SIP Binding

Overview

The SIP Binding feature enables you to configure a source IP address for signaling packets and media packets.

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.

Note All Cisco Unified Border Element (CUBE) Enterprise deployments must have signaling and media bind statements specified at the dial-peer or voice class tenant level. For Voice class tenants, you must apply tenants to dial-peers used for CUBE call flows if these dial-peers do not have bind statements specified.

Feature Information

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

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

Table 1: Feature Information for SIP Binding

Feature Name	Releases	Feature Information
Support of Live Binding at dial-peers.	Cisco IOS XE Amsterdam 17.3.1	This feature allows you to either change or add binding on a dial-peer that does not have any active calls, while other dial-peers with the same binding have active calls. The following command was introduced or modified: **voice-class sip bind all**.

Benefits of SIP Binding

- 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 define specific interface for both signaling and media traffic. 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 Quality of Service (QoS) to be monitored.

Source Address

The order of preference for retrieving the SIP signaling and media source address for inbound and outbound calls is as follows:

- Bind configuration at dial peer level
- Bind configuration at tentants
- Bind configuration at global level

The table below describes the state of the system when the **bind** command is applied in the global or dial peer level:

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

Table 2: State of the Interface for the bind Command

Interface State	Result Using Bind Command
Shut down With or without active calls	TCP, TLS, and User Datagram Protocol (UDP) socket listeners are initially closed. (Socket listeners receive datagrams that are addressed to the socket.) Then the sockets are opened to listen to any IP address. If the outgoing gateway has the **bind** command that is 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 dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages.
No shut down No active calls	TCP, TLS, and UDP socket listeners are initially closed. (Socket listeners receive datagrams that are 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. The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages.
No shut down Active calls	TCP, TLS, and UDP socket listeners are initially closed. Then the sockets are opened to listen to any IP address. The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages.
Bound-interface IP address is removed.	TCP, TLS, and UDP socket listeners are initially closed. 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. A message stating that the IP address has been deleted from the SIP bound interface is printed. If the outgoing gateway has the **bind** command that is 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 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 the interface layer is down.	TCP, TLS, 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. The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages.

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. If the bind interface is shut down, 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 if 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 that is applied at the dial peer level can be modified only in the following situations:

Voice Media Stream Processing

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. The table below 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.

Interface State	bind Command	Result Using bind Command
With active calls	**bind all** or **bind control bind media**	Global Configuration: Blocks the command, and the following error message appears: • Error: You cannot change the interface binding for a dial-peer that is processing live traffic.
	bind all or **bind control** or **bind media**	Dial-peer Configuration: You cannot apply **bind** or **no bind** command to a dial-peer that is processing active calls. Blocks the command, and the following error message appears: • Error: You cannot change the interface binding for a dial-peer that is processing live traffic.

Consider the following scenarios for attaching a tenant to a dial-peer that is processing active calls:

- You can attach a tenant to a dial-peer, when the dial-peer has **bind** (**bind control** or **bind all**) command enabled.
- You cannot attach a tenant to a dial-peer, when the dial-peer has **no bind** or **bind media** command that is enabled and the tenant has **bind control** or **bind all** command enabled.

Consider the following scenarios for changing bind configuration on a tenant, when the tentant is attached to a dial-peer that is processing active calls:

- You can change the bind configuration on tenant, when the associated dial-peer has **bind** (**bind control** or **bind all**) command enabled. Because the dial-peer bind configuration takes precedence over the tenant bind configuration.
- You cannot change the bind configuration on tenant, when the associated dial-peer has **no bind** or **bind media** command that is enabled and the tenant has **bind control** or **bind all** command enabled.

The **bind all** and **bind control** commands perform different functions based on the state of the interface.

Note The **bind all** command applies to global and dial peer. The table below 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 With or without active calls	TCP, TLS, and UDP socket listeners are initially closed. (Socket listeners receive datagrams that are addressed to the socket.) Then the sockets are opened to listen to any IP address. If the outgoing gateway has the **bind** command that is 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 dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages.
Not shut down Without active calls	TCP, TLS, 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 that are destined for the bound address only. The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages.
Not shut down With active calls	TCP, TLS, and UDP socket listeners are initially closed. Then the sockets are opened to listen to any IP address. 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. Then the sockets are opened to listen to any address because the IP address is removed. A message is printed that states the IP address has been deleted from the bound SIP interface. If the outgoing gateway has the **bind** command that is 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 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 the interface layer goes down.	TCP, TLS, 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 interfaces that are not shut down. The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages.

Interface State	Result Using bind all or bind control Commands
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. 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. 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.

Configure SIP Binding

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-addressmask* [**secondary**]
5. **exit**
6. Use one of the following commands to configure SIP binding:
   - **bind** {**control** | **all**} **source-interface** *interface-id* [**ipv6-address** *ipv6-address*] in SIP configuration mode.
   - **bind media** {**source-address ipv4** *ipv4-address* | **source-interface** *interface-id* [**ipv6-address** *ipv6-address*]} in SIP configuration mode.
   - **voice-class sip bind media** {**source-address ipv4** *ipv4-address* | **source-interface** *interface-id* [**ipv6-address** *ipv6-address*]} in dial-peer configuration mode.
7. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface fastethernet0/0`	Configures an interface type and enters the interface configuration mode. • *type number* —Type of interface to be configured and the port, connector, or interface card number.
Step 4	**ip address** *ip-addressmask* [**secondary**] **Example:** `Router(config-if)# ip address 192.168.200.33 255.255.255.0`	Configures a primary or secondary IP address for an interface. **Note** Secondary IP address on an interface with SIP binding is not supported for CUBE.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Step 6	Use one of the following commands to configure SIP binding:
	• **bind** {**control** | **all**} **source-interface** *interface-id* [**ipv6-address** *ipv6-address*] in SIP configuration mode.
	• **bind media** {**source-address ipv4** *ipv4-address* | **source-interface** *interface-id* [**ipv6-address** *ipv6-address*]} in SIP configuration mode.
	• **voice-class sip bind media** {**source-address ipv4** *ipv4-address* | **source-interface** *interface-id* [**ipv6-address** *ipv6-address*]} in dial-peer configuration mode.
	Example:
	SIP binding in SIP configuration mode:
	`Device(config)# voice service voip`
	`Device(conf-voi-serv)# sip`
	`Device(conf-serv-sip)# bind control source-interface FastEthernet0/0`
	`Device(conf-serv-sip)# exit`
	`Device(config)# voice service voip`
	`Device(conf-voi-serv)# sip`
	`Device(conf-serv-sip)# bind media source-address ipv4 172.18.192.204`
	`Device(conf-serv-sip)# exit`
	Example:
	SIP binding in dial-peer configuration mode:
	`Device(config)# dial-peer voice 100 voip`
	`Device(config-dial-peer)# session protocol sipv2`
	`Device(config-dial-peer)# voice-class sip bind`
		Sets a source interface for signaling and media packets. The binding applies to the specified interfaces only. SIP must be configured globally or at a dial peer level.
		• **control** —Binds signaling packets.
		• **media** —Binds media packets.
		• **all** —Binds signaling and media packets.
		• **source-address**—Binds media packets directly to an IP address.
		• **ipv4** *ipv4-address*—Configures the IPv4 address.
		• **source interface** *interface-id* —Type of interface and its ID.
		• **ipv6-address** *ipv6-address* —Configures the IPv6 address. Ensure that the IPv6 address is applied to an interface.

	Command or Action	Purpose
	control source-interface fastethernet0/0 Device(config-dial-peer)# exit Device(config)# dial-peer voice 100 voip Device(config-dial-peer)# session protocol sipv2 Device(config-dial-peer)# voice-class sip bind media source-address ipv4 172.18.192.204 Device(config-dial-peer)# exit	
Step 7	**end**	Exits to privileged EXEC mode.

Verify SIP Binding

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:

Example:

```
Device# 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 to enable bind.

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

Example:

```
Device# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): 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.

Example:

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

Example:

```
Device# 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.

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 control and bind media, those are the commands that appear in the show running-config command output.