. 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.

## Benefits of SIP Bind Features

The benefits of SIP Bind feature is as follows:

- SIP signaling and media paths can advertise the same source IP address on the gateway for certain applications, even if the paths used different addresses to reach the source. This eliminates confusion for firewall applications that may have taken action on source address packets before the use of binding.
- Firewalls filter messages based on variables such as the message source, the target address, and available ports. Normally a firewall opens only certain addresses or port combination to the outside world and those addresses can change dynamically. Because VoIP technology requires the use of more than one address or port combination, the **bind** command adds flexibility by assigning a gateway to a specific interface (and therefore the associated address) for the signaling or media application.
- You can obtain a predefined and separate interface for both signaling and media traffic. Once a **bind** command is in effect, the interface it limits is bound solely to that purpose. Administrators can therefore dictate the use of one network to transport the signaling and another network to transport the media. The benefits of administrator control are:
  - Administrators know the traffic that runs on specific networks, thereby making debugging easier.

  - Administrators know the capacity of the network and the target traffic, thereby making engineering and planning easier.
  - Traffic is controlled, allowing Qualtiy of Service (QoS) to be monitored.
- The **bind media** command relaxes the constraints imposed by the **bind control** and **bind all** commands, which cannot be set during an active call. The **bind media** command works with active calls.

To configure SIP Gateway Support for the bind Command, you should understand the following concepts:

- Source Address, page 3
- Voice Media Stream Processing, page 6

# Source Address

In early releases of Cisco IOS software with SIP functionality, 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.

However, the **bind** command allows you to configure the source IP address of signaling and media packets to a specific interface's IP address. Thus, 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 want to specify a bind address or if the interface is down, the IP layer still provides the best local address.

The Support Ability to Configure Source IP Address for Signaling and Media per SIP Trunk feature extends the global bind functionality to support the SIP signaling Transport Layer Socket (TLS) with UDP and TCP. The source address at the dial peer is the source address in all the signaling and media packets between the gateway and the remote SIP entity for calls using the dial-peer. Multiple SIP listen sockets with specific source address handle the incoming SIP traffic from each selected SIP entity. The order of preference for retrieving the SIP signalling and media source address for inbound and outbound calls is as follows:

- Bind configuration at dial peer level
- Bind configuration at global level
- Best local IP address to reach the destination

Table 1 describes the state of the system when the **bind** command is applied in the global or dial peer level:

*Table 1 State of the System for the bind Address*

| Bind State | System Status |
|---|---|
| No global bind | The best local address is used in all outbound SIP messages.<br>Only one SIP listen socket with a wildcard source address. |
| Global bind | Global bind address used in all outbound SIP messages.<br>Only one SIP listen socket with global bind address. |
| No global bind<br>Dial peer bind | Dial peer bind address is used in outbound SIP messages of this dial peer. The remaining SIP messages use the best local address.<br>One SIP listen socket with a wildcard source address.<br>Additional SIP listen socket for each different dial peer bind listening on the specific dial peer bind address. |
| Global bind<br>Dial peer bind | Dial peer bind address is used in outbound SIP messages of this dial peer. The remaining SIP messages use the global bind address.<br>One SIP listen socket with global bind address.<br>Additional SIP listen socket for each different dial peer bind command listening on the specific dial peer bind address. |

The **bind** command performs different functions based on the state of the interface (see Table 2).

*Table 2 State of the Interface for the bind Command*

| Interface State | Result Using Bind Command |
|---|---|
| Shut down<br>With or without active calls | TCP, TLS, and User Datagram Protocol (UDP) socket listeners are initially closed. (Socket listeners receive datagrams addressed to the socket.)<br>Then the sockets are opened to listen to any IP address.<br>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.<br>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages. |
| No shut down<br>No active calls | TCP, TLS, and UDP socket listeners are initially closed. (Socket listeners receive datagrams addressed to the socket.)<br>Then the sockets are opened and bound to the IP address set by the **bind** command.<br>The sockets accept packets destined for the bound address only.<br>The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages. |
| No shut down<br>Active calls | TCP, TLS, and UDP socket listeners are initially closed.<br>Then the sockets are opened to listen to any IP address.<br>The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages. |

*Table 2 State of the Interface for the bind Command (continued)*

| Interface State | Result Using Bind Command |
|---|---|
| Bound-interface IP address is removed | TCP, TLS, and UDP socket listeners are initially closed.<br>Then the sockets are opened to listen to any address, because the IP address has been removed. This happens even when SIP was never bound to an IP address.<br>A message stating that the IP address has been deleted from the SIP bound interface is printed.<br>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.<br>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages. |
| The physical cable is pulled on the bound port, or<br>the interface layer is down | TCP, TLS, and UDP socket listeners are initially closed.<br>Then the sockets are opened and bound to listen to any address.<br>When the pulled cable is replaced, the result is as documented for **no shutdown** interfaces.<br>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages. |
| A bind interface is shut down, or<br>its IP address is changed, or<br>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.<br>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.<br>If the bind interface is shutdown, the dial peer bind socket listeners of the interface are closed. If the IP address of the interface is changed, the socket listeners representing the bind command is opened with the available IP address of the interface and the configuration turns active for all subsequent SIP messages. |
| **Note** If there are active calls, the **bind** command does not take effect if it is issued for the first time or another **bind** command is in effect. A message reminds you that there are active calls and that the change cannot take effect. | |

The **bind** command applied at the dial peer level can be modified only in the following situations:

- Dial peer bind is disabled in the supported IOS configuration options.
- Dial peer bind is removed when the bound interface is removed.
- Dial peer bind is removed when the dial peer is removed.

# Voice Media Stream Processing

The SIP Gateway Support Enhancements to the bind Command feature extends the capabilities of the **bind** command by supporting a deterministic network interface for the voice media stream. Before the voice media stream addition, the **bind** command supported a deterministic network interface for control (signaling) traffic or all traffic. With the SIP Gateway Support Enhancements to the bind Command feature a finer granularity of control is achieved on the network interfaces used for voice traffic.

If multiple **bind** commands are issued in sequence—that is, if one **bind** command is configured and then another **bind** command is configured—a set interaction happens between the commands. Table 3 describes the expected command behavior.

*Table 3 Interaction Between Previously Set and New bind Commands*

| Interface State | bind Command | Result Using bind Command |
|---|---|---|
| Without active calls | **bind all** | Generated **bind control** and **bind media** commands to override existing **bind control** and **bind media** commands. |
| | **bind control** | Overrides existing **bind control** command. |
| | **bind media** | Overrides existing **bind media** command. |
| With active calls | **bind all** or **bind control** | Blocks the command, and the following messages are displayed:<br>00:16:39: There are active calls<br>00:16:39: configure_sip_bind_command: The bind command change will not take effect |
| | **bind media** | Succeeds and overrides any existing **bind media** command. |

The **bind all** and **bind control** commands perform different functions based on the state of the interface. Table 4 describes the actions performed based on the interface state.

**Note** The **bind all** command only applies to global level, whereas the **bind control** and **bind media** command apply to global and dial peer. Table 4 applies to **bind media** only if the media interface is the same as the **bind control** interface. If the two interfaces are different, media behavior is independent of the interface state.

*Table 4 bind all and bind control Functions, Based on Interface State*

| Interface State | Result Using bind all or bind control Commands |
|---|---|
| Shut down<br>With or without active calls | TCP, TLS, and UDP socket listeners are initially closed. (Socket listeners receive datagrams addressed to the socket.)<br>Then the sockets are opened to listen to any IP address.<br>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.<br>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages. |
| Not shut down<br>Without active calls | TCP, TLS, and UDP socket listeners are initially closed. (Socket listeners receive datagrams addressed to the socket.)<br>Then the sockets are opened and bound to the IP address set by the **bind** command.<br>The sockets accept packets destined for the bound address only.<br>The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages. |
| Not shut down<br>With active calls | TCP, TLS, and UDP socket listeners are initially closed.<br>Then the sockets are opened to listen to any IP address.<br>The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages. |
| Bound interface's IP address is removed. | TCP, TLS, and UDP socket listeners are initially closed.<br>Then the sockets are opened to listen to any address because the IP address has been removed.<br>A message is printed that states the IP address has been deleted from the bound SIP interface.<br>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.<br>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages. |

*Table 4 bind all and bind control Functions, Based on Interface State (continued)*

| Interface State | Result Using bind all or bind control Commands |
|---|---|
| The physical cable is pulled on the bound port, or the interface layer goes down. | TCP, TLS, and UDP socket listeners are initially closed.<br>Then the sockets are opened and bound to listen to any address.<br>When the pulled cable is replaced, the result is as documented for interfaces that are not shut down.<br>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages. |
| 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. The media 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.<br>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.<br>If the bind interface is shutdown, the dial peer bind socket listeners of the interface are closed. If the IP address of the interface is changed, the socket listeners representing the bind command is opened with the available IP address of the interface and the configuration turns active for all subsequent SIP messages. |

# How to Configure SIP Bind Features

This section contains the following procedures:

- Setting the Bind Command at the Global Level, page 8 (required)
- Setting the Bind Command at the Dial-peer Level, page 10 (optional)
- Monitoring the Bind Command, page 12 (optional)

## Setting the Bind Command at the Global Level

To configure the **bind** command to an interface at the global level, perform the following steps.

**Note** The **bind media** command applies to specific interfaces.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type/number*
4. **ip address** *ip-address mask* [**secondary**]
5. **exit**
6. **voice service voip**

7. **sip**
8. **bind** {**control** | **media** | **all**} **source-interface** *interface-id* [**ipv6-address** *ipv6-address*]
9. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type/number*<br><br>**Example:**<br>`Router(config)# interface fastethernet0/0` | Configures an interface type and enters the interface configuration mode.<br>• *type/number*—Type of interface to be configured and the port, connector, or interface card number. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br><br>**Example:**<br>`Router(config-if)# ip address 192.168.200.33 255.255.255.0` | Configures a primary or secondary IP address for an interface.<br>• *ip-address mask*—IP address and mask for the associated IP subnet.<br>• **secondary**—Makes the configured address a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | Exits the current mode. |
| **Step 6** | **voice service voip**<br><br>**Example:**<br>`Router(config)# voice service voip` | Enters voice service configuration mode. |
| **Step 7** | **sip**<br><br>**Example:**<br>`Router(conf-voi-serv)# sip` | Enters SIP configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **bind** {**control** \| **media** \| **all**} **source-interface** *interface-id* [**ipv6-address** *ipv6-address*]<br><br>**Example:**<br>`Router(conf-serv-sip)# bind control source-interface FastEthernet0/0` | Sets a source interface for signaling and media packets.<br>• **control**—Binds signaling packets.<br>• **media**—Binds media packets.<br>• **all**—Binds signaling and media packets.<br>• **source interface** *interface-id*—Type of interface and its ID.<br>• **ipv6-address** *ipv6-address*—Configures the IPv6 address. |
| **Step 9** | **exit**<br><br>**Example:**<br>`Router(conf-serv-sip)# exit` | Exits the current mode. |

# Setting the Bind Command at the Dial-peer Level

To configure the **bind** command on SIP for a VoIP dial-peer, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type/number*
4. **ip address** *ip-address mask* [**secondary**]
5. **exit**
6. **dial-peer voice** *tag* **voip**
7. **session protocol sipv2**
8. **voice-class sip bind** {**control** | **media**} **source interface** *interface-id* [**ipv6-address** *ipv6-address*]
9. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *type/number*<br><br>**Example:**<br>`Router(config)# interface fastethernet0/0` | Configures an interface type and enters the interface configuration mode.<br>• *type/number*—Type of interface to be configured and the port, connector, or interface card number.<br>**Note** You can only bind Loopback, Ethernet, FastEthernet, GigabitEthernet and Serial interfaces for dial peer. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br><br>**Example:**<br>`Router(config-if)# ip address 2001:0DB8:0:1::1` | Configures a primary or secondary IP address for an interface.<br>• *ip-address mask*—IP address and mask for the associated IP subnet.<br>• **secondary**—Makes the configured address a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | Exits the current mode. |
| **Step 6** | **dial-peer voice** *tag* **voip**<br><br>**Example:**<br>`Router(config)# dial-peer voice 100 voip` | Enters dial peer voice configuration mode for the specified VoIP dial peer. |
| **Step 7** | **session protocol sipv2**<br><br>**Example:**<br>`Router(config-dial-peer)# session protocol sipv2` | Specifies use of IETF SIP. |
| **Step 8** | **voice-class sip bind** {**control** \| **media**} **source interface** *interface-id* [**ipv6-address** *ipv6-address*]<br><br>**Example:**<br>`Router(config-dial-peer)# voice-class sip bind control source-interface fastethernet0/0 ipv6-address 2001:0DB8:0:1::1` | Sets a source interface for signaling and media packets.<br>• **control**—Binds signaling packets.<br>• **media**—Binds media packets.<br>• **source interface** *interface-id*—Type of interface and its ID.<br>• **ipv6-address** *ipv6-address*—(Optional) Configures the IPv6 address to the source interface. |
| **Step 9** | **exit**<br><br>**Example:**<br>`Router(config-dial-peer)# exit` | Exits the current mode. |

## Troubleshooting Tips

For troubleshooting tips and a list of important debug commands, see *Verifying and Troubleshooting SIP Features*.

# Monitoring the Bind Command

To monitor the **bind** command, perform the following steps.

## SUMMARY STEPS

1. **show ip sockets**
2. **show sip-ua status**
3. **show sip-ua connections** {**tcp** [**tls**] | **udp**} {**brief** | **detail**}
4. **show dial-peer voice**

## DETAILED STEPS

### Step 1 show ip sockets

Use this command to display IP socket information and indicate whether the bind address of the receiving gateway is set.

The following sample output indicates that the bind address of the receiving gateway is set:

```
Router# show ip sockets

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
```

### Step 2 show sip-ua status

Use this command to display SIP user-agent status and indicate whether bind is enabled.

The following sample output indicates that signaling is disabled and media on 172.18.192.204 is enabled:

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED

SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): ENABLED 172.18.192.204
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv4
```

```
SDP application configuration:
 Version line (v=) required
Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

**Step 3** **show sip-ua connections {tcp [tls] | udp} {brief | detail}**

Use this command to display the connection details for the UDP transport protocol. The command output looks identical for TCP and TLS.

```
Router# show sip-ua connections udp detail

Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 10

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

 No Active Connections Found


-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id               Local-Address
 ===========    ============================
   2             [9.42.28.29]:5060
```

**Step 4** **show dial-peer voice**

Use this command, for each dial peer configured, to verify that the dial-peer configuration is correct. The following is sample output from this command for a VoIP dial peer:

```
Router# show dial-peer voice 101

VoiceOverIpPeer1234
        peer type = voice, system default peer = FALSE, information type = voice,
        description = `',
        tag = 1234, destination-pattern = `',
        voice reg type = 0, corresponding tag = 0,
        allow watch = FALSE
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        CLID Override RDNIS = disabled,
        rtp-ssrc mux = system
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 1234, Admin state is up, Operation state is down,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
```

```
modem transport = system,
URI classes:
    Incoming (Request) =
    Incoming (Via) =
    Incoming (To) =
    Incoming (From) =
    Destination =
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
outgoing COR list:minimum requirement
outgoing LPCOR:
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = `'
disconnect-cause = `no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
mailbox selection policy: none
type = voip, session-target = `',
technology prefix:
settle-call = disabled
ip media DSCP = ef, ip media rsvp-pass DSCP = ef
ip media rsvp-fail DSCP = ef, ip signaling DSCP = af31,
ip video rsvp-none DSCP = af41,ip video rsvp-pass DSCP = af41
ip video rsvp-fail DSCP = af41,
ip defending Priority = 0, ip preemption priority = 0
ip policy locator voice:
ip policy locator video:
UDP checksum = disabled,
session-protocol = sipv2, session-transport = system,
req-qos = best-effort, acc-qos = best-effort,
req-qos video = best-effort, acc-qos video = best-effort,
req-qos audio def bandwidth = 64, req-qos audio max bandwidth = 0,
req-qos video def bandwidth = 384, req-qos video max bandwidth = 0,
RTP dynamic payload type values: NTE = 101
Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
       CAS=123, TTY=119, ClearChan=125, PCM switch over u-law=0,
       A-law=8, GSMAMR-NB=117 iLBC=116, AAC-ld=114, iSAC=124
       lmr_tone=0, nte_tone=0
       h263+=118, h264=119
       G726r16 using static payload
       G726r24 using static payload
RTP comfort noise payload type = 19
fax rate = voice,   payload size =  20 bytes
fax protocol = system
fax-relay ecm enable
Fax Relay ans enabled
Fax Relay SG3-to-G3 Enabled (by system configuration)
fax NSF = 0xAD0051 (default)
codec = g729r8,   payload size =  20 bytes,
video codec = None
voice class codec = `'
voice class sip session refresh system
voice class sip rsvp-fail-policy voice post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy voice post-alert optional keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert optional keep-alive interval 30
text relay = disabled
Media Setting = forking (disabled) flow-through (global)
Expect factor = 10, Icpif = 20,
```

```
Playout Mode is set to adaptive,
Initial 60 ms, Max 1000 ms
Playout-delay Minimum mode is set to default, value 40 ms
Fax nominal 300 ms
Max Redirects = 1, signaling-type = cas,
VAD = enabled, Poor QOV Trap = disabled,
Source Interface = NONE
voice class sip url = system,
voice class sip tel-config url = system,
voice class sip rel1xx = system,
voice class sip anat = system,
voice class sip outbound-proxy = "system",
voice class sip associate registered-number =
                 system,
voice class sip asserted-id system,
voice class sip privacy system
voice class sip e911 = system,
voice class sip history-info = system,
voice class sip reset timer expires 183 = system,
voice class sip pass-thru headers = system,
voice class sip pass-thru content unsupp = system,
voice class sip pass-thru content sdp = system,
voice class sip copy-list = system,
voice class sip g729 annexb-all = system,
voice class sip early-offer forced = system,
voice class sip negotiate cisco = system,
voice class sip block 180 = system,
voice class sip block 183 = system,
voice class sip block 181 = system,
voice class sip preloaded-route = system,
voice class sip random-contact = system,
voice class sip random-request-uri validate = system,
voice class sip call-route p-called-party-id = system,
voice class sip call-route history-info = system,
voice class sip privacy-policy send-always = system,
voice class sip privacy-policy passthru = system,
voice class sip privacy-policy strip history-info = system,
voice class sip privacy-policy strip diversion = system,
voice class sip map resp-code 181 = system,
voice class sip bind control = enabled, 9.42.28.29,
voice class sip bind media = enabled, 9.42.28.29,
voice class sip bandwidth audio = system,
voice class sip bandwidth video = system,
voice class sip encap clear-channel = system,
voice class sip error-code-override options-keepalive failure = system,
voice class sip calltype-video = false
voice class sip registration passthrough = System
voice class sip authenticate redirecting-number  = system,
redirect ip2ip = disabled
local peer = false
probe disabled,
Secure RTP: system (use the global setting)
voice class perm tag = `'
Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Last Disconnect Time = 0.
```

**Note** If the bind address is not configured at the dial-peer, the output of the **show dial-peer voice** command remains the same except for the values of the **voice class sip bind control** and **voice class sip bind media**, which display “system”, indicating that the bind is configured at the global level.

## Troubleshooting Tips

For troubleshooting tips and a list of important debug commands, see *Verifying and Troubleshooting SIP Features*.

# Configuration Examples for SIP Bind Features

This section provides the following configuration examples:

- Example: Verifying the bind Command, page 16

## Example: Verifying the bind Command

This sample output shows that bind is enabled on router 172.18.192.204:

```
Router# show running-config

Building configuration...

Current configuration : 2791 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
ip subnet-zero
ip ftp source-interface Ethernet0
!
voice service voip
 sip
  bind control 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
!
voice-port 1/1/1
no supervisory disconnect lcfo
!
```

```
dial-peer voice 1 pots
application session
destination-pattern 5550111
port 1/1/1
!
dial-peer voice 29 voip
application session
destination-pattern 5550133
session protocol sipv2
session target ipv4:172.18.200.33
codec g711ulaw
!
gateway
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

# Additional References

## Related Documents

| Related Topic | Document Title |
|---|---|
| SIP Roadmap | *SIP Features Roadmap* |
| SIP Overview | *Overview of SIP* |
| Cisco IOS commands | *Cisco IOS Master Commands List, All Releases* |
| Voice commands | *Cisco IOS Voice Command Reference* |

## Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

## MIBs

| MIB | MIBs Link |
|---|---|
| CISCO-SIP-UA-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

# RFCs

| RFC | Title |
|---|---|
| RFC 2543 | SIP: Session Initiation Protocol |
| RFC 2806 | URLs for Telephone Calls |

# 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.<br>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.<br>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 |

# Feature Information for SIP Bind Features

Table 5 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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.

**Note** Table 5 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.

*Table 5 Feature Information for SIP Bind Features*

| Feature Name | Releases | Feature Information |
|---|---|---|
| SIP Gateway Support for the bind Command | 12.2(2)XB<br>12.2(2)XB2<br>12.2(8)T<br>12.2(11)T<br>12.3(4)T | The SIP Gateway Support for the **bind** command feature allows you to configure the source IP address of signaling packets and media packets.<br>In 12.2(2)XB, this feature was introduced.<br>In 12.3(4)T, this feature was expanded to provide the flexibility to specify different source interfaces for signaling and media, and allow network administrators a finer granularity of control on the network interfaces used for voice traffic.<br>The following sections provide information about this feature:<br>• Information About SIP Bind Features, page 2<br>• How to Configure SIP Bind Features, page 8<br>The following commands were introduced or modified: **bind**, **show dial-peer voice**, **show ip sockets**, **show sip-ua connections**, **show sip-ua status**, **voice-class sip bind**. |
| Support Ability to Configure Source IP Address for Signaling and Media per SIP Trunk | 15.1(2)T | This feature allows you to configure a separate source IP address per SIP trunk. This source IP address is embedded in all SIP signaling and media packets that traverse the SIP trunk. This feature enables service providers for better profiling and billing policies. It also enables greater security for enterprises by the use of distinct IP addresses within and outside the enterprise domain.<br>The following section provides information about this feature:<br>• Setting the Bind Command at the Dial-peer Level, page 10<br>The following command was introduced or modified: **voice-class sip bind**. |