

signal through srv version

- signal, on page 3
- signal did, on page 7
- signal keepalive, on page 8
- signal pattern, on page 10
- signal sequence oos, on page 13
- signal timing idle suppress-voice, on page 15
- signal timing oos, on page 18
- signal timing oos restart, on page 20
- signal timing oos standby, on page 22
- signal timing oos suppress-all, on page 24
- signal timing oos suppress-voice, on page 26
- signal timing oos timeout, on page 28
- signaling forward, on page 30
- signaling forward (dial peer), on page 35
- signal-type, on page 40
- silent-discard untrusted, on page 42
- silent-fax, on page 43
- sip, on page 44
- sip-header, on page 46
- sip-header SIP-StatusLine, on page 47
- sip-server, on page 48
- sip-ua, on page 50
- sni send (voice class), on page 53
- snmp enable peer-trap dscp-profile, on page 54
- snmp enable peer-trap poor-qov, on page 55
- snmp-server enable traps voice (DSCP profile), on page 56
- soft-offhook, on page 57
- source-address (uc-wsapi), on page 59
- source carrier-id, on page 60
- source filter, on page 61
- source-ip (media-profile), on page 62
- source trunk-group-label, on page 63
- speed dial, on page 64

- srtp (dial peer), on page 67
- srtp (voice), on page 69
- srtp-auth, on page 71
- srtp-crypto, on page 73
- srtp negotiate, on page 75
- srv version, on page 77

signal

To specify the type of signaling for a voice port, use the **signal** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

Foreign Exchange Office (FXO) and Foreign Exchange Station (FXS) Voice Ports
signal {**groundstart** | **loopstart** [**live-feed**]}
no signal {**groundstart** | **loopstart**}

Ear and mouth (EandM) Voice Ports
signal {**delay-dial** | **immediate** | **lmr** | **wink-start**}
no signal {**delay-dial** | **immediate** | **lmr** | **wink-start**}

Centralized Automatic Message Accounting (CAMA) Ports
signal {**cama** {**kp-0-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st** | **kp-2-st** | **kp-npd-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st**} | **groundstart** | **loopstart**}
no signal {**cama** {**kp-0-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st** | **kp-2-st** | **kp-npd-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st**} | **groundstart** | **loopstart**}

Syntax Description

groundstart	Specifies the use of groundstart signaling. Used for FXO and FXS interfaces. Groundstart signaling allows both sides of a connection to place a call and to hang up. **Note** The CAMA version of this keyword is **groundstart**. Both forms operate identically.
loopstart	Specifies the use of loop start signaling. Used for FXO and FXS interfaces. With loopstart signaling, only one side of a connection can hang up. This is the default setting for FXO and FXS voice ports. **Note** The CAMA version of this keyword is **loopstart**. Both forms operate identically.
live-feed	(Optional) Enables an MOH audio stream from a live feed to be directly connected to the router through an FXO port.
delay-dial	The calling side seizes the line by going off-hook on its E-lead. After a timing interval, the calling side looks at the supervision from the called side. If the supervision is on-hook, the calling side starts sending information as dual tone multifrequency (DTMF) digits; otherwise, the calling side waits until the called side goes on-hook and then starts sending address information. Used for E&M tie trunk interfaces.
immediate	The calling side seizes the line by going off-hook on its E-lead and sends address information as DTMF digits. Used for E&M tie trunk interfaces.

lmr	Specifies the use of Land Mobile Radio signaling.
wink-start	The calling side seizes the line by going off-hook on its E-lead then waits for a short off-hook "wink" indication on its M-lead from the called side before sending address information as DTMF digits. Used for E&M tie trunk interfaces. This is the default setting for E&M voice ports.
cama	Selects and configures the port for 911 calls.
kp-0-npa-nxx-xxxx-st	10-digit transmission. The E.164 number is fully transmitted.
kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st	Supports CAMA Signaling with ANI/Pseudo ANI (PANI).
kp-0-nxx-xxxx-st	7-digit automatic number identification (ANI) transmission. The Numbering Plan Area (NPA) or area code is implied by the trunk group and is not transmitted.
kp-2-st	Default transmission when the CAMA trunk cannot get a corresponding Numbering Plan Digit (NPD) digit in the lookup table, or when the calling number is fewer than ten digits in length. (NPA digits are not available.)
kp-npd-nxx-xxxx-st	8-digit ANI transmission, where the NPD is a single multifrequency (MF) digit that is expanded into the NPA. The NPD table is preprogrammed in the sending and receiving equipment (on each end of the MF trunk); for example: 0 = 415, 1 = 510, 2 = 650, 3 = 916 05550100 = (415) 555-0100, 15550100 = (510) 555-0100, and so on. NPD range is from 0 to 3.

Command Default

FXO and FXS interfaces: **loopstart** E&M interfaces: **wink-start** CAMA interfaces: **loopstart**

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(11)T	This command was modified to support ANI transmission.
12.3(4)XD	The **lmr** keyword was added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(9)T	The kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st keyword was added to support CAMA Signaling with ANI/Pseudo ANI (PANI).
12.4(11)XJ	The **live-feed** keyword was added.

Release	Modification
12.4(15)T	The **live-feed** keyword was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command applies to analog voice ports only. A voice port must be shut down and then activated before the configured values take effect.

For an E&M voice port, this command changes only the signal value for the selected voice port.

For an FXO or FXS voice port, this command changes the signal value for both voice ports on a voice port module (VPM). If you change the signal type for an FXO voice port on Cisco 3600 series routers, you need to move the appropriate jumper in the voice interface card of the voice network module. For more information about the physical characteristics of the voice network module, see the installation documentation that came with your voice network module.

Some PBXs miss initial digits if the E&M voice port is configured for immediate start signaling. Immediate start signaling should be used for dial pulse outpulsing only and only on circuits for which the far end is configured to accept digits within a few milliseconds of seizure. Delay dial signaling, which is intended for use on trunks and not lines, relies on the far end to return an off-hook indication on its M-lead as soon as the circuit is seized. When a receiver is attached, the far end removes the off-hook indication to indicate that it is ready to receive digits. Delay dial must be configured on both ends to work properly. Some non-Cisco devices have a limited number of DTMF receivers. This type of equipment must delay the calling side until a DTMF receiver is available.

To specify which VIC-2CAMA ports are designated as dedicated CAMA ports for emergency 911 calls, use the **signal cama** command. No two service areas in the existing North American telephony infrastructure supporting E911 calls have identical service implementations, and many of the factors that drive the design of emergency call handling are matters of local policy and therefore outside the scope of this document. Local policy determines which ANI format is appropriate for the specified Physical Service Access Point (PSAP) location.

The following four types of ANI transmittal schemes are based on the actual number of digits transmitted toward the E911 tandem. In each instance, the actual calling number is proceeded with a key pulse (KP) followed by an information (I) field or a NPD, which is then followed by the ANI calling number, and finally is followed by a start pulse (ST), STP, ST2P, or ST3P, depending on the trunk group type in the PSTN and the traffic mix carried.

The information field is one or two digits, depending on how the circuit was ordered originally. For one-digit information fields, a value of 0 indicates that the calling number is available. A value of 1 indicates that the calling number is not available. A value of 2 indicates an ANI failure. For a complete list of values for two-digit information fields, see *SR-2275: Telcordia Notes on the Networks* at www.telcordia.com .

- 7-digit transmission (**kp 0 nxx xxxx st**):

The calling phone number is transmitted, and the NPA is implied by the trunk group and not transmitted.

- 8-digit transmission (**KP npd nxx xxxx st**) :

The I field consists of single-digit NPD-to-NPA mapping. When the calling party number of 415-555-0122 places a 911 call, and the Cisco 2600 series or Cisco 3600 series has an NPD (0)-to-NPA (415) mapping, the NPA signaling format is received by the selective router at the central office (CO).

Note NPD values greater than 3 are reserved for signifying error conditions.

- 10-digit transmission (**kp 0 npa nxx xxxx st)**

The E.164 number is fully transmitted.

- 20-digit transmission (**kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st**):

Twenty digits support (two 10 digit numbers) on FGD-OS in the following format, KP+II+10 digit ANI+ST+KP+7/10 digit PANI+ ST

- kp-2-st transmission (**kp-2-st**):

kp-2-st transmission is used if the PBX is unable to out-pulse the ANI. If the ANI received by the Cisco router is not as per configured values, kp-2-st is transmitted. For example, if the voice port is configured for out-pulsing a ten-digit ANI and the 911 call it receives has a seven-digit calling party number, the router transmits kp-2-st.

Note Emergency 911 calls are not rejected for an ANI mismatch. The call establishes a voice path. The E911 network, however, does not receive the ANI.

Examples

The following example configures groundstart signaling on the Cisco 3600 series as the signaling type for a voice port, which means that both sides of a connection can place a call and hang up:

```
voice-port 1/1/1
 signal groundstart
```

The following example configures a ten-digit ANI transmission:

```
Router(config)#
voice-port 1/0/0
Router(config-voiceport)# signal cama kp-0-npa-nxx-xxxx-st
```

The following example configures 20-digit CAMA Signaling with ANI/Pseudo ANI:

```
Router(config-voiceport)# signal cama KP-0-NPA-NXX-XXXX-ST-KP-YYY-YYY-YYYY-ST
```

Related Commands

Command	Description
ani mapping	Preprograms the NPA, or area code, into a single MF digit.

signal did

To enable direct inward dialing (DID) on a voice port, use the **signal did command in**voice-port configuration mode. To disable DID and reset to loop-start signaling, use the **no** form of this command.

signal did { **immediate-start** | **wink-start** | **delay-dial** }
no signal did

Syntax Description

immediate -start	Enables immediate-start signaling on the DID voice port.
wink -start	Enables wink-start signaling on the DID voice port.
delay -start	Enables delay-dial signaling on the DID voice port.

Command Default

No default behavior or values

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco IAD2420 series.

Examples

The following example configures a voice port with immediate-start signaling enabled:

```
Router# voice-port 1/17
Router (config-voiceport)# signal did immediate-start
```

signal keepalive

To configure the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks, use the **signal keepalive** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal keepalive {*seconds* | **disabled**}
no signal keepalive {*seconds* | **disabled**}

Syntax Description

seconds	Keepalive signaling packet interval, in seconds. Range is from 1 to 65535. Default is 5 seconds.
disabled	Specifies that no keepalive signals are sent.

Command Default

seconds : 5 seconds

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.3(7)T	The **disabled** keyword was added.

Usage Guidelines

Before configuring the keepalive signaling interval, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer using the **voice-class permanent** (dial-peer) command.

To avoid sending keepalive signals to a multicasting network with no specified destination, we recommend that you use the **disabled**keyword when configuring this command for use in networks that use connection trunk connections and multicasting.

Examples

The following example shows the keepalive signaling interval set to 3 seconds for voice class 10:

```
voice class permanent 10
 signal keepalive 3
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies a dial-peer type.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.

Command	Description
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal pattern

To define the ABCD bit patterns that identify the idle and out-of-service (OOS) states for Cisco trunks and FRF.11 trunks, use the **signal pattern** command in voice-class configuration mode. To remove the patterns from the voice class, use the **no** form of this command.

signal pattern {**idle receive** | **idle transmit** | **oos receive** | **oos transmit**} *bit-pattern*
no signal pattern {**idle receive** | **idle transmit** | **oos receive** | **oos transmit**} *bit-pattern*

Syntax Description

idle receive	Signaling pattern for identifying an idle message from the network. Also defines the idle signaling pattern to be sent to the PBX if the network trunk is out of service and the **signal sequence oos idle-only** or **signal sequence oos both** command is configured.
idle transmit	Signaling pattern for identifying an idle message from the PBX.
oos receive	OOS signaling pattern to be sent to the PBX if the network trunk is out of service and the **signal sequence oos oos-only** or **signal sequence oos both** command is configured.
oos transmit	Signaling pattern for identifying an OOS message from the PBX.
bit -pattern	ABCD bit pattern. Range is from 0000 to 1111.

Command Default

idle receive	Near-end E&M: 0000 (for T1) or 0001 (for E1) Near-end FXO loop start: 0101 Near-end FXO ground start: 1111 Near-end FXS: 0101 Near-end MELCAS: 1101
idle transmit	Near-end E&M: 0000 Near-end FXO: 0101 Near-end FXS loop start: 0101 Near-end FXS ground start: 1111 Near-end MELCAS: 1101
oos receive	Near-end E&M: 1111 Near-end FXO loop start: 1111 Near-end FXO ground start: 0000 Near-end FXS loop start: 1111 Near-end FXS ground start: 0101 Near-end MELCAS: 1111
oos transmit	No default signaling pattern is defined.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	Default signaling patterns were defined.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring the signaling pattern, you must use the **voice-class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you define the voice class, you assign it to a dial peer.

Idle Patterns

An idle state is generated if the router detects an idle signaling pattern coming from either direction. If an idle pattern is configured for only one direction (transmit or receive), an idle state can be detected only in the configured direction. Therefore, you should normally enter both the **idle receive** and the **idle transmit** keywords.

To suppress voice packets whenever the transmit or receive trunk is in the idle state, use the **idle receive** and **idle transmit** keywords in conjunction with the **signal timing idle suppress-voice** command.

OOS Patterns

An OOS state is generated differently in each direction under the following conditions:

- If the router detects an **oos transmit** signaling pattern sent from the PBX, the router transmits the **oos transmit** signaling pattern to the network.
- If the **signal timing oos timeout** timer expires and the router receives no signaling packets from the network (network is OOS), the router sends an **oos receive** signaling pattern to the PBX. (The **oos receive** pattern is not matched against the signaling packets received from the network; the receive packets indicate an OOS condition directly by setting the AIS alarm indication bit in the packet.)

To suppress voice packets whenever the transmit or receive trunk is in the OOS state, use the **oos receive** and **oos transmit**keywords in conjunction with the **signal timing oos suppress-voice** command.

To suppress voice and signaling packets whenever the transmit or receive trunk is in the OOS state, use the **oos receive** and **oos transmit** keywords in conjunction with the **signal timing oos suppress-all** command.

PBX Busyout

To "busy out" a PBX if the network connection fails, set the **oos receive** pattern to match the seized state (busy), and set the **signal timing oos** timeout value. When the timeout value expires and no signaling packets are received, the router sends the **oos receive** pattern to the PBX.

Use the busy seized pattern only if the PBX does not have a specified pattern for indicating an OOS state. If the PBX has a specific OOS pattern, use that pattern instead.

Examples

The following example, beginning in global configuration mode, configures the signaling bit pattern for the idle receive and transmit states:

```
voice class permanent 10
 signal keepalive 3
 signal pattern idle receive 0101
 signal pattern idle transmit 0101
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

The following example, beginning in global configuration mode, configures the signaling bit pattern for the out-of-service receive and transmit states:

```
voice class permanent 10
 signal keepalive 3
 signal pattern oos receive 0001
```

```
 signal pattern oos transmit 0001
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

The following example restores default signaling bit patterns for the receive and transmit idle states:

```
voice class permanent 10
 signal keepalive 3
 signal timing idle suppress-voice
 no signal pattern idle receive
 no signal pattern idle transmit
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

The following example configures nondefault signaling bit patterns for the receive and transmit out-of-service states:

```
voice class permanent 10
 signal keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies a dial-peer type.
signal timing idle suppress-voice	Specifies the length of time before voice traffic is stopped after a trunk goes into the idle state.
signal timing oos	Configures the signal timing parameter for the OOS call state.
signal timing oos standby	Specifies that a secondary port return to its initial standby state after the trunk has been OOS for a specified time.
signal timing oos suppress-all	Stops sending voice and signaling packets to the network if a transmit OOS signaling pattern id detected from the PBX for a specified time.
signal timing oos suppress-voice	Stops sending voice packets to the network if a transmit OOS signaling pattern is detected from the PBX for a specified time.
signal timing oos timeout	Changes the delay time between the loss of signaling packets from the network and the start time for the OOS state.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal sequence oos

To specify which signaling pattern is sent to the PBX when the far-end keepalive message is lost or an alarm indication signal (AIS) is received from the far end, use the **signal sequence oos** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal sequence oos {**no-action** | **idle-only** | **oos-only** | **both**}
no signal sequence oos

Syntax Description

no -action	No signaling pattern is sent.
idle -only	Only the idle signaling pattern is sent.
oos -only	Only the out-of-service (OOS) signaling pattern is sent.
both	Both idle and OOS signaling patterns are sent. This is the default value.

Command Default

Both idle and OOS signaling patterns are sent.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring the idle or OOS signaling patterns to be sent, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

Use the **signal sequence oos** command to specify which signaling pattern) to send. Use the **signal pattern idle receive** or the **signal pattern oos receive** command to define the bit patterns of the signaling patterns if other than the defaults.

Examples

The following example, beginning in global configuration mode, defines voice class 10, sets the **signal sequence oos**command to send only the idle signal pattern to the PBX, and applies the voice class configuration to VoFR dial peer 100.

```
voice-class permanent 10
 signal-keepalive 3
 signal sequence oos idle-only
 signal timing idle suppress-voice
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
 signal-type transparent
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies a dial-peer type.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Specifies the length of time before the router stops sending voice packets after a trunk goes into the idle state.
signal timing oos	Specifies that a permanent voice connection be torn down and restarted after the trunk has been OOS for a specified time.
signal timing oos standby	Specifies that a port return to its initial standby state after the trunk has been OOS for a specified time.
signal timing oos suppress-all	Configures the router or concentrator to stop sending voice and signaling packets to the network if it detects an OOS signaling pattern from the PBX for a specified time.
signal timing oos suppress-voice	Configures the router or concentrator to stop sending voice packets to the network if it detects a transmit OOS signaling pattern from the PBX for a specified time.
signal timing oos timeout	Changes the delay time between the loss of signaling packets from the network and the start time for the OOS state.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing idle suppress-voice

To configure the signal timing parameter for the idle state of a call, use the s**ignal timing idle suppress-voice** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing idle suppress-voice *seconds* [**resume-voice** [*milliseconds*]]
no signal timing idle suppress-voice *seconds* [**resume-voice** [*milliseconds*]]

Syntax Description

seconds	Duration of the idle state, in seconds, before the voice traffic is stopped. Range is from 0 to 65535.
resume-voice	(Optional) Sets a timer that controls the delay between when trunk activity is detected and when active packetization of voice resumes.
milliseconds	(Optional) Duration of the delay, in milliseconds (ms), for the resume-voice timer. Range is from 40 to 5000. Default is 500 ms.

Command Default

No signal timing idle suppress-voice timer is configured.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 platform.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was modified to simplify the configuration process.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.4(15)T10	This command was modified to add the **resume-voice** *milliseconds* option.

Usage Guidelines

Before configuring the signal timing idle suppress-voice timer, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer.

The **signal timing idle suppress-voice**command is used when the **signal-type** command is set to **transparent** in the dial peer for the Cisco trunk or FRF.11 trunk connection. The router stops sending voice packets when the timer expires. Signaling packets are still sent.

To detect an idle trunk state, the router or concentrator monitors both transmit and receive signaling for the idle transmit and idle receive signaling patterns. These can be configured by the **signal pattern idle transmit** or **signal pattern idle receive** command, or they can be the defaults. The default idle receive pattern is the idle pattern of the local voice port. The default idle transmit pattern is the idle pattern of the far-end voice port.

In some circumstances, the default delay of 500 ms between the detection of incoming seizure and the opening of the audio path may cause a timing issue.

If, during this delay of 500 ms, the near-end originating PBX has already received the acknowledgement from the far-end PBX to begin playing out digits and the audio path is not yet open, the first Dual Tone Multi-Frequency (DTMF) digit might be lost over the permanent trunk.

This loss of the first DTMF digit can occur if a Cisco voice gateway has the following trunk conditioning setting:

```
!
voice class permanent 1
signal pattern idle transmit 0000
signal pattern idle receive 0000
signal pattern oos transmit 1111
signal pattern oos receive 1111
signal timing idle suppress-voice 10
!
```

The **resume-voice** *milliseconds* option has been added in Release 12.4(15)T10 to modify the delay timer and reduce the wait time. We recommend that you specify a delay of less than 500 ms to avoid the loss of any digits due to the possible discrepancy between the detection of incoming seizure and the opening of the audio path.

The output of the **show voice trunk-conditioning supervisory** command has been modified in Release 12.4(15)T10 to report values for the **suppress-voice** and **resume-voice** keywords (of the **signal timing idle suppress-voice** command) as the "idle = *seconds* " and "idle_off = *milliseconds* " fields, respectively.

Examples

The following example, beginning in global configuration mode, sets the signal timing idle suppress-voice timer to 5 seconds for the idle state on voice class 10:

```
voice class permanent 10
 signal keepalive 3
 signal pattern idle receive 0101
 signal pattern idle transmit 0101
 signal timing idle suppress-voice 5
 exit
 dial-peer voice 100 vofr
 voice-class permanent 10
 signal-type transparent
```

The following example defines voice class 10, sets the idle detection time to 5 seconds, configures the trunk to use the default transmit and receive idle signal patterns, and applies the voice class configuration to VoFR dial peer 100:

```
voice class permanent 10
 signal keepalive 3
 signal timing idle suppress-voice 5
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
 signal-type transparent
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
show voice trunk-conditioning supervisory	Displays the status of trunk supervision and configuration parameters for a voice port.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and OOS states for Cisco trunks and FRF.11 trunks.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent (dial peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos

To configure the signal timing parameter for the out-of-service (OOS) state of the call, use the **signal timing oos**command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos { **restart** | **standby** | **suppress-all** | **suppress-voice** | **timeout** } *seconds*
no signal timing oos { **restart** | **standby** | **suppress-all** | **suppress-voice** | **timeout** } *seconds*

Syntax Description

restart	If no signaling packets are received for this period, the permanent voice connection is torn down and an attempt to achieve reconnection is made.
standby	If no signaling packets are received for this period, a secondary port returns to its initial standby state. This option applies only to secondary ports (ports configured using the **connection trunk** *number* **answer-mode** command).
suppress -all	If the transmit OOS pattern (from the PBX to the network) matches for this period of time, the router stops sending all packets to the network.
suppress -voice	If the transmit OOS pattern (from the PBX to the network) matches for this period of time, the router stops sending voice packets to the network. signaling packets continue to be sent with the alarm indication set (AIS).
timeout	If no signaling packets are received for this period of time, the router sends the configured receive OOS pattern to the PBX. Also, the router stops sending voice packets to the network. Use this option to perform busyout to the PBX.
seconds	Duration, in seconds, for the above settings. Range is from 0 to 65535.

Command Default

No signal timing OOS pattern parameters are configured.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(4)T	This command was introduced.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer.

You can enter several values for this command. However, the **suppress-all** and **suppress-voice** options are mutually exclusive.

Examples

The following example, beginning in global configuration mode, configures the signal timeout parameter for the OOS state on voice class 10. The **signal timing oos timeout**command is set to 60 seconds.

```
voice-class permanent 10
```

```
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of the call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos restart

To specify that a permanent voice connection be torn down and restarted after the trunk has been out-of-service (OOS) for a specified time, use the **signal timing oos restart** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos restart *seconds*
no signal timing oos restart

Syntax Description

seconds	Delay duration, in seconds, for the restart attempt. Range is from 0 to 65535. There is no default.

Command Default

No restart attempt is made if the trunk becomes OOS.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. You then assign the voice class to a dial peer.

The **signal timing oos restart** command is valid only if the **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos restart** command does not start until the trunk is OOS.

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS **timeout** time to 60 seconds and sets the **restart** time to 30 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 signal timing oos restart 30
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos standby

To configure a secondary port to return to its initial standby state after the trunk has been out-of-service (OOS) for a specified time, use the **signal timing oos standby** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos standby *seconds*
no signal timing oos standby

Syntax Description

seconds	Delay duration, in seconds. If no signaling packets are received for this period, the secondary port returns to its initial standby state. Range is from 0 to 65535. There is no default.

Command Default

The secondary port does not return to its standby state if the trunk becomes OOS.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent**command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

If no signaling packets are received for the specified delay period, the secondary port returns to its initial standby state. The **signal timing oos standby** command is valid only if both of the following conditions are true:

- The **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos standby** command does not start until the trunk is OOS.
- The voice port is configured as a secondary port with the **connection trunk** *digits* **answer-mode** command.

Examples

The following example, beginning in global configuration mode, creates a voice port as a secondary voice port, creates voice class 10, sets the OOS **timeout** time to 60 seconds, and sets the return-to-**standby** time to 120 seconds:

```
4351-Router #signal timing oos standby ?
  <0-65535>  Time in seconds
4351-Router #signal timing oos standby
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos suppress-all

To configure the router or concentrator to stop sending voice and signaling packets to the network if it detects a transmit out-of-service (OOS) signaling pattern from the PBX for a specified time, use the **signal timing oos suppress-all** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos suppress-all *seconds*
no signal timing oos suppress-all

Syntax Description

seconds	Delay duration, in seconds, before packet transmission is stopped. Range is from 0 to 65535. There is no default.

Command Default

The router or concentrator does not stop sending packets to the network if it detects a transmit OOS signaling pattern from the PBX.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

The **signal timing oos suppress-all** command is valid only if you configure an OOS transmit signaling pattern with the **signal pattern oos transmit** command. (There is no default **oos transmit** signaling pattern.)

The **signal timing oos suppress-all** command is valid whether or not the **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos suppress-all** command starts immediately when the OOS transmit signaling pattern is matched.

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS **timeout** time to 60 seconds, and sets the packet suppression time to 60 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 signal timing oos suppress-all 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos suppress-voice

To configure the router or concentrator to stop sending voice packets to the network if it detects a transmit out-of-service (OOS) signaling pattern from the PBX for a specified time, use the **signal timing oos suppress-voice** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos suppress-voice *seconds*
no signal timing oos suppress-voice

Syntax Description

seconds	Delay duration, in seconds, before voice-packet transmission is stopped. Range is from 0 to 65535. There is no default.

Command Default

The router or concentrator does not stop sending voice packets to the network if it detects a transmit OOS signaling pattern from the PBX.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

The **signal timing oos suppress-voice** command is valid only if you configure an OOS transmit signaling pattern with the **signal pattern oos transmit** command. (There is no default **oos transmit** signaling pattern.)

The **signal timing oos suppress-voice** s command is valid whether or not the **signal timing oos timeout**command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos suppress-voice** command starts immediately when the OOS transmit signaling pattern is matched.

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS **timeout** time to 60 seconds, and sets the packet suppression time to 60 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 signal timing oos suppress-voice 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos timeout

To change the delay time between the loss of signaling packets from the network and the start time for the out-of-service (OOS) state, use the **signal timing oos timeout** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos timeout [*seconds* | **disabled**]
no signal timing oos timeout

Syntax Description

seconds	(Optional) Delay duration, in seconds, between the loss of signaling packets and the beginning of the OOS state. Range is from 1 to 65535. Default is 30.
disabled	(Optional) Deactivates the detection of packet loss. If no signaling packets are received from the network, the router does not sent an OOS pattern to the PBX and it continues sending voice packets to the network. Use this option to disable busyout to the PBX.

Command Default

No signal timing OOS pattern parameters are configured.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

You can use the **signal timing oos timeout**command to enable busyout to the PBX.

The **signal timing oos timeout**command controls the starting time for the **signal timing oos restart** and **signal timing oos -standby** commands. If this command is entered with the **disabled** keyword, the **signal timing oos restart** and **signal timing oos standby** commands are ineffective.

Examples

The following example, beginning in global configuration mode, creates voice class 10 and sets the OOS **timeout** time to 60 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signaling forward

To configure global settings for transparent tunneling of Q-signaling (QSIG), Q.931, H.225, and ISDN User Part (ISUP) messages on a Cisco IOS voice gateway, use the **signaling forward** command in voice service VoIP configuration mode. To return to the default tunneling configuration for a gateway, use the **no** form of this command.

Cisco IOS H.323 Gateways
signaling forward {**conditional** | **none** | **rawmsg** | **unconditional**}
no signaling forward

Cisco IOS SIP Gateways
signaling forward {**none** | **rawmsg** | **unconditional**}
no signaling forward

Syntax Description

conditional	Specifies that tunneling on an H.323 gateway is determined by the target, which is defined using the **session target** command. This is the default setting for H.323 gateways. **Note** The **conditional** keyword is not supported on Session Initiation Protocol (SIP) gateways. Instead, the default setting for SIP gateways is that no tunneling is configured (**none**).
none	Specifies that H.323 and SIP gateways do not forward Generic Transparency Descriptor (GTD), QSIG, or Q.931 payloads to any endpoint in the network. This is the default setting for SIP gateways.
rawmsg	Specifies that H.323 and SIP gateways tunnel H.225, QSIG (application-qsig), or Q.931 raw messages (application-Xq931) only, without GTD.
unconditional	Specifies unconditional tunneling and forwards GTD payload along with the QSIG or Q.931 message body even if the attached external route server has modified it. (The gatekeeper sends its own GTD back to itself.)

Command Default

- **conditional** --messages are forwarded according to the target:
  - Non-Registration, Admission, and Status (RAS) targets--only the original payload (without GTD) is forwarded to the H.323 endpoint.
  - All other targets--GTD payload is forwarded along with the message body.

No transparent tunneling of QSIG or Q.931 messages is configured.

Command Modes

Voice service VoIP configuration (conf-voi-serv)

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Release	Modification
12.3(1)	Support was added for SIP Public Switched Telephone Network (PSTN) transport using Cisco GTD.
12.4(15)XY	Support was added for passing RELEASE and RELEASE COMPLETE messages end to end over SIP using QSIG tunneling on Cisco IOS voice gateways.
12.4(15)XZ	Support was added for Q.931 tunneling over SIP on Cisco IOS voice gateways and tunneling of both QSIG and Q.931 over SIP was extended to the Cisco Unified Border Element (CUBE). **Note** The CUBE is formerly known as the Cisco IOS Session Border Controller (SBC) or the Cisco Multiservice IP-to-IP Gateway.
12.4(20)T	Support was added for QSIG and Q.931 tunneling over SIP on Cisco IOS voice gateways and the CUBE.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

This command is used on H.323 and SIP voice gateways to configure tunneling behavior. Depending on your specific Cisco router, platform, and network, you can use this command to configure tunneling behavior for various messages, such as QSIG, Q.931, H.225, and ISUP messages. To override the global setting for a gateway or to configure tunneling settings on a dial peer, use the **signaling forward** command in dial peer voice configuration mode.

For more specific information about controlling tunneling behavior using the **signaling forward** command, see the information included in the following sections:

QSIG and Q.931 Tunneling

Tunneling of QSIG and Q.931 on H.323 gateways is enabled by default for Cisco IOS gateway platforms supporting the **signaling forward** command. For QSIG and Q.931 tunneling on SIP gateways, however, you must configure at least one interface on both an ingress, or originating gateway (OGW), and an egress, or terminating gateway (TGW).

In addition to signaling forward settings, you must specify QSIG or Q.931 as the central office switch type on the ISDN interface for both the OGW and TGW on a SIP or H.323 network. Use the **isdn switch-type** command to enable and specify the switch type:

- For tunneling QSIG messages, specify the **primary-qsig** switch type.
- For tunneling Q.931 messages, specify any ISDN switch type except **primary-qsig** and **primary-dpness**.



Note Cisco IOS SIP gateways do not support the **primary-dpness** switch type for tunneling of Q.931.

The table below displays QSIG and Q.931 tunneling behavior as determined by gateway voice class and configuration settings.

Table 1: QSIG Tunneling Behavior by Voice Class and Signaling Forward Setting

Signaling Forward Configuration	H.323 Gateway	SIP Gateway
conditional or no specified setting:	Default.	Not supported.
session target *non-ras*	Tunnels GTD payload with QSIG or Q.931 message bodies.	No tunneling.
session target ras	Tunnels only QSIG or Q.931 message bodies.	No tunneling.
none	No tunneling.	No tunneling.
rawmsg	Tunnels QSIG or Q.931 message bodies only.	Tunnels QSIG or Q.931 message bodies only.
unconditional	Tunnels GTD payload along with QSIG or Q.931 message bodies.	Tunnels GTD payload along with QSIG or Q.931 message bodies.

SS7 ISUP and H.225 Tunneling over H.323

ISUP defines the protocol and procedures used to configure, manage, and release trunk circuits that carry voice and data calls over the PSTN. ISUP is used for both ISDN and non-ISDN calls and is reconstructed on the basis of the protocol at the egress side of the network, without any concern for the ISDN or ISUP variant on the ingress side of the network.

When you specify that the ISDN (H.225) or ISUP information be provided in text format, the information can also be used by applications inside the core H.323 network such as, in a route server, which can use certain ISDN and ISUP information for routing decisions. Additionally, transporting ISUP encapsulated in GTD maintains compatibility with the H.323 protocol.

If the target is a RAS target, for a non-GTD signaling payload, the original payload is forwarded. For a GTD signaling payload, the payload is encapsulated in an admission request (ARQ)/disengage request (DRQ) message and sent to the originating gatekeeper. The gatekeeper conveys the payload to the Gatekeeper Transaction Message Protocol (GKTMP) and external route server for a flexible route decision based upon the ISUP GTD parameters. The gateway then conditionally forwards the GTD payload on the basis of the instruction from the route server.

To tunnel the ISUP GTD, you must configure the OGW and TGW to encapsulate SS7 ISUP messages in GTD format.

Note If you specify **primary-qsig** as the **isdn switch-type** setting, you must assign network-side functionality (either at the global or dial-peer level) using the **isdn protocol-emulate** command.

Examples

The following example shows unconditional signal forwarding being set on a global basis, where the GTD payload is tunneled to endpoints over either H.323 or SIP:

```
Router> enable
```

```
Router# configure
 terminal
Router(config)# voice service voip
Router(conf-voi-serv)# signaling forward unconditional
```

The following example is sample output from the **show running-config** command when a router is globally configured with unconditional signal forwarding over SIP:

```
Router# show running-config
Building configuration...
Building configuration...
Current configuration : 2357 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!
!
.
.
!
voice service voip
 signaling forward unconditional
 sip
!
.
.
```

The following example is sample output from the **show running-config** command when a router is globally configured with unconditional signal forwarding over H.323:

```
Router# show running-config
Building configuration...
Current configuration : 4201 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
!
hostname as5300-2
!
no logging buffered
logging rate-limit console 10 except errors
aaa new-model
!
.
.
.
!
voice service voip
 signaling forward unconditional
 h323
!
.
```

.
.

Related Commands

clid network-number	Configures a network number in the router for CLID and uses it as the calling party number.
clid restrict	Prevents the calling party number from being presented by CLID.
clid second-number strip	Prevents the second network number from being sent in the CLID information.
isdn global-disconnect	Specifies setting for allowing passage of Release and Release Complete messages over a voice network.
isdn protocol-emulate	Enables emulation of the network side of an ISDN configuration for a PRI Net5 or PRI NTT switch type.
isdn protocol-emulate (dial)	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI to emulate NT (network) or TE (user) functionality.
isdn switch-type (BRI)	Specifies the central office switch type on an ISDN BRI.
isdn switch-type (PRI)	Specifies the central office switch type or enables support of QSIG or Q.931 signaling on an ISDN PRI.
session target	Specifies a network-specific address for a dial peer.
signal-end-to-end	Configures R2 transparency using GTD on an R2-based E1 CAS network. (Does not apply to SIP.)
signaling forward (dial-peer)	Specifies tunneling for QSIG, Q.931, H.225, and ISUP messages over a specific dial peer on a SIP or H.323 gateway.

signaling forward (dial peer)

To configure settings for transparent tunneling of Q-signaling (QSIG), Q.931, H.225, and ISDN User Part (ISUP) messages over an individual dial peer that override global settings for a Cisco IOS voice gateway, use the **signaling forward** command in dial peer voice configuration mode. To specify that transparent tunneling behavior on a dial peer be determined by global settings for the gateway, use the **no** form of this command.

Cisco IOS H.323 Dial Peers
signaling forward {**conditional** | **none** | **rawmsg** | **unconditional**}
no signaling forward

Cisco IOS SIP Dial Peers
signaling forward {**none** | **rawmsg** | **unconditional**}
no signaling forward

Syntax Description

conditional	Overrides global settings for the gateway and specifies that tunneling on an H.323 dial peer is determined by the target. (The target is defined using the **session target** command.) This is the default setting for an H.323 dial peer if a global setting is not configured for the gateway. **Note** The **conditional** keyword is not supported on Session Initiation Protocol (SIP) dial peers. Instead, the default setting for SIP dial peers is that no tunneling is configured (**none**).
none	Overrides global settings for the gateway and specifies that the dial peer does not forward Generic Transparency Descriptor (GTD), QSIG, or Q.931 payloads to any endpoint in the network. This is the default setting for a SIP dial peer.
rawmsg	Overrides global settings for the gateway and specifies that the dial peer tunnel QSIG (application-qsig) or Q.931 raw messages (application-Xq931) only, without GTD.
unconditional	Specifies unconditional tunneling and forwards GTD payload along with the QSIG or Q.931 message body even if the attached external route server has modified it. (The gatekeeper sends its own GTD back to itself.)

Command Default

The dial peers use the global setting for transparent tunneling if it is configured for the gateway. If global configuration of the gateway is not specified, the following are the default behaviors for dial peers:

- **conditional** --messages are forwarded according to the target:
  - Non-Registration, Admission, and Status (RAS) targets--only the original payload (without GTD) is forwarded to the H.323 endpoint.
  - All other targets--GTD payload is forwarded along with the message body.

No transparent tunneling of QSIG or Q.931 messages is configured.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco AS5350 and Cisco AS5850.
12.4(15)XY	Support was added for passing RELEASE and RELEASE COMPLETE messages end to end over SIP using QSIG tunneling on Cisco IOS voice gateways.
12.4(15)XZ	Support was added for Q.931 tunneling over SIP on Cisco IOS voice gateways and tunneling of both QSIG and Q.931 over SIP was extended to the Cisco Unified Border Element (CUBE). **Note** The CUBE is formerly known as the Cisco IOS Session Border Controller (SBC) or the Cisco Multiservice IP-to-IP Gateway.
12.4(20)T	Support was added for QSIG and Q.931 tunneling over SIP on Cisco IOS voice gateways and the CUBE.

Usage Guidelines

This command is used to configure tunneling behavior for individual dial peers on H.323 and SIP voice gateways. Depending on your specific Cisco router, platform, and network, you can use this command to configure tunneling behavior for various messages, such as QSIG, Q.931, H.225, and ISUP messages. To configure the global setting for a gateway, use the **signaling forward** command in voice service VoIP configuration mode.

For more specific information about controlling tunneling behavior using the **signaling forward** command, see the information included in the following sections:

QSIG and Q.931 Tunneling

Tunneling of QSIG and Q.931 on H.323 gateways is enabled by default for Cisco IOS gateway platforms supporting the **signaling forward** command. For QSIG and Q.931 tunneling on SIP gateways, however, you must configure at least one interface on both an ingress, or originating gateway (OGW), and an egress, or terminating gateway (TGW).

In addition to signaling forward settings, you must specify QSIG or Q.931 as the central office switch type on the ISDN interface for both the OGW and TGW on a SIP or H.323 network. Use the **isdn switch-type** command to enable and specify the switch type:

- For tunneling QSIG messages, specify the **primary-qsig** switch type.
- For tunneling Q.931 messages, specify any ISDN switch type except **primary-qsig** and **primary-dpness**.



Note Cisco IOS SIP gateways do not support the **primary-dpness** switch type for tunneling of Q.931.

Displays QSIG and Q.931 tunneling behavior as determined by gateway voice class and configuration settings.

Table 2: QSIG Tunneling Behavior by Voice Class and Signaling Forward Setting

Signaling Forward Configuration	H.323 Gateway	SIP Gateway
conditional or no specified setting:	Default.	Not supported.

Signaling Forward Configuration	H.323 Gateway	SIP Gateway
session target *non-ras*	Tunnels GTD payload with QSIG or Q.931 message bodies.	No tunneling.
session target ras	Tunnels only QSIG or Q.931 message bodies.	No tunneling.
none	No tunneling.	No tunneling.
rawmsg	Tunnels QSIG or Q.931 message bodies only.	Tunnels QSIG or Q.931 message bodies only.
unconditional	Tunnels GTD payload along with QSIG or Q.931 message bodies.	Tunnels GTD payload along with QSIG or Q.931 message bodies.

SS7 ISUP and H.225 Tunneling over H.323

ISUP defines the protocol and procedures used to configure, manage, and release trunk circuits that carry voice and data calls over the Public Switched Telephone Network (PSTN). ISUP is used for both ISDN and non-ISDN calls and is reconstructed on the basis of the protocol at the egress side of the network, without any concern for the ISDN or ISUP variant on the ingress side of the network.

When you specify that ISDN (H.225) or ISUP information be provided in text format, the information can also be used by applications inside the core H.323 network such as, in a route server, which can use certain ISDN and ISUP information for routing decisions. Additionally, transporting ISUP encapsulated in GTD maintains compatibility with the H.323 protocol.

If the target is a RAS target, for a non-GTD signaling payload, the original payload is forwarded. For a GTD signaling payload, the payload is encapsulated in an admission request (ARQ)/disengage request (DRQ) message and sent to the originating gatekeeper. The gatekeeper conveys the payload to the Gatekeeper Transaction Message Protocol (GKTMP) and external route server for a flexible route decision based upon the ISUP GTD parameters. The gateway then conditionally forwards the GTD payload on the basis of the instruction from the route server.

To tunnel the ISUP GTD, you must configure a dial peer on both the OGW and TGW to encapsulate SS7 ISUP messages in GTD format.

Note If you specify **primary-qsig** as the **isdn switch-type** setting, you must assign network-side functionality (either at the global or dial-peer level) using the **isdn protocol-emulate** command.

Examples

The following example shows unconditional signal forwarding being set on a SIP dial peer (overriding the global setting for the Cisco IOS voice gateway):

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer
 voice 1
Router(config-dial-peer)# signaling forward unconditional
Router(config-dial-peer)# session protocol sipv2
```

The following example is sample output from the **show running-config** command when a SIP dial peer is configured with unconditional signal forwarding:

```
Router# show running-config
Building configuration...
Current configuration : 2357 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!
boot-start-marker
no boot startup-test
boot-end-marker
.
.
.
!
dial-peer voice 101 voip
 signaling forward unconditional
 session protocol sipv2
 session target ipv4:9.13.19.114
 incoming called-number 8000
 codec g711ulaw
!
.
```

Note The "session protocol sipv2" in the output indicates that this is a SIP dial peer.

The following example shows unconditional signal forwarding being set on an H.323 dial peer (overriding the global setting for the Cisco IOS voice gateway):

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer
 voice 1
Router(config-dial-peer)# signaling forward unconditional
```

The following example is sample output from the **show running-config** command when an H.323 dial peer is configured with unconditional signal forwarding:

```
Router# show running-config
Building configuration...
Current configuration : 2357 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!
boot-start-marker
no boot startup-test
boot-end-marker
.
```

```
.
.
!
dial-peer voice 101 voip
 signaling forward unconditional
 session target ipv4:9.13.19.114
 incoming called-number 8000
 codec g711ulaw
!
.
.
```

Note There is no "session protocol sipv2" in the output, indicating that this is an H.323 dial peer.

Related Commands

clid network-number	Configures a network number in the router for CLID and uses it as the calling party number.
clid restrict	Prevents the calling party number from being presented by CLID.
clid second-number strip	Prevents the second network number from being sent in the CLID information.
isdn global-disconnect	Specifies setting for allowing passage of Release and Release Complete messages over a voice network.
isdn protocol-emulate	Enables emulation of the network side of an ISDN configuration for a PRI Net5 or PRI NTT switch type.
isdn protocol-emulate (dial)	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI to emulate NT (network) or TE (user) functionality.
isdn switch-type (BRI)	Specifies the central office switch type on an ISDN BRI.
isdn switch-type (PRI)	Specifies the central office switch type or enables support of QSIG or Q.931 signaling on an ISDN PRI.
session protocol (dial peer)	Specifies a session protocol on a dial peer for calls between local and remote routers using the packet network.
session target	Specifies a network-specific address for a dial peer.
signal-end-to-end	Configures R2 transparency using GTD on an R2-based E1 CAS network. (Does not apply to SIP.)
signaling forward	Specifies tunneling for QSIG, Q.931, H.225, and ISUP messages globally for a SIP or H.323 gateway.

signal-type

To set the signaling type to be used when connecting to a dial peer, use the **signal-type** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

signal-type {**cas** | **cept** | **ext-signal** | **transparent**}
no signal-type

Syntax Description

cas	North American EIA-464 channel-associated signaling (robbed bit signaling). If the Digital T1 Packet Voice Trunk Network Module is installed, this option might not be available.
cept	Provides a basic E1 ABCD signaling protocol. Used primarily for E&M interfaces. When used with FXS/FXO interfaces, this protocol is equivalent to MELCAS.
ext -signal	External signaling. The digital signal processor (DSP) does not generate any signaling frames. Use this option when there is an external signaling channel, for example, CCS, or when you need to have a permanent "dumb" voice pipe.
transparent	Selecting this option produces different results depending on whether you are using a digital voice module (DVM) or an analog voice module (AVM). For a DVM: The ABCD signaling bits are copied from or transported through the T1/E1 interface "transparently" without modification or interpretation. This enables the handling of arbitrary or unknown signaling protocols. For an AVM: It is not possible to provide "transparent" behavior without interpreting the signaling information to read and write the correct state to the analog hardware. This option is mapped to be equal to **cas**.

Command Default

cas

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco 2600, Cisco 3600, and Cisco MC3810.
12.0(4)T	This command was implemented on the Cisco 7200 series.
12.0(7)XK	The **cept** and **transparent** keywords, previously supported only on the Cisco MC3810, are now supported on the Cisco 2600 series, Cisco 3600 series, and 7200 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command applies to Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) dial peers. It is used with permanent connections only (Cisco trunks and FRF.11 trunks), not with switched calls.

This command is used to inform the local telephony interface of the type of signaling it should expect to receive from the far-end dial peer. To turn signaling off at this dial peer, select the **ext-signal** option. If

signaling is turned off and there are no external signaling channels, a "hot" line exists, enabling this dial peer to connect to anything at the far end.

When you connect an FXS to another FXS, or if you have anything other than an FXS/FXO or E&M/E&M pair, the appropriate signaling type on Cisco 2600 and Cisco 3600 series routers is **ext-signal** (disabled).

If you have a digital E1 connection at the remote end that is running cept/MELCAS signaling and you then trunk that across to an analog port, you should make sure that you configure both ends for the **cept** signal type.

If you have a T1 or E1 connection at both ends and the T1/E1 is running a signaling protocol that is neither EIA-464, or cept/MELCAS, you might want to configure the signal type for the transparent option in order to pass through the signaling.

Examples

The following example disables signaling for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 signal-type ext-signal
 exit
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
connection	Specifies the connection mode for a voice port.
destination-pattern	Specifies the telephone number associated with a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Enables the preferred dial peer to be selected when multiple dial peers within a hunt group are matched for a dial string.
sequence-numbers	Enables the generation of sequence numbers in each frame generated by the DSP.
session protocol	Establishes the VoFR protocol for calls between local and remote routers.
session target	Specifies a network-specific address for a dial peer.

silent-discard untrusted

To discard SIP requests from untrusted sources on an incoming SIP trunk, use **silent-discard untrusted** command in "voice service voip >> sip" configuration mode. To disable, use **no** form of this command.

silent-discard untrusted
no silent-discard untrusted

Command Default

This command is enabled by default. SIP requests from untrusted sources are discarded.

Command Modes

voice service voip >> sip

Command History

Release	Modification
Cisco IOS XE 3.10S Cisco IOS 15.3(3)M	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to enable TDoS attack mitigation.

Example

The following example shows how to configure CUBE to discard SIP requests from untrusted sources on an incoming SIP trunk:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# ip address trusted authenticate
Device(conf-voi-serv)# allow-connections sip to sip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# silent-discard untrusted
```

silent-fax

To configure the voice dial peer for a Type 2 silent fax machine, use the **silent-fax** command in dial peer configuration mode. To disable a silent fax call to any POTS ports, use the **no** form of this command.

silent-fax
no silent-fax

Syntax Description

This command has no arguments or keywords.

Command Default

Silent fax is not configured.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813.

Usage Guidelines

Use this command to configure the router to send a no ring alert tone to a Type 2 silent fax machine that is connected to any of the POTS ports. To check the status of the silent-fax configuration, use the **show running-config** command.

Examples

The following example shows that the **silent-fax** command has been configured on POTS port 1 but not on POTS port 2.

```
dial-peer voice 1 pots
 destination-pattern 5551111
 port 1
 no call-waiting
 ring 0
 volume 4
 caller-number 3334444 ring 1
 subaddress 20
 silent-fax
dial-peer voice 2 pots
 destination-pattern 5552222
 port 2
 no call-waiting
 ring 0
 volume 2
 caller-number 3214567 ring 2
 subaddress 10
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

sip

To enter the Session Initiation Protocol (SIP) configuration mode, use the **sip** command in voice-service VoIP configuration mode.

sip

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Voice-service VoIP configuration (config-voi-srv)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.
12.2(2)XB2	This command was implemented on the Cisco AS5850 platform.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and support was added for the Cisco 3700 series. Cisco AS5300, Cisco AS5350, Cisco AS5850, and Cisco AS5400 platforms were not supported in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

From the voice-service VoIPconfiguration mode, the **sip** command enables you to enter SIP configuration mode. From this mode, several SIP commands are available, such as **bind**, **session transport**, and **url**.

Examples

The following example illustrates entering SIP configuration mode and then setting the **bind** command on the SIP network:

```
Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(conf-serv-sip)# bind control source-interface FastEthernet 0
```

Related Commands

Command	Description
voice service voip	Enters the voice-service configuration mode.

Command	Description
session transport	Configures the voice dial peer to use Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) as the underlying transport layer protocol for SIP messages.

sip-header

To specify the Session Initiation Protocol (SIP) header to be sent to the peer call leg, use the **sip-header** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

sip-header {**sip-req-uri***header-name*}
no sip-header {**sip-req-uri***header-name*}

Syntax Description

sip-req-uri	Configures Cisco Unified Border Element (UBE) to send a SIP request Uniform Resource Identifier (URI) to the peer call leg.
header-name	Name of the header to be sent to the peer call leg.

Command Default

SIP header is not sent to the peer call leg.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **sip-header** command to configure Cisco UBE to pass the unsupported parameters present in a mandatory header from one peer call leg to another of a Cisco UBE.

Examples

The following example shows how to configure Cisco UBE to send a "From" header to the peer call leg:

```
Router(config)# voice class sip-copylist 2
Router(config-class)# sip-header From
```

Related Commands

Command	Description
voice class sip-copylist	Configures a list of entities to be sent to a peer call leg and enters voice class configuration mode.

sip-header SIP-StatusLine

To specify that the Session Initiation Protocol (SIP) status line header must be sent to the peer call leg, use the **sip-header SIP-StatusLine** command in voice class configuration mode. To disable this configuration, use the **no** form of the command.

sip-header SIP-StatusLine
no sip-header SIP-StatusLine

Syntax Description

This command has no keywords or arguments.

Command Default

The SIP status line header is not sent to the peer call leg.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Usage Guidelines

A list of entities to be sent to the peer call leg using the **voice class sip-copylist** command must be configured before specifying that the SIP status line header must be sent to the peer call leg using the **sip-header SIP-StatusLine** command.

Example

The following example shows how to specify that the SIP status line header must be sent to the peer call leg using the **sip-header SIP-StatusLine** command:

```
Device> enable
Device# configure terminal
Device(config)# voice class sip-copylist 1
Device(config-class)# sip-header SIP-StatusLine
```

Related Commands

Command	Description
voice class sip-copylist	Configures a list of entities to be sent to the peer call leg.

sip-server

To configure a network address for the Session Initiation Protocol (SIP) server interface, use the **sip-server** command in SIP user-agent configuration mode or voice class tenant configuration mode. To remove a network address configured for SIP, use the **no** form of this command.

sip-server {**dns:***host-name* | **ipv4:***ipv4-address[:port-num]* | **ipv6:***ipv6-address*[*:port-num*]}
no sip-server

Syntax Description

dns:*host-name*	Sets the global SIP server interface to a Domain Name System (DNS) hostname. If you specify a hostname, the default DNS defined by the ip name-server command is used. Hostname is optional. Valid DNS hostname in the following format: name.gateway.xyz.
ipv4:*ipv4-address*	Sets the global SIP server interface to an IPv4 address. A valid IPv4 address takes the following format: xxx.xxx.xxx.xxx.
ipv6:*ipv6-address*	Sets the global SIP server interface to an IPv6 address. You must enter brackets around the IPv6 address.
:*port-num*	(Optional) Port number for the SIP server.

Command Default

No network address is configured.

Command Modes

SIP user-agent configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(22)T	Support for IPv6 was added.
15.6(2)T and IOS XE Denali 16.3.1	This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

If you use this command, you can also use the **session target sip-server** command on each dial peer instead of repeatedly entering the SIP server interface address for each dial peer. Configuring a SIP server as a session target is useful if a Cisco SIP proxy server (SPS) is present in the network. With an SPS, you can configure the SIP server option and have the interested dial peers use the SPS by default.

To reset this command to a null value, use the **default** command.

To configure an IPv6 address, the user must enter brackets [ ] around the IPv6 address.

Examples

The following example, beginning in global configuration mode, sets the global SIP server interface to the DNS hostname "3660-2.sip.com." If you also use the **session target sip server** command , you need not set the DNS hostname for each individual dial peer.

```
sip-ua
 sip-server dns:3660-2.sip.com
dial-peer voice 29 voip
 session target sip-server
```

The following example sets the global SIP server interface to an IPv4 address:

```
sip-ua
 sip-server ipv4:10.0.2.254
```

The following example sets the global SIP server interface to an IPv6 address. Note that brackets were entered around the IPv6 address:

```
sip-ua
 sip-server ipv6:[2001:0DB8:0:0:8:800:200C:417A]
```

Related Commands

Command	Description
default	Enables a default aggregation cache.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
session target (VoIP dial peer)	Specifies a network-specific address for a dial peer.
session target sip-server	Instructs the dial peer session target to use the global SIP server.
sip-ua	Enters SIP user-agent configuration mode in order to configure the SIP user agent.

sip-ua

To enable Session Initiation Protocol (SIP) user-agent configuration commands, use the **sip-ua** command in global configuration mode. To reset all SIP user-agent configuration commands to their default values, use the **no** form of this command.

sip-ua
no sip-ua

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not enabled, no SIP user-agent configuration commands can be entered.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support for Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was included.
15.1(2)T	This command was modified. The **connection-reuse** SIP user-agent configuration mode command was added to the **sip-ua** command.
15.2(4)M	This command was modified. The **via-port** option was added to the **connection-reuse** SIP user-agent configuration mode command.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use this command to enter SIP user-agent configuration mode. The table below lists the SIP user-agent configuration mode commands.

Table 3: SIP User-Agent Configuration Mode Commands

Command	Description
connection-reuse	Uses the listener port for sending requests over the UDP. The **via-port** option sends SIP responses to the port present in the Via header instead of the source port on which the request was received. Note that the **connection-reuse** command is a SIP user-agent configuration mode command.
exit	Exits SIP user-agent configuration mode.
inband-alerting	This command is no longer supported as of Cisco IOS Release 12.2 because the gateway handles remote or local ringback on the basis of SIP messaging.
max-forwards	Specifies the maximum number of hops for a request.
retry	Configures the SIP signaling timers for retry attempts.
sip-server	Configures the SIP server interface.
timers	Configures the SIP signaling timers.
transport	Enables or disables a SIP user agent transport for the TCP or UDP that the protocol SIP user agents listen for on port 5060 (default).

Examples

The following example shows how to enter SIP user-agent configuration mode and configure the SIP user agent:

```
Device> enable
Device# configure terminal
Device(config)# sip-ua
Device(config-sip-ua)# retry invite 2
Device(config-sip-ua)# retry response 2
Device(config-sip-ua)# retry bye 2
Device(config-sip-ua)# retry cancel 2
Device(config-sip-ua)# sip-server ipv4:192.0.2.1
Device(config-sip-ua)# timers invite-wait-100 500
Device(config-sip-ua)# exit
Device#
```

Related Commands

Command	Description
exit	Exits SIP user-agent configuration mode.
max-forwards	Specifies the maximum number of hops for a request.
retry	Configures the retry attempts for SIP messages.
show sip-ua	Displays statistics for SIP retries, timers, and current listener status.
sip-server	Configures the SIP server interface.
timers	Configures the SIP signaling timers.

Command	Description
transport	Configures the SIP user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP or UDP socket.

sni send (voice class)

To enable Server Name Indication (SNI), and associate it to a TLS profile, use the command **sni send** in voice class configuration mode. To disable Server Name Indication, use the **no** form of this command.

sni send
no sni send

Syntax Description

This command has no arguments or keywords.

Command Default

Server Name Indication (SNI) is disabled.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1a	This command was introduced under voice class configuration mode.

Usage Guidelines

Server Name Indication (SNI) functionality is associated to a TLS profile through the command **voice class tls-profile** *tag*. The *tag* associates the SNI functionality to the command **crypto signaling**.

sni send enables Server Name Indication (SNI), a TLS extension that allows a TLS client to indicate the name of the server that it is trying connect during the initial TLS handshake process. Only the fully qualified DNS hostname of the server is sent in the client hello. SNI does not support IPv4 and IPv6 addresses in the client hello extension. After receiving a "hello" with the server name from the TLS client, the server uses appropriate certificate in the subsequent TLS handshake process. Only TLS1.2 version is supported with SNI.

Examples

The following example illustrates how to create a voice class tls-profile and associate SNI functionality that is required during the TLS handshake:

```
Router(config)#voice class tls-profile 2
Router(config-class)#sni send
```

Related Commands

Command	Description
voice class tls-profile	Provides sub-options to configure the commands that are required for a TLS session.
crypto signaling	Identifies the trustpoint or the **tls-profile** *tag* that is used during the TLS handshake process.

snmp enable peer-trap dscp-profile

To enable differentiated services code point (DSCP) profile violation traps at the dial peer level, use the **snmp enable peer-trap dscp-profile** command in dial peer voice configuration mode. To disable the configuration, use the **no** form of this command.

snmp enable peer-trap dscp-profile
no snmp enable peer-trap dscp-profile

Syntax Description

This command has no arguments or keywords.

Command Default

DSCP profile violation traps are not enabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

If you enable the DSCP profile violation trap both at the global level and the dial peer level, the dial peer configuration takes precedence over the global level configuration.

Examples

The following example shows how to enable DSCP profile violation traps for a dial peer:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 4 voip
Router(config-dial-peer)# snmp enable peer-trap dscp-profile
Router(config-dial-peer)# end
```

Related Commands

Command	Description
snmp-server enable traps voice dscp-profile	Enables DSCP profile violation traps at the global level.

snmp enable peer-trap poor-qov

To generate poor-quality-of-voice notifications for applicable calls associated with VoIP dial peers, use the **snmp enable peer-trap poor-qov**command in dial peer configuration mode. To disable notification, use the **no** form of this command.

snmp enable peer-trap poor-qov
no snmp enable peer-trap poor-qov

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.

Usage Guidelines

Use this command to generate poor-quality-of-voice notification for applicable calls associated with a dial peer. If you have a Simple Network Management Protocol (SNMP) manager that uses SNMP messages when voice quality drops, you might want to enable this command. Otherwise, you should disable this command to reduce unnecessary network traffic.

Examples

The following example enables poor-quality-of-voice notification for calls associated with VoIP dial peer 10:

```
dial-peer voice 10 voip
 snmp enable peer-trap poor-qov
```

Related Commands

Command	Description
snmp -server enable traps	Enables a router to send SNMP traps and information.
snmp trap link -status	Enables SNMP trap messages to be generated when a specific port is brought up or down.

snmp-server enable traps voice (DSCP profile)

To enable Simple Network Management Protocol (SNMP) voice notifications, use the **snmp-server enable traps voice** command in global configuration mode. To disable the voice notifications, use the **no** form of this command.

snmp-server enable traps voice [**dscp-profile**] [**fallback**] [**high-ds0-util**] [**low-ds0-util**] [**media-policy**] [**poor-qov**]
no snmp-server enable traps voice dscp-profile [**fallback**] [**high-ds0-util**] [**low-ds0-util**] [**media-policy**] [**poor-qov**]

Syntax Description

dscp-profile	(Optional) Enables differentiated services code point (DSCP) voice traps.
fallback	(Optional) Enables SNMP fallback voice traps.
high-ds0-util	(Optional) Enables SNMP high utilization of Digital Signal 0 (DS0) traps.
low-ds0-util	(Optional) Enables SNMP low utilization of DS0 traps.
media-policy	(Optional) Enables SNMP media policy voice traps.
poor-qov	(Optional) Enables SNMP poor quality of voice traps.

Command Default

SNMP DSCP profile voice notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **snmp-server enable traps voice** command to enable SNMP traps for DSCP marking and policing.

Examples

The following example shows how to enable SNMP media policy voice notifications:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps voice dscp-profile media-policy
```

Related Commands

Command	Description
dscp media	Specifies the RPH to DSCP mapping.
violation	Specifies the action that needs to be performed on any violation in the DSCP policy.

soft-offhook

To enable stepped off-hook resistance during seizure, use the **soft-offhook** command in voice-port (FXO) configuration mode. To disable this command, use the **no** form of this command.

soft-offhook
no soft-offhook

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default, which means there is no stepped off-hook resistance during seizure.

Command Modes

Voice-port (FXO) configuration (config-voiceport)

Command History

Release	Modification
12.4(3f) 12.4(4)T4	This command was introduced.

Usage Guidelines

An off-hook indication into a far-end ringing cadence ON condition can occur during glare conditions (outgoing seizure occurring at the same time as an incoming ring). This condition can also occur when the interface configuration includes the **connection plar-opx** command. If the **connection plar-opx** command is not configured, the FXO software waits for a ringing cadence to transition from ON to OFF prior to transitioning to the off-hook condition. (Glare can be minimized by configuring ground-start signaling.)

When the **soft-offhook** command is entered, the FXO hookswitch off-hook resistance is initially set to a midresistance value for outgoing or incoming seizure. This resistance limits the ringing current that occurs during seizure into ringing signals prior to far-end ring-trip. When ringing is no longer detected, hookswitch resistance is returned to its normal lower value. This prevents damage to the FXO line interface that may occur in locations with short loops and conventional ringing sources with low output impedance ringing sources that have the potential to deliver high current.

The **soft-offhook** command applies to the following FXO interface cards (which use the 3050i chipset):

- EM-HDA-3FXS/4FXO (EVM-HD-8FXS/DID, FXO ports only)
- EM-HDA-6FXO (on EVM-HD-8FXS/DID)
- EM2-HDA-4FXO (NM-HDA-4FXS network module only)
- VIC2-4FXO, VIC2-2FXO

Examples

The following example shows a sample configuration session to enable stepped off-hook resistance during seizure on voice port 1/0/0 on a Cisco 3725 router:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# voice-port 1/0/0
Router(config-voiceport)# soft-offhook
Router(config-voiceport)# shutdown
Router(config-voiceport)#
Nov  3 11:08:53.313 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 1/0/0, changed
```

```
state to Administrative Shutdown
Router(config-voiceport)# no shutdown

Router(config-voiceport)#
Nov  3 11:08:58.290 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 1/0/0, changed
state to up
Router(config-voiceport)# ^Z

Router#
Nov  3 11:09:01.086 EST: %SYS-5-CONFIG_I: Configured from console by console
Router#
```

Related Commands

Command	Description
connection plar-opx	Specifies the connection mode for a voice port as PLAR-OPX.
voice-port	Enters voice-port configuration mode.

source-address (uc-wsapi)

To specify the source IP address or hostname for the Cisco Unified Communication IOS services in the NotifyProviderStatus message, use the **source-address** command in uc wsapi configuration mode. To disable the router from sending NotifyProviderStatus message, use the **no** form of this command.

source-address *ip-address*
no source-address

Syntax Description

ip-address	The IP address identified as the source address by the service provider in the NotifyProviderStatus message.

Command Default

No IP address

Command Modes

uc wsapi

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

This command enables the service provider on the router to send messages to the application via the NotifyProvicerStatus message.

Examples

The following example shows how to set the IP source address and port.

```
Router(config)# uc wsapi
Router(config-register-global)# source-address 172.1.12.13
```

Related Commands

Command	Description
provider	Enables a provider service.
remote-url	Specifies the URL of the application.
uc wsapi	Enters Cisco Unified Communication IOS services configuration mode.

source carrier-id

To configure debug filtering for the source carrier ID, use the **source carrier-id** command in call filter match list configuration mode. To disable, use the **no** form of this command.

source carrier-id *string*
no source carrier-id *string*

Syntax Description

string	Alphanumeric identifier for the carrier ID.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match source carrier ID 4321:

```
call filter match-list 1 voice
 source carrier-id 4321
```

Related Commands

Command	Description
call filter match-list voice	Creates a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
show call filter match-list	Displays call filter match lists.
source trunk-group-label	Configures debug filtering for a source trunk group.
target carrier-id	Configures debug filtering for the target carrier ID.
target trunk-group-label	Configures debug filtering for a target trunk group.

source filter

To filter Real-time Transport Protocol (RTP) packets with a source IP address and port number that are different from the one negotiated through Session Initiation Protocol (SIP) signaling, use the **source filter** command in voice service SIP configuration mode. To disable filtering, use the **no** form of this command.

source filter
no source filter

Command Default

RTP source filtering is disabled.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Public Switched Telephone Network (PSTN) callers may experience crosstalk when the SIP IOS gateway receives an invalid RTP stream destined to the same IP address and port of an active call. The invalid stream has a different source IP address and port than the one negotiated using SIP Session Description Protocol (SDP). The Digital Signal Processor (DSP) within the gateway mixes both the valid and invalid RTP streams and plays it to the PSTN caller. Use the **source filter** command when you want to filter RTP packets with a source IP address and port number that are different from the one negotiated through SIP signaling.

Examples

The following example shows how to filter RTP packets:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# source filter
```

Related Commands

Command	Description
sip	Enters SIP configuration mode.
voice service voip	Specifies the voice-encapsulation type and enters voice service configuration mode.

source-ip (media-profile)

To configure the local source IP address of a WebSocket connection in CUBE, use the **source-ip** command in media profile configuration mode. To remove the configuration, use the **no** form of this command.

source-ip *ip-address*
no source-ip *ip-address*

Syntax Description

ip-address	IP address of the interface to bind with the WebSocket.

Command Default

Disabled by default.

Command Modes

Media Profile configuration mode (cfg-mediaprofile)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced on Cisco Unified Border Element.

Usage Guidelines

A CUBE router can have single or multiple interfaces configured on it. In either case, you must specify the IP address of the interface to bind it with the socket in a WebSocket connection. Use the **source-ip** command in media profile configuration mode to bind the router interface with the socket. The **source-ip** *ip-address* configuration has preference over **http client source interface GigabitEthernet** configuration. If you do not configure **source-ip** , CUBE binds to a suitable IP address on the local interface by default.

Examples

The following is a sample configuration for **source-ip (media-profile)** in CUBE:

```
csr(cfg-mediaprofile)#source-ip ?
ip-address Enter the source IP address

csr(cfg-mediaprofile)#source-ip 10.64.86.70
```

Related Commands

Command	Description
media profile stream-service	Enables stream service on CUBE.
connection (media-profile)	Configures idle timeout and call threshold for a media profile.
proxy (media-profile)	Configures IP address or hostname of proxy in media profile.
description (media-profile)	Specifies a description for the media profile.
media class	Applies the media class at the dial peer level.

source trunk-group-label

To configure debug filtering for a source trunk group, use the **source trunk-group-label** command in call filter match list configuration mode. To disable, use the **no** form of this command.

source trunk-group-label *group_number*
no source trunk-group-label *group_number*

Syntax Description

group_number	A value from 0 to 23 that identifies the trunk group.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match source trunk group 21:

```
call filter match-list 1 voice
 source trunk-group-label 21
```

Related Commands

Command	Description
call filter match-list voice	Creates a call filter match list for debugging voice calls.
debug condition match-list	Runs a filtered debug on a voice call.
show call filter match-list	Displays call filter match lists.
source carrier-id	Configures debug filtering for the source carrier ID.
target carrier-id	Configures debug filtering for the target carrier ID.
target trunk-group-label	Configures debug filtering for a target trunk group.

speed dial

To designate a range of digits for SCCP telephony control (STC) application feature speed-dial codes, use the **speed dial** command in STC application feature speed-dial configuration mode. To return the range to its default, use the **no** form of this command.

speed dial from *digit* **to** *digit*
no speed dial

Syntax Description

from *digit*	Starting number for the range of speed-dial codes. Range is 0 to 9 for one-digit codes; 00 to 99 for two-digit codes. Default is 1 for one-digit codes; 01 for two-digit codes. **Note** Range depends on the number of digits set with the **digit** command.
to *digit*	Ending number for the range of speed-dial codes. Range is 0 to 9 for one-digit codes; 00 to 99 for two-digit codes. Default is 9 for one-digit codes; 99 for two-digit codes. **Note** Range depends on the number of digits set with the **digit** command.

Command Default

The default speed-dial codes are 1 to 9 for one-digit codes; 01 to 99 for two-digit codes.

Command Modes

STC application feature speed-dial configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(6)T	The *digit* argument was modified to allow two-digit codes.

Usage Guidelines

This command is used with the STC application, which enables features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

Use this command to set the range of speed-dial codes only if you want to change the range from its default. The **digit** command determines whether speed-dial codes are one-digit or two-digit.

A maximum of nine one-digit or 99 two-digit speed-dial codes are supported. If you set the starting number to 0, the highest number you can set for the ending number is 8 for one-digit codes, or 98 for two-digit codes.

Note that the actual telephone numbers that are speed dialed are stored on Cisco CallManager or the Cisco CallManager Express system. The speed-dial codes that you set with this command are mapped to speed-dial positions on the call-control device. For example, if you set the starting number to 2 and the ending number to 7, the system maps 2 to speed-dial 1 and maps 7 to speed-dial 6.

You can enter numbers in this command in ascending or descending order. For example, the following commands are both valid:

```
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# speed dial from 7 to 2
```

To use the speed-dial feature on a phone, dial the STC application feature speed-dial (FSD) prefix and one of the speed-dial codes that has been configured with this command (or the default if this command was not used). For example, if the FSD prefix is * (the default) and the speed-dial codes are 1 to 9 (the default), dial *3 to dial the telephone number stored with speed-dial 3.

This command resets to its default range if you modify the value of the **digit** command. For example, if you set the **digit** command to 2, then change the **digit** command back to its default of 1, the speed-dial codes are reset to 1 to 9.

If the **digit** command is set to 2 and you configure a single-digit speed-dial code, the system converts the speed-dial code to two digits. For example, if you enter the range 1 to 5 in a two-digit configuration, the system converts the speed-dial codes to 11 to 15.

If you set any of the FSD codes in this range to a value that is already in use for another FSD code, you receive a warning message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

The **show running-config** command displays nondefault FSD codes only. The **show stcapp feature codes** command displays all FSD codes.

Examples

The following example sets an FSD code prefix of two pound signs (##) and a speed-dial code range of 2 to 7. After these values are configured, a phone user presses ##2 to dial the number that is stored with speed-dial 1 on the call-control system (Cisco CallManager or Cisco CallManager Express).

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix ##
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# exit
```

The following example shows how the speed-dial range that is set in the example above is mapped to the speed-dial positions on the call-control system. Note that the range from 2 to 7 is mapped to speed-dial 1 to 6.

```
Router# show stcapp feature codes
.
.
.
  stcapp feature speed-dial
    prefix ##
    redial ###
    speeddial number of digit(s) 1
    voicemail ##0
    speeddial1 ##2
    speeddial2 ##3
    speeddial3 ##4
    speeddial4 ##5
    speeddial5 ##6
    speeddial6 ##7
```

The following example sets a FSD code prefix of two asterisks (**) and a speed-dial code range of 12 to 17.

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix **
Router(stcapp-fsd)# digit 2
Router(stcapp-fsd)# speed dial from 12 to 17
Router(stcapp-fsd)# exit
```

Related Commands

Command	Description
digit	Designates the number of digits for STC application feature speed-dial codes.
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
show running-config	Displays current nondefault configuration settings.
show stcapp feature codes	Displays configured and default STC application feature access codes.
stcapp feature speed-dial	Enters STC application feature speed-dial configuration mode to set feature speed-dial codes.
voicemail (stcapp-fsd)	Designates an STC application feature speed-dial code to dial the voice-mail number.

srtp (dial peer)

To specify that Secure Real-Time Transport Protocol (SRTP) be used to enable secure calls for a specific VoIP dial peer, to enable fallback, and to override global SRTP configuration, use the **srtp** command in dial peer voice configuration mode. To disable secure calls, to disable fallback, and to override global SRTP configuration, use the **no** form of this command.

srtp [**fallback** | **pass-thru]** | **system**]
no srtp [**fallback** | **pass-thru]** | **system**]

Syntax Description

fallback	(Optional) Enables specific dial peer calls to fall back to nonsecure mode.
pass-thru	(Optional) Enables transparent passthrough of all crypto suites (supported and unsupported).
system	(Optional) Enables the global SRTP configuration that was set using the **srtp** command in voice service voip configuration mode. This is the default if the **srtp** command is enabled in dial peer voice configuration mode.

Command Default

Global SRTP configuration set in voice service voip configuration mode is enabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(6)T1	This command was introduced.
15.6(1)T and 3.17S	This command was modified to include keyword: **pass-thru**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

You can enable secure calls using the **srtp** command either at the dial peer level, or at the global level. The **srtp** command in dial peer voice mode configures call security at the dial-peer level and takes precedence over the global **srtp** command. Use the **srtp** command in dial peer voice configuration mode to enable secure calls for a specific dial peer. Use the **no** form of this command to disable secure calls.

Use the **srtp fallback** command to enable secure calls and allow calls to fallback to nonsecure mode for a specific dial peer. This security policy applies to all calls going through the dial peer and is not configurable on a per-call basis. Using the **srtp fallback** command to configure call fallback at the dial-peer level takes precedence over the global **srtp fallback** command. The **no** form of this command disables SRTP and fallback. If you disallow fallback using the **no srtp fallback** command, a call cannot fall back to nonsecure mode.

To enable the transparent passthrough of all crypto suites for a specific dial peer, use the **srtp pass-thru** command in dial-peer voice configuration mode. If SRTP pass-thru feature is enabled, media interworking will not be supported.

Note Ensure that you have symmetric configuration on both the incoming and outgoing dial-peers to avoid media-related issues.

Use the **srtp system**command to apply global level security settings to dial peers.

Examples

The following example enables secure calls and disallows fallback for a specific dial peer:

```
Router(config-dial-peer)# srtp
```

The following example enables secure calls and allows call fallback to nonsecure mode:

```
Router(config-dial-peer)# srtp fallback
```

The following example enables the transparent passthrough of crypto suites:

```
Router(config-dial-peer)# srtp pass-thru
```

The following example defaults call security to global level SRTP behavior:

```
Router(config-dial-peer)# srtp system
```

Related Commands

Command	Description
srtp (voice)	Enables secure calls globally in voice service voip configuration mode.
srtp fallback (voice)	Enables SRTP and fallback globally.

srtp (voice)

To specify that Secure Real-Time Transport Protocol (SRTP) be used to enable secure calls and call fallback, use the **srtp** command in the global VoIP configuration mode. To disable secure calls and disallow fallback, use the **no** form of this command.

srtp [fallback | pass-thru]
no srtp [fallback | pass-thru]

Syntax Description

fallback	(Optional) Enables call fallback to nonsecure mode.
pass-thru	(Optional) Enables transparent passthrough of all crypto suites (supported and unsupported).

Command Default

Voice call security and fallback are disabled.

Command Modes

Voice service configuration (config-voi-serv)

Dial-peer voice configuration mode (config-dial-peer)

Command History

Release	Modification
12.4(6)T1	This command was introduced.
15.6(1)T and 3.17S	This command was modified to include keyword: **pass-thru**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **srtp** command in voice service voip configuration mode to globally enable secure calls using SRTP media authentication and encryption. This security policy applies to all calls going through the gateway and is not configurable on a per-call basis. To enable secure calls for a specific dial peer, use the **srtp** command in dial-peer voice configuration mode. Using the **srtp** command to configure call security at the dial-peer level takes precedence over the global **srtp** command.

Use the **srtp fallback** command to globally enable secure calls and allow calls to fall back to RTP (nonsecure) mode. This security policy applies to all calls going through the gateway and is not configurable on a per-call basis. To enable secure calls for a specific dial peer, use the **srtp** command in dial-peer voice configuration mode. Using the **srtp fallback** command in dial-peer voice configuration mode to configure call security takes precedence over the **srtp fallback** global command in voice service voip configuration mode. If you use the **no srtp fallback** command, fallback from SRTP to RTP (secure to nonsecure) is disallowed.

Use the **srtp pass-thru** to globally enable the transparent passthrough of all (supported and unsupported) crypto suites. To enable the transparent passthrough of all crypto suites for a specific dial peer, use the **srtp pass-thru** command in dial-peer voice configuration mode. If SRTP pass-thru feature is enabled, media interworking will not be supported.



Note Ensure that you have symmetric configuration on both the incoming and outgoing dial-peers to avoid media-related issues.

Examples

The following example enables secure calls:

```
Router(config-voi-serv)# srtp
```

The following example enables call fallback to nonsecure mode:

```
Router(config-voi-serv)# srtp fallback
```

The following example enables the transparent passthrough of crypto suites:

```
Router(config-voi-serv)# srtp pass-thru
```

Related Commands

Command	Description
srtp (dial-peer)	Enables secure calls on an individual dial peer.
srtp fallback (dial-peer)	Enables call fallback to RTP (nonsecure) mode on an individual dial peer.
srtp fallback (voice)	Enables call fallback globally to RTP (nonsecure) mode.
srtp pass-thru (dial-peer)	Enables the transparent passthrough of unsupported crypto suites on an individual dial peer.
srtp system	Enables secure calls on a global level.

srtp-auth

Note Effective Cisco IOS XE Everest Releases 16.5.1b, **srtp-auth** command is deprecated. Although this command is still available in Cisco IOS XE Everest software, executing this command does not cause any configuration changes. Use **voice class srtp-crypto** command to configure SRTP connection using preferred crypto-suites. For more information, see voice class srtp-crypto command documentation.

To configure a Secure Real-time Transport Protocol (SRTP) connection on Cisco Unified Border Element (Cisco UBE) using the preferred crypto suite in the global level, use the **srtp-auth** command in the SIP configuration mode. To disable this configuration, use the **no** form of the command.

srtp-auth {**sha1-32** | **sha1-80**}
no srtp-auth

Syntax Description

sha1-32	Allows Secure calls with AES_CM_128_HMAC_SHA1_32 crypto suite.
sha1-80	Allow Secure calls with AES_CM_128_HMAC_SHA1_80 crypto suite.

Command Default

AES_CM_128_HMAC_SHA1_32 crypto suite is selected.

Command Modes

SIP configuration mode (conf-serv-sip)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Everest 16.5.1b	This command was deprecated.

Example

The following example shows how to configure an SRTP connection on Cisco UBE in the global level using the AES_CM_128_HMAC_SHA1_80 crypto suite:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# srtp-auth sha1-80
Device(conf-serv-sip)# end
```

Related Commands

Command	Description
show sip-ua srtp	Displays Session Initiation Protocol (SIP) user-agent (UA) Secure Real-time Transport Protocol (SRTP) information.

Command	Description
voice-class sip srtp-auth	Configures a Secure Real-time Transport Protocol (SRTP) connection on Cisco Unified Border Element (CUBE) in the dial peer level using the preferred crypto suite.

srtp-crypto

To assign a previously configured crypto-suite selection preference list globally or to a voice class tenant, use the **srtp-crypto** command. To remove the crypto-suite selection preference and return to default preference list, use the **no** or **default** form of this command.

srtp-crypto *crypto-tag*
no srtp-crypto
default srtp-crypto

Syntax Description

crypto-tag	Unique number assigned to the voice class. The range is from 1 to 10000. This number maps to the tag created using the **voice class srtp-crypto** command available in global configuration mode.

Command Default

No crypto-suite preference assigned.

Command Modes

voice class tenant configuration (config-class)

voice service voice sip configuration (conf-serv-sip)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1b	This command was introduced.

Usage Guidelines

Note Ensure that srtp voice-class is created using the **voice class srtp-crypto** *crypto-tag* command before executing the **srtp-crypto** *crypto tag* command to apply the crypto-tag under global or tenant configuration mode.

You can assign only one crypto-tag. If you assign another crypto-tag, the last crypto-tag assigned replaces the previous crypto-tag.

Example

Example for assigning a crypto-suite preference to a voice class tenant:

```
Device> enable
Device# configure terminal
Device(config)# voice class tenant 100
Device(config-class)# srtp-crypto 102
```

Example for assigning a crypto-suite preference globally:

```
Device> enable
Device# configure terminal
Device(config)# voice service voice
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# srtp-crypto 102
```

Related Commands

Command	Description
voice class sip srtp-crypto	Enters voice class configuration mode and assigns an identification tag for a srtp-crypto voice class.
crypto	Specifies the preference for the SRTP cipher-suite that will be offered by Cisco Unified Border Element (CUBE) in the SDP in offer and answer.
show sip-ua calls	Displays active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (SIP) calls.
show sip-ua srtp	Displays Session Initiation Protocol (SIP) user-agent (UA) Secure Real-time Transport Protocol (SRTP) information.

srtp negotiate

To enable the Cisco IOS Session Initiation Protocol (SIP) gateway to accept and send a Real-Time Transport Protocol (RTP) Audio/Video Profile (AVP) at the global configuration level, use the **srtp negotiate** command in voice service VoIP SIP configuration mode or voice class tenant configuration mode. To disable accepting and sending the RTP AVP, use the **no** form of this command.

srtp negotiate cisco system
no srtp negotiate system

Syntax Description

cisco	Allows an RTP to answer an Secure Real-time Transport Protocol (SRTP) offer.
system	Specifies that the negotiate method use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Support for accepting and sending the RTP AVP at the global configuration level is disabled.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	Support was extended to the Cisco Unified Border Element.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

The **srtp fallback** command enables a SIP gateway to allow SRTP fallback using SIP 4*xx* message responses. With the **srtp negotiate** command, a SIP gateway can be configured to accept and send an RTP (nonsecure) profile in response to an SRTP profile.

Use the **srtp negotiate** command in voice service SIP configuration mode to enable SRTP negotiation globally on a SIP gateway to accept and send nonsecure RTP profiles in response to SRTP offers. To override the global setting and specify this behavior for an individual dial peer on a Cisco IOS SIP gateway, use the **voice-class sip srtp negotiate** command in dial peer voice configuration mode.

There are two scenarios for SRTP negotiation when the **srtp negotiate** command is enabled:

- On a SIP gateway with the **srtp fallback** command enabled, the gateway accepts RTP answers to SRTP offers.
- On a SIP gateway with the **srtp fallback** command disabled, the gateway allows incoming SRTP calls and responds with an RTP answer.

These behaviors are accomplished using the "X-cisco-srtp-fallback" extension in the supported header of initial SIP messages involved in establishment of the session.

Examples

The following example shows how to accept and send an SRTP AVP at the global configuration level:

```
Device> enable

Device# configure
 terminal
Device(config)# voice
 service
 voip

Device(conf-voi-serv)# sip
Device(conf-serv-sip)# srtp negotiate cisco
```

The following example shows SRTP negotiation being enabled globally on a SIP gateway:

```
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# srtp negotiate cisco
```

The following example shows SRTP negotiation being enabled globally in the voice class tenant configuration mode:

```
Router(config-class)# srtp negotiate system
```

Related Commands

Command	Description
srtp (dial peer)	Specifies that an individual dial peer use SRTP to enable secure calls and, optionally, enables fallback to RTP (overriding global settings).
srtp (voice)	Specifies use of SRTP to enable secure calls and, optionally, enables fallback to RTP globally on a Cisco IOS SIP gateway.
voice class sip srtp negotiate	Enables the Cisco IOS SIP gateway to accept and send an RTP AVP at the dial-peer configuration level.

srv version

To generate Domain Name System Server (DNS SRV) queries with either the RFC 2052 or RFC 2782 format, use the **srv version** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

srv version {**1** | **2**}
no srv version

Syntax Description

1	Specifies the domain-name prefix of format protocol.transport. (RFC 2052 style).
2	Specifies the domain-name prefix of format _protocol._transport. (RFC 2782 style).

Command Default

2 (RFC 2782 style)

Command Modes

SIP UA configurationn (config-sip-ua)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5850 was not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5850 in this release.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Session Initiation Protocol (SIP) on Cisco VoIP gateways uses DNS SRV queries to determine the IP address of the user endpoint. The query string has a prefix in the form of "protocol.transport." (RFC 2052) or "_protocol._transport." (RFC 2782). The selected string is then attached to the fully qualified domain name (FQDN) of the next hop SIP server.

By configuring the value of 1, this command provides compatibility with older equipment that supports only RFC 2052.

Examples

The following example sets up the **srv version**command in the RFC 2782 style (underscores surrounding the protocol):

```
Router(config)# sip-ua
Router(config-sip-ua)# srv version 2
```

Related Commands

Command	Description
show sip-ua status	Displays SIP status.