



Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms

Document Update Alert

This document was originally produced for Cisco IOS Release 12.2(11)T. This feature has been updated in subsequent releases, and more recent documentation is available.

If you are using Cisco IOS Release 12.2(11)T or higher, refer to the following documentation in the Cisco IOS Voice Configuration Library, Release 12.3:

- [Cisco IOS SIP Configuration Guide](#)
-

Feature History

Release	Modification
12.1(3)T	This feature was first introduced in Cisco IOS Release 12.1(3)T and implemented on the Cisco AS5300.
12.2(2)XA	This feature was implemented on the Cisco AS5400 and Cisco AS5350 platforms.
12.2(2)XB1	This feature was implemented on the Cisco AS5850 universal gateway.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

This document describes the enhancements to the Session Initiation Protocol (SIP) for Voice over Internet Protocol (VoIP) on Cisco access platforms in Cisco IOS Release 12.2(11)T.

This document includes the following sections:

- [Feature Overview, page 2](#)
- [Supported Platforms, page 7](#)
- [Supported Standards, MIBs, and RFCs, page 8](#)
- [Prerequisites, page 8](#)
- [Configuration Tasks, page 8](#)
- [Configuration Examples, page 13](#)
- [Command Reference, page 18](#)

- [Glossary, page 83](#)

Feature Overview

VoIP currently implements the ITU H.323 specification within Internet Telephony Gateways (ITGs) to signal voice call setup. The Session Initiation Protocol (SIP) is a new protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP. SIP features are compliant with IETF RFC 2543, SIP: Session Initiation Protocol, published in March 1999.

The Cisco SIP functionality enables Cisco access platforms to signal the setup of voice and multimedia calls over IP networks. The SIP feature also provides non-proprietary advantages in the areas of:

- Protocol extensibility
- System scalability
- Personal mobility services
- Interoperability with different vendors

The SIP feature enhancements include the following:

- Configurable in-band alerting.
- Ability to specify the maximum number of SIP redirects.
- Ability to specify SIP or H.323 on a dial-peer basis.
- Configurable SIP message timers and retries.
- Interoperability with unified call services (UCS).
- Support for a variety of signaling protocols, including ISDN, PRI, and CAS.
- Support for a variety of interfaces, including
 - Analog interfaces: FXS/FXO/E&M analog interfaces.
 - Digital interfaces: T1 CAS and E1 CAS.
- Support for SIP redirection messages and interaction with SIP proxies. The gateway can redirect an unanswered call to another SIP gateway or SIP-enabled IP phone. In addition, the gateway supports proxy-routed calls.
- Interoperability with DNS servers including support for DNS SRV and “A” records to look up SIP URLs.
- Support for SIP over TCP and UDP network protocols.
- Support RTP/RTCP for media transport in VoIP networks.
- Support for the following codecs:

Codec	SDP
G711ulaw	0
G711alaw	8
G723r63	4
G726r16	2
G728	15
G729r8	18

- Support for Record-Route headers.
- Support for IP QoS and IP precedence.
- Support for IP Security (IPSec) for SIP signalling messages.
- AAA support. For accounting, the gateway device generates call data record (CDR) accounting records for export. For authentication, the SIP Gateway sends validate requests to AAA server. For authorization, the existing access lists are used.
- Support for call hold and call transfer features. The call hold sends a mid-call INVITE message, which requests that the remote endpoint stop sending media streams. The call transfer is done without consultation. This is called a blind transfer. The transfer can be initiated by a remote SIP endpoint.
- Support for configurable expiration time for SIP INVITEs and maximum number of proxies or redirect servers that can forward a SIP request.
- Ability to hide the calling party's identity based on the setting of the ISDN presentation indicator.
- Expanded support for the mapping of public switched telephone network (PSTN) cause codes to SIP events.

Table 1 lists the PSTN cause codes that can be sent as an ISDN cause information element (IE) and the corresponding SIP event for each.

Table 1 PSTN Cause Code to SIP Event Mappings

PSTN Cause Code	Description	SIP Event
1	Unallocated number	410 Gone
3	No route to destination	404 Not found
16	Normal call clearing	BYE
17	User busy	486 Busy here
18	No user responding	480 Temporarily unavailable
19	No answer from the user	
21	Call rejected	603 Decline
22	Number changed	301 Moved temporarily
27	Destination out of order	404 Not found
28	Address incomplete	484 Address incomplete
29	Facility rejected	501 Not implemented
31	Normal unspecified	404 Not found
34	No circuit available	503 Service unavailable
38	Network out of order	
41	Temporary failure	
42	Switching equipment congestion	
44	Requested channel not available	
47	Resource unavailable	
55	Incoming class barred within CUG	603 Decline

PSTN Cause Code	Description	SIP Event
57	Bearer capability not authorized	501 Not implemented
58	Bearer capability not presently available	
63	Service or option unavailable	503 Service unavailable
65	Bearer cap not implemented	501 Not implemented
79	Service or option not implemented	
87	User not member of CUG	603 Decline
88	Incompatible destination	400 Bad request
95	Invalid message	
102	Recover on timer expiry	408 Request timeout
111	Protocol error	400 Bad request
127	Interworking unspecified	500 Internal server error
Any code other than those listed above		500 Internal server error

Table 2 lists the SIP events and the corresponding PSTN cause codes for each.

Table 2 SIP Event to PSTN Cause Code Mapping

SIP Event	PSTN Cause Code	Description
400 Bad request	127	Interworking
401 Unauthorized	57	Bearer cap not authorized
402 Payment required	21	Call rejected
403 Forbidden	57	Bearer cap not authorized
404 Not found	1	Unallocated number
405 Method not allowed	127	Interworking
406 Not acceptable		
407 Proxy authentication required	21	Call rejected
408 Request timeout	102	Recover on timer expiry
409 Conflict	41	Temporary failure
410 Gone	1	Unallocated number
411 Length required	127	Interworking
413 Request entity too long		
414 Request URI too long		
415 Unsupported media type	79	Service or option not available
420 Bad extension	127	Interworking
480 Temporarily unavailable	18	No user response

SIP Event	PSTN Cause Code	Description
481 Call leg does not exist	127	Interworking
482 Loop detected		
483 Too many hops		
484 Address incomplete	28	Address incomplete
485 Address ambiguous	1	Unallocated number
486 Busy here	17	User busy
500 Internal server error	41	Temporary failure
501 Not implemented	79	Service or option not implemented
502 Bad gateway	38	Network out of order
503 Service unavailable	63	Service or option not available
504 Gateway timeout	102	Recover on timer expiry
505 Version not implemented	127	Interworking
600 Busy everywhere	17	User busy
603 Decline	21	Call rejected
604 Does not exist anywhere	1	Unallocated number
606 Not acceptable	58	Bearer cap not presently available

Benefits

The SIP feature enhancements enable SIP gateways to do the following:

- Enable Cisco voice-enabled platforms to provide RFC2543 compliant user-agent client gateways.
- Support proxy-routed calls.
- Redirect an unanswered call to another SIP gateway or SIP-enabled IP phone.
- Allow end users to place calls on hold.
- Hide the calling party's identity based on the setting of the ISDN presentation indicator.

Restrictions

- The SIP Gateway does not support codecs other than those listed in the [“Feature Overview”](#) section.
- With this release, the SIP Gateway requires each INVITE to include a Session Description Protocol (SDP) header.
- With this release, the contents of the SDP header cannot change between the 180 Ringing message and the 200 OK message.
- The Enhancements to SIP for VoIP on Cisco Access Platforms feature supports plain old telephone service (POTS) to POTS hair-pinning (which means the call comes in one voice-port and is routed out another voice-port). It also supports POTS to IP call legs and IP to POTS call legs. However, it does not support IP to IP hair-pinning. This means the SIP Gateway cannot take an inbound SIP call and reroute it back to another SIP device using the VoIP dial peers.

- Ensure that your access platform has 16 MB Flash and 64 MB DRAM memory minimum, and that I/O memory is set to either 8 MB or 16 MB.
- SIP requires that all times be sent in Greenwich Mean Time (GMT). The INVITE is sent with GMT. However, the default for routers is to use Coordinated Universal Time (UTC). To configure the router to use GMT, issue the **clock timezone** command in global configuration mode and specify the GMT time.
- VoIP dial peers allow a user to configure the **bytes** parameter associated with a codec. However, Cisco SIP gateways currently do not present or respond to this parameter. Currently, the **a=ptime** parameter is not sent or recognized in the SDP body of a SIP message.
- With call transfer, the Requested-By header identifies the party initiating the transfer. The Requested-By header is included in the Invite request that is sent to the transferred-to party only if a Requested-By header was also included in the Bye request.
- With call transfer, the Also header identifies the transferred-to party. To invoke a transfer, the user portion of the Also header must be defined explicitly or with wildcards as a destination pattern on a VoIP dial peer. The transferred call is routed using the session target parameter on the dial peer instead of the host portion of the Also header. Therefore, the Also header can contain *user@host* but the *host* portion is ignored for call routing purposes.
- The grammar for the Also and Requested-By headers is not fully supported. Only the name-addr is supported. This implies that the crypto-param, which might be present in the Bye request, will not be populated in the ensuing Invite to the transferred-to party.
- Cisco SIP Gateways do not support the “user=np-queried” parameter in a Request URI.
- If a Cisco SIP Gateway receives an ISDN Progress message, it generates a 183 Session progress message. If the gateway receives an ISDN ALERT, it generates a 180 Ringing message.

Related Features and Technologies

The SIP feature is dependent upon the interoperability of Service Provider Features for VoIP.

Related Documents

The following documents contain information related to the Cisco SIP functionality:

- Cisco IOS Multiservice Applications Command Reference
- Cisco IOS Multiservice Applications Configuration Guide
- Voice over IP for the Cisco AS5300
- *Voice over IP for the Cisco 2600/3600 Series*
- *Configuring H.323 VoIP Gateway for Cisco Access Platforms*
- *Configuring H.323 VoIP Gatekeeper for Cisco Access Platforms*
- *Service Provider Features for Voice over IP*
- Dial Peer Enhancements
- SIP Call Flows, Version 2

Supported Platforms

- Cisco AS5300
- Cisco AS5350
- Cisco AS5400
- Cisco AS5850

Table 3 Cisco IOS Release and Platform Support for this Feature

Platform	12.1(3)T	12.2(2)XA	12.2(2)XB1	12.2(11)T
Cisco AS5300	X	Not supported	Not supported	X
Cisco AS5350	Not supported	X	X	X
Cisco AS5400	Not supported	X	X	X
Cisco AS5850	Not supported	Not supported	X	X

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

- RFC 2543
- RFC2543 v2

Prerequisites

- Your gateway must have voice functionality that is configurable for either SIP or H.323.
- Establish a working IP network.
For more information about configuring IP, refer to *Cisco IOS IP and IP Routing Configuration Guide*.
- Configure VoIP. For more information about configuring VoIP, refer to the *Cisco IOS Release 12.1 Multiservice Applications Configuration Guide* for the appropriate access platform.
- Ensure that your router supports 64 MB or DRAM, and 16 MB of Flash memory.

Configuration Tasks

See the following sections for configuration tasks for this feature. Each task in the list is identified as either required or optional.

- [Configuring SIP Support for VoIP Dial Peers, page 9](#) (Required)
- [Changing the Configuration of the SIP User Agent \(UA\), page 9](#) (Optional)
- [Configuring SIP Call Transfer, page 9](#) (Optional)
- [Configuring Phone Number Translation Rules, page 12](#) (Required)

Configuring SIP Support for VoIP Dial Peers

To configure SIP support for a VoIP dial peer, you must enter the following commands beginning in global configuration mode:

Step	Command	Purpose
Step 1	Router(config)# dial-peer voice <i>number</i> voip	Enters dial-peer configuration mode to configure a VoIP dial peer.
Step 2	Router(config-dial-peer)# session transport {udp tcp}	Enters the session transport type for the SIP user agent.
Step 3	Router(config-dial-peer)# session protocol sipv2	Enters the session protocol type.
Step 4	Router(config-dial-peer)# session target <i>sip-server</i>	Specifies the dial peer session target to use the global SIP server.

Changing the Configuration of the SIP User Agent (UA)

It is not necessary to configure a SIP UA to place a call. A SIP UA is configured to listen by default. However, if you want to adjust any of the settings, you can do so by using the following commands beginning in global configuration mode:

Step	Command	Purpose
Step 1	Router(config)# sip-ua	Enters SIP user agent (sip-ua) mode to configure SIP-UA related commands.
Step 2	Router(config-sip-ua)# transport {udp tcp}	Configures the SIP user agent (sip-ua) for SIP signaling messages. The default value is udp.
Step 3	Router(config-sip-ua)# sip-server {dns:[host-name] ipv4:ip_address}	Enters the host name or IP address of the SIP server interface.
Step 4	Router(config-sip-ua)# timers trying <i>number</i>	Sets time to wait for a response.
Step 5	Router(config-sip-ua)# timers expires <i>time</i>	Limits the time duration (in milliseconds) of a search for an INVITE.
Step 6	Router(config-sip-ua)# retry invite <i>number</i>	Configures the SIP signaling timers for retry attempts.
Step 7	Router(config-sip-ua)# max-forwards <i>number_of_hops</i>	Limits the number of proxy or redirect servers that can forward a request.

Configuring SIP Call Transfer

The following example illustrates how to configure call transfer. In [Figure 1](#), User A and User C are in an established call. User C then transfers the call to User B. This results in a call being established between User A and User B. User C is then disconnected with User A, regardless of whether the transfer fails or succeeds.

When a call originates or terminates on a gateway, either the calling party number, the called party number, or the port is used (depending on the scenario) to match a dial peer to determine the basic call characteristics. One of the characteristics to determine is which application to use for the call. For the call transfer to succeed, the matching dial peer must have application set to “session” on the gateway that is controlling the transfer. (This is the gateway that receives the Bye with an Also header).

There are two scenarios for dial-peer matching based on whether the call is coming from a POTS interface or from the IP network.

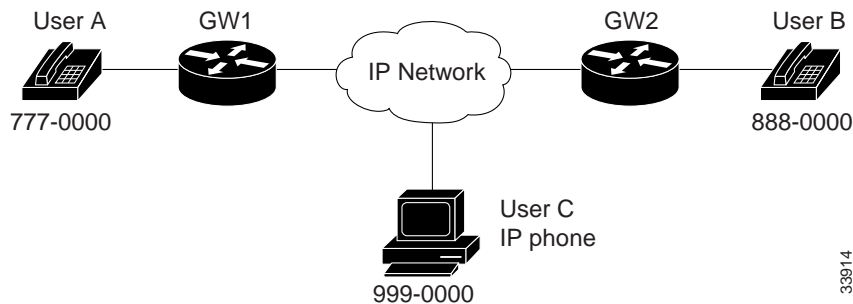
- For calls coming from a POTS interface, the port will be used to match a POTS dial peer with the port the call came in from. This dial peer should have “application session.”
- For calls coming from the IP network, a series of criteria is used (in the order listed below) to match dial peers. If the first criteria does not result in a match, the second criteria is used. If the second criteria does not result in a match, the third criteria is used. If a match does not occur, the default application, which does not support call transfer, is used.
 - a. The called number matches the “incoming called-number” on a VoIP dial peer.
 - b. The calling number matches the “answer-address” on a VoIP dial peer.
 - c. The calling number matches the “destination-pattern” on a VoIP dial peer.



Note

For calls coming from the IP network, it is possible for the calling number to be blocked based on privacy restrictions. In such cases, the “incoming called-number” can be used for call transfers.

Figure 1 Call Transfer Example



In this example, Gateway 1 handles the transfer (recipient of the Bye with the Also header). User C invokes the transfer service (originator of the Bye with the Also header). There are two scenarios in which a dial peer match must have application set to “session” for the transfer to succeed:

- Incoming call from the PSTN—User A originates a call to User C. From the perspective of Gateway 1, this would be an incoming call from the POTS interface so Gateway 1 looks for a POTS dial-peer matching the port on which the call came in. Gateway 1 must have a POTS dial peer for User A with application set to “session” if transfer is later invoked by User C.
- Incoming call from IP network—User C calls User A. From the perspective of Gateway 1 this is an incoming call from the IP network. Gateway 1 uses the criteria previously discussed for a VoIP dial peer (match on incoming called-number, answer-address, or destination pattern). Gateway 1 must have one of the following:
 - A VoIP dial peer with an incoming called-number of User A
 - A VoIP dial peer with answer-address of User C
 - A VoIP dial peer with destination-pattern of User C.

The matching dial peer must have application set to “session” if transfer is later invoked by User C.



Note

To handle all call transfer situations, you should configure both POTS and VoIP dial peers.

To configure SIP call transfer for a POTS dial peer, enter the following commands beginning in global configuration mode:

Step	Command	Purpose
Step 1	Router(config)# dial-peer voice <i>number</i> pots	Enters dial-peer mode to configure a POTS dial peer.
Step 2	Router(config-dial-peer)# application session	Specifies that the standard session application be invoked for this dial peer.
Step 3	Router(config-dial-peer)# destination-pattern <i>pattern</i>	Specifies the telephone number associated with the dial peer.
Step 4	Router(config-dial-peer)# port <i>slot/port</i>	Specifies the voice slot number and port through which incoming VoIP calls are received.

To configure SIP call transfer for a VoIP dial peer, enter the following commands beginning in global configuration mode.

Step	Command	Purpose
Step 1	Router(config)# dial-peer voice <i>number</i> voip	Enters dial-peer configuration mode to configure a VoIP dial peer.
Step 2	Router(config-dial-peer)# application session	Specifies that the standard session application is invoked for this dial peer.
Step 3	Router(config-dial-peer)# destination-pattern <i>pattern</i>	Specifies the telephone number associated with the dial peer.
Step 4	Router(config-dial-peer)# session target ipv4 : <i>x.x.x.x</i>	Specifies the IP address of the destination gateway for outbound dial peers.

To configure a POTS dial peer with the session application, enter the following commands beginning in config-dial-peer configuration mode:

Step	Command	Purpose
Step 1	Router(config-dial-peer)# dial-peer voice <i>number</i> pots	Enters dial-peer mode to configure a POTS dial peer.
Step 2	Router(config-dial-peer)# application session	Specifies that the standard session application is invoked for this dial peer.

To configure a VoIP dial peer with a destination pattern, enter the following commands beginning in config-dial-peer configuration mode:

Step	Command	Purpose
Step 1	Router(config-dial-peer)# dial-peer voice <i>number</i> voip	Enters dial-peer mode to configure a VoIP dial peer.
Step 2	Router(config-dial-peer)# destination-pattern <i>pattern</i>	Specifies the telephone number associated with the dial peer.

To configure a VoIP dial peer with an incoming called-number, enter the following commands beginning in config-dial-peer configuration mode:

Step	Command	Purpose
Step 1	Router(config-dial-peer)# dial-peer voice <i>number</i> voip	Enters dial-peer mode to configure a VoIP dial peer.
Step 2	Router(config-dial-peer)# incoming called-number <i>number</i>	Specifies an incoming called number of a dial peer.

To configure a VoIP dial peer with an incoming called-number, enter the following commands beginning in config-dial-peer configuration mode:

Step	Command	Purpose
Step 1	Router(config-dial-peer)# dial-peer voice <i>number</i> voip	Enters dial-peer mode to configure a VoIP dial peer.
Step 2	Router(config-dial-peer)# answer-address [+]string[T]	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.

Configuring Phone Number Translation Rules

By default, the SIP gateway tags called numbers that have 11 or more digits as “international” when sending SETUP messages to the PSTN switch. In some cases, such as situations where the user must dial 9 to access an outside line, this assumption may not be correct.

To accommodate such situations, you can define translation rules on the outbound POTS dial peer to convert the “type of number” to the correct value. Translation rules manipulate the called number digits and the “type of number” value associated with the called digits.

To define translation rules on a POTS dial peer, enter the following commands beginning in global configuration mode:

Step	Command	Purpose
Step 1	Router(config)# translation-rule <i>name-tag</i>	Defines a translation-rule tag number and enters translation-rule configuration mode. All subsequent commands that you enter in this mode before you exit apply to this translation-rule tag.
Step 2	Router(config-translate)# rule <i>precedence input_searched_pattern</i> <i>substituted_pattern</i> [[<i>match-type</i>] [<i>substituted-type</i>]]	Specifies translation rules. This command can be entered multiple times and is applied to the translation-rule defined in Step 1.
Step 3	Router(config)# dial-peer voice <i>number</i> pots	Enters dial-peer configuration mode to configure a POTS dial peer.
Step 4	Router(config-dial-peer)# translate- outgoing called <i>name-tag</i>	Specifies the translation tag for an outbound called number.
Step 5	Router(config-dial-peer)# port <i>slot-number/port</i>	Specifies the voice port.

For more information about the commands used to configure translation rules, see the Dial Peer Enhancements documentation on Cisco.com.

Verifying the SIP Feature Configuration

Enter the following **show** commands to verify your configuration:

- **show running configuration**
- **show sip-ua statistics**
- **show sip-ua status**
- **show sip-ua timers**

Troubleshooting Tips

Use the following **debug** commands to troubleshoot your configuration:

- **debug ccsip all**
- **debug ccsip calls**
- **debug ccsip error**
- **debug ccsip events**
- **debug ccsip messages**
- **debug ccsip states**

Configuration Examples

This section contains examples of the following:

- [Basic SIP Configuration Example](#)
- [Translation Rule Example](#)

- [Call Transfer Example](#)

Basic SIP Configuration Example

The following shows an example of the output that appears when you enter the **show running configuration** command.

```
Router# show running configuration
```

```
Building configuration...
```

```
Current configuration:
```

```
!
version 12.1
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
!
!
clock timezone GMT 5
voice-card 1
!
ip subnet-zero
ip tcp path-mtu-discovery
ip name-server 172.18.192.48
!
isdn voice-call-failure 0
!
!
controller T1 1/0
 framing esf
 clock source line primary
 linecode b8zs
!
controller T1 1/1
!
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice class codec 1
 codec preference 1 g711alaw
 codec preference 2 g723r63
 codec preference 3 g723r53
!
!
dial-peer voice 100 pots
 destination-pattern 3660110
 port 2/0/0
!
dial-peer voice 200 pots
 application session
 destination-pattern 3660120
 port 2/0/1
!
dial-peer voice 101 voip
 destination-pattern 3660210
```

```
session protocol sipv2
session target ipv4:166.34.244.73
codec g711ulaw
!
dial-peer voice 201 voip
application session
destination-pattern 3660220
session protocol sipv2
session target dns:3660-2.sip.com
codec g711ulaw
!
dial-peer voice 999 voip
destination-pattern 5551111
session protocol sipv2
session target ipv4:161.44.53.89
session transport tcp
!
dial-peer voice 300 pots
destination-pattern 2101100
!
dial-peer voice 350 voip
destination-pattern 3100607
session protocol sipv2
session target ipv4:172.18.192.197
codec g711ulaw
!
dial-peer voice 301 voip
application session
destination-pattern 1234
session protocol sipv2
session target ipv4:172.18.192.193
codec g711ulaw
!
dial-peer voice 333 voip
application session
destination-pattern 1235
session protocol sipv2
session target ipv4:172.18.192.199
codec g711ulaw
!
dial-peer voice 888 voip
destination-pattern 888
session protocol sipv2
session target ipv4:161.44.53.89
session transport tcp
codec g711ulaw
!
dial-peer voice 260011 voip
destination-pattern 260011
session protocol sipv2
session target ipv4:172.18.192.164
codec g711ulaw
!
dial-peer voice 444 voip
destination-pattern 2339000
session protocol sipv2
session target ipv4:172.18.192.205
codec g711ulaw
!
dial-peer voice 111 voip
destination-pattern 111
session protocol sipv2
session target sip-server
codec g711ulaw
```

```

!
dial-peer voice 7777777 voip
 destination-pattern 19197777777
 session protocol sipv2
 session target ipv4:172.18.192.38
 codec g711ulaw
!
!
sip-ua
retry invite 2
retry response 2
retry bye 2
retry cancel 2
no inband-alerting
sip-server dns:
!
!
interface FastEthernet0/0
 ip address 172.18.192.194 255.255.255.0
 load-interval 30
 speed auto
 half-duplex
!
interface FastEthernet0/1
 ip address 166.34.245.230 255.255.255.224
 load-interval 30
 speed auto
 half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.192.1
ip route 166.34.0.0 255.255.0.0 166.34.245.225
no ip http server
!
access-list 101 permit ip host 10.0.2.30 host 10.0.2.31
access-list 101 deny udp any eq rip any
access-list 101 deny udp any any eq rip
access-list 101 deny udp any eq isakmp any
access-list 101 deny udp any any eq isakmp
access-list 101 permit ip any any
snmp-server engineID local 000000090200003094202740
snmp-server community public RW
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password xxx
 login
!
end

```

Translation Rule Example

The following example illustrates a translation rule for dialing national numbers in the situation where the user must dial 9 to access an outside line. In the rule command in this example:

- **91%** is the input search pattern. The percent sign (%) is a wild card.
- The second **1** is the substituted pattern.

- **international** is the match type of number.
- **national** is the substituted type of number.

The result of this command is that any outgoing call that is destined for a number that starts with 91 and that is considered by the gateway to be an international number, will be sent to the PSTN as a national number with a prefix of 1.

```
translation-rule 10
Rule 1 91% 1 international national
!
!
!
dial-peer voice 10 pots
destination-pattern 91.....
translate-outgoing called 10
port 1:D
!
```

The following example illustrates a translation rule for dialing national numbers in the situation where the user does not need to dial 9 to access an outside line.

```
translation-rule 10
Rule 1 1% 1 international national
!
!
!
dial-peer voice 10 pots
destination-pattern 1.....
translate-outgoing called 10
port 1:D
prefix 1
!
```

The following example illustrates a translation rule for dialing international numbers in the situation where the user must dial 9 to access an outside line.

```
translation-rule 20
Rule 1 9011% 011 unknown international
!
!
!
dial-peer voice 10 pots
destination-pattern 9011T
translate-outgoing called 20
port 1:D
!
```

The following example illustrates a translation rule for dialing international numbers in the situation where the user does not need to dial 9 to access an outside line.

```
translation-rule 20
Rule 1 011% 011 unknown international
!
!
!
dial-peer voice 10 pots
destination-pattern 011T
translate-outgoing called 20
port 1:D
prefix 011
!
```

Call Transfer Example

The following example shows how to configure SIP call transfer for a VoIP dial peer:

```
Router(config)# dial-peer voice number voip
Router(config-dial-peer)# application session
Router(config-dial-peer)# destination-
pattern pattern
Router(config-dial-peer)# session target ipv4:x.x.x.x
```

The following example shows how to configure SIP call transfer for a VoIP dial peer:

```
Router(config)# dial-peer voice number voip
Router(config-dial-peer)# application session
Router(config-dial-peer)# destination-
pattern pattern
Router(config-dial-peer)# session target ipv4:x.x.x.x
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3T command reference publications.

This section documents the following commands:

- [debug ccsip all](#)
- [debug ccsip calls](#)
- [debug ccsip error](#)
- [debug ccsip events](#)
- [debug ccsip messages](#)
- [debug ccsip states](#)
- [default](#)
- [gw-accounting](#)
- [inband-alerting](#)
- [max-redirects](#)
- [max-forwards](#)
- [session protocol](#)
- [session target \(VoIP\)](#)
- [session transport](#)
- [show sip-ua statistics](#)
- [show sip-ua status](#)
- [show sip-ua timers](#)

- [sip-server](#)
- [sip-ua](#)
- [timers](#)
- [transport](#)

debug ccsip all

To enable all SIP-related debugging, enter the **debug ccsip all** command in privileged EXEC configuration mode. To disable debugging output, use the **no** form of this command.

debug ccsip all

no debug ccsip all

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	
12.1(1)T	This command was introduced.
12.1(3)T	The output of the command was changed.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines The **debug ccsip all** command enables the following SIP debug commands:

- **debug ccsip events**
- **debug ccsip error**
- **debug ccsip states**
- **debug ccsip messages**
- **debug ccsip calls**

Examples From one side of the call, the debug output is as follows:

```
Router1# debug ccsip all
```

```
All SIP call tracing enabled
```

```
Router1#
```

```
*Mar 6 14:10:42: 0x624CFEF8 : State change from (STATE_NONE, SUBSTATE_NONE) to (STATE_IDLE, SUBSTATE_NONE)
```

```
*Mar 6 14:10:42: Queued event from SIP SPI : SIPSPI_EV_CC_CALL_SETUP
```

```
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: act_idle_call_setup
```

```
*Mar 6 14:10:42: act_idle_call_setup:Not using Voice Class Codec
```

```
*Mar 6 14:10:42: act_idle_call_setup: preferred_codec set[0] type :g711ulaw bytes: 160
```

```
*Mar 6 14:10:42: Queued event from SIP SPI : SIPSPI_EV_CREATE_CONNECTION
```

```
*Mar 6 14:10:42: 0x624CFEF8 : State change from (STATE_IDLE, SUBSTATE_NONE) to (STATE_IDLE, SUBSTATE_CONNECTING)
```

```
*Mar 6 14:10:42: REQUEST CONNECTION TO IP:166.34.245.231 PORT:5060
```

```

*Mar 6 14:10:42: 0x624CFEF8 : State change from (STATE_IDLE, SUBSTATE_CONNECTING) to
(State_IDLE, SUBSTATE_CONNECTING)
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: act_idle_connection_created
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: act_idle_connection_created: Connid(1) created to
166.34.245.231:5060, local_port 54113
*Mar 6 14:10:42: sipSPIAddLocalContact
*Mar 6 14:10:42: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: sip_stats_method
*Mar 6 14:10:42: 0x624CFEF8 : State change from (STATE_IDLE, SUBSTATE_CONNECTING) to
(State_SENT_INVITE, SUBSTATE_NONE)
*Mar 6 14:10:42: Sent:
INVITE sip:3660210@166.34.245.231;user=phone;phone-context=unknown SIP/2.0
Via: SIP/2.0/UDP 166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Sat, 06 Mar 2002 19:10:42 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Cisco-Guid: 2881152943-2184249548-0-483039712
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Max-Forwards: 6
Timestamp: 731427042
Contact: <sip:3660110@166.34.245.230:5060;user=phone>
Expires: 180
Content-Type: application/sdp
Content-Length: 137

v=0
o=CiscoSystemsSIP-GW-UserAgent 1212 283 IN IP4 166.34.245.230
s=SIP Call
t=0 0
c=IN IP4 166.34.245.230
m=audio 20208 RTP/AVP 0

*Mar 6 14:10:42: Received:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 2002 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Length: 0

*Mar 6 14:10:42: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:5060
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: act_sentininvite_new_message
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: sipSPICheckResponse
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 6 14:10:42: Roundtrip delay 4 milliseconds for method INVITE

*Mar 6 14:10:42: 0x624CFEF8 : State change from (STATE_SENT_INVITE, SUBSTATE_NONE) to
(State_REC'D_PROCEEDING, SUBSTATE_PROCEEDING_PROCEEDING)
*Mar 6 14:10:42: Received:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 2002 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194

```

debug ccsip all

```

Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 137

v=0
o=CiscoSystemsSIP-GW-UserAgent 969 7889 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20038 RTP/AVP 0

*Mar 6 14:10:42: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:5060
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: act_recdproc_new_message
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: sipSPICheckResponse
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: sipSPICheckResponse : Updating session description
*Mar 6 14:10:42: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 6 14:10:42: Roundtrip delay 8 milliseconds for method INVITE

*Mar 6 14:10:42: HandleSIP1xxRinging: SDP MediaTypes negotiation successful!
Negotiated Codec      : g711ulaw , bytes :160
Inband Alerting      : 0

*Mar 6 14:10:42: 0x624CFEF8 : State change from (STATE_REC'D_PROCEEDING,
SUBSTATE_PROCEEDING_PROCEEDING) to (STATE_REC'D_PROCEEDING, SUBSTATE_PROCEEDING_ALERTING)
*Mar 6 14:10:46: Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
Date: Mon, 08 Mar 2002 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Contact: <sip:3660210@166.34.245.231:5060;user=phone>
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 137

v=0
o=CiscoSystemsSIP-GW-UserAgent 969 7889 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20038 RTP/AVP 0

*Mar 6 14:10:46: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:5060
*Mar 6 14:10:46: CCSIP-SPI-CONTROL: act_recdproc_new_message
*Mar 6 14:10:46: CCSIP-SPI-CONTROL: sipSPICheckResponse
*Mar 6 14:10:46: CCSIP-SPI-CONTROL: sipSPICheckResponse : Updating session description
*Mar 6 14:10:46: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 6 14:10:46: Roundtrip delay 3536 milliseconds for method INVITE

*Mar 6 14:10:46: CCSIP-SPI-CONTROL: act_recdproc_new_message: SDP MediaTypes negotiation
successful!
Negotiated Codec      : g711ulaw , bytes :160

*Mar 6 14:10:46: CCSIP-SPI-CONTROL: sipSPIReconnectConnection
*Mar 6 14:10:46: Queued event from SIP SPI : SIPSPI_EV_RECONNECT_CONNECTION
*Mar 6 14:10:46: CCSIP-SPI-CONTROL: recv_200_OK_for_invite
*Mar 6 14:10:46: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE

```

```

*Mar 6 14:10:46: CCSIP-SPI-CONTROL: sip_stats_method
*Mar 6 14:10:46: 0x624CFEF8 : State change from (STATE_REC'D_PROCEEDING,
SUBSTATE_PROCEEDING_ALERTING) to (STATE_ACTIVE, SUBSTATE_NONE)
*Mar 6 14:10:46: The Call Setup Information is :

      Call Control Block (CCB) : 0x624CFEF8
      State of The Call       : STATE_ACTIVE
      TCP Sockets Used       : NO
      Calling Number         : 3660110
      Called Number          : 3660210
      Negotiated Codec       : g711ulaw
      Source IP Address (Media): 166.34.245.230
      Source IP Port (Media): 20208
      Destn IP Address (Media): 166.34.245.231
      Destn IP Port (Media): 20038
      Destn SIP Addr (Control) : 166.34.245.231
      Destn SIP Port (Control) : 5060
      Destination Name       : 166.34.245.231

*Mar 6 14:10:46: HandleUdpReconnection: Udp socket connected for fd: 1 with
166.34.245.231:5060
*Mar 6 14:10:46: Sent:
ACK sip:3660210@166.34.245.231:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
Date: Sat, 06 Mar 2002 19:10:42 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Max-Forwards: 6
Content-Type: application/sdp
Content-Length: 137
CSeq: 101 ACK

v=0
o=CiscoSystemsSIP-GW-UserAgent 1212 283 IN IP4 166.34.245.230
s=SIP Call
t=0 0
c=IN IP4 166.34.245.230
m=audio 20208 RTP/AVP 0

*Mar 6 14:10:46: CCSIP-SPI-CONTROL: ccsip_caps_ind
*Mar 6 14:10:46: ccsip_caps_ind: Load DSP with codec (5) g711ulaw, Bytes=160
*Mar 6 14:10:46: ccsip_caps_ind: set DSP for dtmf-relay = CC_CAP_DTMF_RELAY_INBAND_VOICE
*Mar 6 14:10:46: CCSIP-SPI-CONTROL: ccsip_caps_ack
*Mar 6 14:10:50: Received:
BYE sip:3660110@166.34.245.230:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 166.34.245.231:54835
From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
To: "3660110" <sip:3660110@166.34.245.230>
Date: Mon, 08 Mar 2002 22:36:44 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Max-Forwards: 6
Timestamp: 731612207
CSeq: 101 BYE
Content-Length: 0

*Mar 6 14:10:50: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:54835
*Mar 6 14:10:50: CCSIP-SPI-CONTROL: act_active_new_message
*Mar 6 14:10:50: CCSIP-SPI-CONTROL: sact_active_new_message_request
*Mar 6 14:10:50: CCSIP-SPI-CONTROL: sip_stats_method

```

```
debug ccsip all
```

```
*Mar 6 14:10:50: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 6 14:10:50: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 6 14:10:50: CCSIP-SPI-CONTROL: sipSPIInitiateCallDisconnect : Initiate call
disconnect(16) for outgoing call
*Mar 6 14:10:50: 0x624CFEF8 : State change from (STATE_ACTIVE, SUBSTATE_NONE) to
(STATE_DISCONNECTING, SUBSTATE_NONE)
*Mar 6 14:10:50: Sent:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 166.34.245.231:54835
From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
To: "3660110" <sip:3660110@166.34.245.230>
Date: Sat, 06 Mar 2002 19:10:50 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Timestamp: 731612207
Content-Length: 0
CSeq: 101 BYE

*Mar 6 14:10:50: Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_DISCONNECT
*Mar 6 14:10:50: CCSIP-SPI-CONTROL: act_disconnecting_disconnect
*Mar 6 14:10:50: CCSIP-SPI-CONTROL: sipSPICallCleanup
*Mar 6 14:10:50: Queued event from SIP SPI : SIPSPI_EV_CLOSE_CONNECTION
*Mar 6 14:10:50: CLOSE CONNECTION TO CONNID:1

*Mar 6 14:10:50: sipSPIIcpifUpdate :CallState: 4 Payout: 1755 DiscTime:48305031 ConnTime
48304651

*Mar 6 14:10:50: 0x624CFEF8 : State change from (STATE_DISCONNECTING, SUBSTATE_NONE) to
(STATE_DEAD, SUBSTATE_NONE)
*Mar 6 14:10:50: The Call Setup Information is :

Call Control Block (CCB) : 0x624CFEF8
State of The Call      : STATE_DEAD
TCP Sockets Used      : NO
Calling Number        : 3660110
Called Number         : 3660210
Negotiated Codec      : g711ulaw
Source IP Address (Media): 166.34.245.230
Source IP Port (Media): 20208
Destn IP Address (Media): 166.34.245.231
Destn IP Port (Media): 20038
Destn SIP Addr (Control) : 166.34.245.231
Destn SIP Port (Control) : 5060
Destination Name      : 166.34.245.231

*Mar 6 14:10:50:

Disconnect Cause (CC)   : 16
Disconnect Cause (SIP)  : 200

*Mar 6 14:10:50: udpsock_close_connect: Socket fd: 1 closed for connid 1 with remote
port: 5060
Router1#
```

From the other side of the call, the debug output is as follows:

```
Router2# debug ccsip all

All SIP call tracing enabled
Router2#
*Mar 8 17:36:40: Received:
```

```

INVITE sip:3660210@166.34.245.231;user=phone;phone-context=unknown SIP/2.0
Via: SIP/2.0/UDP 166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Sat, 06 Mar 2002 19:10:42 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Cisco-Guid: 2881152943-2184249548-0-483039712
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Max-Forwards: 6
Timestamp: 731427042
Contact: <sip:3660110@166.34.245.230:5060;user=phone>
Expires: 180
Content-Type: application/sdp
Content-Length: 137

```

```

v=0
o=CiscoSystemsSIP-GW-UserAgent 1212 283 IN IP4 166.34.245.230
s=SIP Call
t=0 0
c=IN IP4 166.34.245.230
m=audio 20208 RTP/AVP 0

```

```

*Mar 8 17:36:40: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.230:54113
*Mar 8 17:36:40: CCSIP-SPI-CONTROL: sipSPISipIncomingCall
*Mar 8 17:36:40: 0x624D8CCC : State change from (STATE_NONE, SUBSTATE_NONE) to
(STATE_IDLE, SUBSTATE_NONE)
*Mar 8 17:36:40: CCSIP-SPI-CONTROL: act_idle_new_message
*Mar 8 17:36:40: CCSIP-SPI-CONTROL: sact_idle_new_message_invite
*Mar 8 17:36:40: CCSIP-SPI-CONTROL: sip_stats_method
*Mar 8 17:36:40: sact_idle_new_message_invite:Not Using Voice Class Codec

*Mar 8 17:36:40: sact_idle_new_message_invite: Preferred codec[0] type: g711ulaw Bytes
:160
*Mar 8 17:36:40: sact_idle_new_message_invite: Media Negotiation successful for an
incoming call

*Mar 8 17:36:40: sact_idle_new_message_invite: Negotiated Codec : g711ulaw, bytes
:160
Preferred Codec : g711ulaw, bytes :160

*Mar 8 17:36:40: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 8 17:36:40: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 8 17:36:40: Num of Contact Locations 1 3660110 166.34.245.230 5060

*Mar 8 17:36:40: 0x624D8CCC : State change from (STATE_IDLE, SUBSTATE_NONE) to
(STATE_REC'D_INVITE, SUBSTATE_REC'D_INVITE_CALL_SETUP)
*Mar 8 17:36:40: Sent:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 2002 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Length: 0

*Mar 8 17:36:40: Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_PROCEEDING
*Mar 8 17:36:40: CCSIP-SPI-CONTROL: act_recdinvite_proceeding

```

debug ccsip all

```

*Mar 8 17:36:40: Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_ALERTING
*Mar 8 17:36:40: CCSIP-SPI-CONTROL: ccsip_caps_ind
*Mar 8 17:36:40: ccsip_caps_ind: codec(negotiated) = 5(Bytes 160)
*Mar 8 17:36:40: ccsip_caps_ind: Load DSP with codec (5) g711ulaw, Bytes=160
*Mar 8 17:36:40: ccsip_caps_ind: set DSP for dtmf-relay = CC_CAP_DTMF_RELAY_INBAND_VOICE
*Mar 8 17:36:40: CCSIP-SPI-CONTROL: ccsip_caps_ack
*Mar 8 17:36:40: CCSIP-SPI-CONTROL: act_recdininvite_alerting
*Mar 8 17:36:40: 180 Ringing with SDP - not likely

*Mar 8 17:36:40: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 8 17:36:40: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 8 17:36:40: 0x624D8CCC : State change from (STATE_REC'D_INVITE,
SUBSTATE_REC'D_INVITE_CALL_SETUP) to (STATE_SENT_ALERTING, SUBSTATE_NONE)
*Mar 8 17:36:40: Sent:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 2002 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 137

v=0
o=CiscoSystemsSIP-GW-UserAgent 969 7889 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20038 RTP/AVP 0

*Mar 8 17:36:44: Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_CONNECT
*Mar 8 17:36:44: CCSIP-SPI-CONTROL: act_sentalert_connect
*Mar 8 17:36:44: sipSPIAddLocalContact
*Mar 8 17:36:44: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 8 17:36:44: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 8 17:36:44: 0x624D8CCC : State change from (STATE_SENT_ALERTING, SUBSTATE_NONE) to
(STATE_SENT_SUCCESS, SUBSTATE_NONE)
*Mar 8 17:36:44: Sent:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 166.34.245.230:54113
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
Date: Mon, 08 Mar 2002 22:36:40 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Timestamp: 731427042
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Contact: <sip:3660210@166.34.245.231:5060;user=phone>
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 137

v=0
o=CiscoSystemsSIP-GW-UserAgent 969 7889 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20038 RTP/AVP 0

*Mar 8 17:36:44: Received:
ACK sip:3660210@166.34.245.231:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 166.34.245.230:54113

```

```

From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
Date: Sat, 06 Mar 2002 19:10:42 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
Max-Forwards: 6
Content-Type: application/sdp
Content-Length: 137
CSeq: 101 ACK

v=0
o=CiscoSystemsSIP-GW-UserAgent 1212 283 IN IP4 166.34.245.230
s=SIP Call
t=0 0
c=IN IP4 166.34.245.230
m=audio 20208 RTP/AVP 0

*Mar 8 17:36:44: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.230:54113
*Mar 8 17:36:44: CCSIP-SPI-CONTROL: act_sentsucc_new_message
*Mar 8 17:36:44: CCSIP-SPI-CONTROL: sip_stats_method
*Mar 8 17:36:44: 0x624D8CCC : State change from (STATE_SENT_SUCCESS, SUBSTATE_NONE) to
(STATE_ACTIVE, SUBSTATE_NONE)
*Mar 8 17:36:44: The Call Setup Information is :

      Call Control Block (CCB) : 0x624D8CCC
      State of The Call       : STATE_ACTIVE
      TCP Sockets Used       : NO
      Calling Number        : 3660110
      Called Number         : 3660210
      Negotiated Codec      : g711ulaw
      Source IP Address (Media): 166.34.245.231
      Source IP Port (Media): 20038
      Destn IP Address (Media): 166.34.245.230
      Destn IP Port (Media): 20208
      Destn SIP Addr (Control) : 166.34.245.230
      Destn SIP Port (Control) : 5060
      Destination Name      : 166.34.245.230

*Mar 8 17:36:47: Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_DISCONNECT
*Mar 8 17:36:47: CCSIP-SPI-CONTROL: act_active_disconnect
*Mar 8 17:36:47: Queued event from SIP SPI : SIPSPI_EV_CREATE_CONNECTION
*Mar 8 17:36:47: 0x624D8CCC : State change from (STATE_ACTIVE, SUBSTATE_NONE) to
(STATE_ACTIVE, SUBSTATE_CONNECTING)
*Mar 8 17:36:47: REQUEST CONNECTION TO IP:166.34.245.230 PORT:5060

*Mar 8 17:36:47: 0x624D8CCC : State change from (STATE_ACTIVE, SUBSTATE_CONNECTING) to
(STATE_ACTIVE, SUBSTATE_CONNECTING)
*Mar 8 17:36:47: CCSIP-SPI-CONTROL: act_active_connection_created
*Mar 8 17:36:47: CCSIP-SPI-CONTROL: sipSPICheckSocketConnection
*Mar 8 17:36:47: CCSIP-SPI-CONTROL: sipSPICheckSocketConnection: Connid(1) created to
166.34.245.230:5060, local_port 54835
*Mar 8 17:36:47: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 8 17:36:47: CCSIP-SPI-CONTROL: sip_stats_method
*Mar 8 17:36:47: 0x624D8CCC : State change from (STATE_ACTIVE, SUBSTATE_CONNECTING) to
(STATE_DISCONNECTING, SUBSTATE_NONE)
*Mar 8 17:36:47: Sent:
BYE sip:3660110@166.34.245.230:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 166.34.245.231:54835
From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
To: "3660110" <sip:3660110@166.34.245.230>
Date: Mon, 08 Mar 2002 22:36:44 GMT
Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Max-Forwards: 6

```

debug ccsip all

Timestamp: 731612207
 CSeq: 101 BYE
 Content-Length: 0

*Mar 8 17:36:47: Received:
 SIP/2.0 200 OK
 Via: SIP/2.0/UDP 166.34.245.231:54835
 From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27D3FCA8-C7F
 To: "3660110" <sip:3660110@166.34.245.230>
 Date: Sat, 06 Mar 2002 19:10:50 GMT
 Call-ID: ABBAE7AF-823100CE-0-1CCAA69C@172.18.192.194
 Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
 Timestamp: 731612207
 Content-Length: 0
 CSeq: 101 BYE

*Mar 8 17:36:47: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
 166.34.245.230:54113
 *Mar 8 17:36:47: CCSIP-SPI-CONTROL: act_disconnecting_new_message
 *Mar 8 17:36:47: CCSIP-SPI-CONTROL: sact_disconnecting_new_message_response
 *Mar 8 17:36:47: CCSIP-SPI-CONTROL: sipSPICheckResponse
 *Mar 8 17:36:47: CCSIP-SPI-CONTROL: sip_stats_status_code
 *Mar 8 17:36:47: Roundtrip delay 4 milliseconds for method BYE

 *Mar 8 17:36:47: CCSIP-SPI-CONTROL: sipSPICallCleanup
 *Mar 8 17:36:47: Queued event from SIP SPI : SIPSPI_EV_CLOSE_CONNECTION
 *Mar 8 17:36:47: CLOSE CONNECTION TO CONNID:1

 *Mar 8 17:36:47: sipSPIIcpifUpdate :CallState: 4 Payout: 1265 DiscTime:66820800 ConnTime
 66820420

 *Mar 8 17:36:47: 0x624D8CCC : State change from (STATE_DISCONNECTING, SUBSTATE_NONE) to
 (STATE_DEAD, SUBSTATE_NONE)
 *Mar 8 17:36:47: The Call Setup Information is :

 Call Control Block (CCB) : 0x624D8CCC
 State of The Call : STATE_DEAD
 TCP Sockets Used : NO
 Calling Number : 3660110
 Called Number : 3660210
 Negotiated Codec : g711ulaw
 Source IP Address (Media): 166.34.245.231
 Source IP Port (Media): 20038
 Destn IP Address (Media): 166.34.245.230
 Destn IP Port (Media): 20208
 Destn SIP Addr (Control) : 166.34.245.230
 Destn SIP Port (Control) : 5060
 Destination Name : 166.34.245.230

 *Mar 8 17:36:47:

 Disconnect Cause (CC) : 16
 Disconnect Cause (SIP) : 200

 *Mar 8 17:36:47: udpsock_close_connect: Socket fd: 1 closed for connid 1 with remote
 port: 5060

Related Commands

Command	Description
debug ccsip calls	Shows all SIP Service Provider Interface (SPI) call tracing.
debug ccsip error	Shows SIP SPI errors.
debug ccsip events	Shows all SIP SPI events tracing.
debug ccsip messages	Shows all SIP SPI message tracing.
debug ccsip states	Shows all SIP SPI state tracing.

debug ccsip calls

To show all SIP Service Provider Interface (SPI) call tracing, enter the **debug ccsip calls** command in privileged EXEC configuration mode. To disable debugging output, use the **no** form of this command.

debug ccsip calls

no debug ccsip calls

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	
12.1(1)T	This command was introduced.
12.1(3)T	The output of the command was changed.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines This command traces the SIP call details as they are updated in the SIP call control block.

Examples From one side of the call, the debug output is as follows:

```
Router1# debug ccsip calls

SIP Call statistics tracing is enabled
Router1#
*Mar 6 14:12:33: The Call Setup Information is :

      Call Control Block (CCB) : 0x624D078C
      State of The Call       : STATE_ACTIVE
      TCP Sockets Used       : NO
      Calling Number         : 3660110
      Called Number          : 3660210
      Negotiated Codec       : g711ulaw
      Source IP Address (Media): 166.34.245.230
      Source IP Port (Media): 20644
      Destn IP Address (Media): 166.34.245.231
      Destn IP Port (Media): 20500
      Destn SIP Addr (Control) : 166.34.245.231
      Destn SIP Port (Control) : 5060
      Destination Name       : 166.34.245.231

*Mar 6 14:12:40: The Call Setup Information is :

      Call Control Block (CCB) : 0x624D078C
      State of The Call       : STATE_DEAD
      TCP Sockets Used       : NO
      Calling Number         : 3660110
```

```
Called Number          : 3660210
Negotiated Codec       : g711ulaw
Source IP Address (Media) : 166.34.245.230
Source IP Port (Media)   : 20644
Destn IP Address (Media) : 166.34.245.231
Destn IP Port (Media)    : 20500
Destn SIP Addr (Control) : 166.34.245.231
Destn SIP Port (Control) : 5060
Destination Name        : 166.34.245.231

*Mar 6 14:12:40:

Disconnect Cause (CC)  : 16
Disconnect Cause (SIP) : 200
```

Router1#

From the other side of the call, the debug output is as follows:

Router2# **debug ccsip calls**

SIP Call statistics tracing is enabled

Router2#

```
*Mar 8 17:38:31: The Call Setup Information is :

Call Control Block (CCB) : 0x624D9560
State of The Call       : STATE_ACTIVE
TCP Sockets Used        : NO
Calling Number          : 3660110
Called Number           : 3660210
Negotiated Codec        : g711ulaw
Source IP Address (Media) : 166.34.245.231
Source IP Port (Media)   : 20500
Destn IP Address (Media) : 166.34.245.230
Destn IP Port (Media)    : 20644
Destn SIP Addr (Control) : 166.34.245.230
Destn SIP Port (Control) : 5060
Destination Name        : 166.34.245.230

*Mar 8 17:38:38: The Call Setup Information is :

Call Control Block (CCB) : 0x624D9560
State of The Call       : STATE_DEAD
TCP Sockets Used        : NO
Calling Number          : 3660110
Called Number           : 3660210
Negotiated Codec        : g711ulaw
Source IP Address (Media) : 166.34.245.231
Source IP Port (Media)   : 20500
Destn IP Address (Media) : 166.34.245.230
Destn IP Port (Media)    : 20644
Destn SIP Addr (Control) : 166.34.245.230
Destn SIP Port (Control) : 5060
Destination Name        : 166.34.245.230

*Mar 8 17:38:38:

Disconnect Cause (CC)  : 16
Disconnect Cause (SIP) : 200
```

Related Commands	Command	Description
	debug ccsip all	Enables all SIP-related debugging.
	debug ccsip error	Shows SIP SPI errors.
	debug ccsip events	Shows all SIP SPI events tracing.
	debug ccsip messages	Shows all SIP SPI message tracing.
	debug ccsip states	Shows all SIP SPI state tracing.

debug ccsip error

To show SIP SPI errors, enter the **debug ccsip error** command in privileged EXEC configuration mode. To disable debugging output, use the **no** form of this command.

debug ccsip error

no debug ccip error

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	
12.1(1)T	This command was introduced.
12.1.(3)T	The output of the command was changed.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines This command traces all error messages generated from errors encountered by the SIP subsystem.

Examples From one side of the call, the debug output is as follows:

```
Router1# debug ccsip error

SIP Call error tracing is enabled
Router1#
*Mar 6 14:16:41: CCSIP-SPI-CONTROL: act_idle_call_setup
*Mar 6 14:16:41: act_idle_call_setup:Not using Voice Class Codec

*Mar 6 14:16:41: act_idle_call_setup: preferred_codec set[0] type :g711ulaw bytes: 160
*Mar 6 14:16:41: REQUEST CONNECTION TO IP:166.34.245.231 PORT:5060

*Mar 6 14:16:41: CCSIP-SPI-CONTROL: act_idle_connection_created
*Mar 6 14:16:41: CCSIP-SPI-CONTROL: act_idle_connection_created: Connid(1) created to
166.34.245.231:5060, local_port 55674
*Mar 6 14:16:41: sipSPIAddLocalContact
*Mar 6 14:16:41: CCSIP-SPI-CONTROL: sip_stats_method
*Mar 6 14:16:41: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:5060
*Mar 6 14:16:41: CCSIP-SPI-CONTROL: act_sentinvite_new_message
*Mar 6 14:16:41: CCSIP-SPI-CONTROL: sipSPICheckResponse
*Mar 6 14:16:41: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 6 14:16:41: Roundtrip delay 4 milliseconds for method INVITE

*Mar 6 14:16:41: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:5060
*Mar 6 14:16:41: CCSIP-SPI-CONTROL: act_recdproc_new_message
*Mar 6 14:16:41: CCSIP-SPI-CONTROL: sipSPICheckResponse
```

■ debug ccsip error

```

*Mar 6 14:16:41: CCSIP-SPI-CONTROL: sipSPICheckResponse : Updating session description
*Mar 6 14:16:41: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 6 14:16:41: Roundtrip delay 8 milliseconds for method INVITE

*Mar 6 14:16:41: HandleSIP1xxRinging: SDP MediaTypes negotiation successful!
Negotiated Codec      : g711ulaw , bytes :160
Inband Alerting      : 0

*Mar 6 14:16:45: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:5060
*Mar 6 14:16:45: CCSIP-SPI-CONTROL: act_recdproc_new_message
*Mar 6 14:16:45: CCSIP-SPI-CONTROL: sipSPICheckResponse
*Mar 6 14:16:45: CCSIP-SPI-CONTROL: sipSPICheckResponse : Updating session description
*Mar 6 14:16:45: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 6 14:16:45: Roundtrip delay 3844 milliseconds for method INVITE

*Mar 6 14:16:45: CCSIP-SPI-CONTROL: act_recdproc_new_message: SDP MediaTypes negotiation
successful!
Negotiated Codec      : g711ulaw , bytes :160

*Mar 6 14:16:45: CCSIP-SPI-CONTROL: sipSPIReconnectConnection
*Mar 6 14:16:45: CCSIP-SPI-CONTROL: recv_200_OK_for_invite
*Mar 6 14:16:45: CCSIP-SPI-CONTROL: sip_stats_method
*Mar 6 14:16:45: HandleUdpReconnection: Udp socket connected for fd: 1 with
166.34.245.231:5060
*Mar 6 14:16:45: CCSIP-SPI-CONTROL: ccsip_caps_ind
*Mar 6 14:16:45: ccsip_caps_ind: Load DSP with codec (5) g711ulaw, Bytes=160
*Mar 6 14:16:45: ccsip_caps_ind: set DSP for dtmf-relay = CC_CAP_DTMF_RELAY_INBAND_VOICE
*Mar 6 14:16:45: CCSIP-SPI-CONTROL: ccsip_caps_ack
*Mar 6 14:16:49: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.231:56101
*Mar 6 14:16:49: CCSIP-SPI-CONTROL: act_active_new_message
*Mar 6 14:16:49: CCSIP-SPI-CONTROL: sact_active_new_message_request
*Mar 6 14:16:49: CCSIP-SPI-CONTROL: sip_stats_method
*Mar 6 14:16:49: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar 6 14:16:49: CCSIP-SPI-CONTROL: sipSPIInitiateCallDisconnect : Initiate call
disconnect(16) for outgoing call
*Mar 6 14:16:49: CCSIP-SPI-CONTROL: act_disconnecting_disconnect
*Mar 6 14:16:49: CCSIP-SPI-CONTROL: sipSPICallCleanup
*Mar 6 14:16:49: CLOSE CONNECTION TO CONNID:1

*Mar 6 14:16:49: sipSPIIcpifUpdate :CallState: 4 Playout: 2945 DiscTime:48340988 ConnTime
48340525

*Mar 6 14:16:49: udpsock_close_connect: Socket fd: 1 closed for connid 1 with remote
port: 5060
Router1#

```

From the other side of the call, the debug output is as follows:

```
Router2# debug ccsip error
```

```

SIP Call error tracing is enabled
Router2#
*Mar 8 17:42:39: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.230:55674
*Mar 8 17:42:39: CCSIP-SPI-CONTROL: sipSPISipIncomingCall
*Mar 8 17:42:39: CCSIP-SPI-CONTROL: act_idle_new_message
*Mar 8 17:42:39: CCSIP-SPI-CONTROL: sact_idle_new_message_invite
*Mar 8 17:42:39: CCSIP-SPI-CONTROL: sip_stats_method
*Mar 8 17:42:39: sact_idle_new_message_invite:Not Using Voice Class Codec

```

```

*Mar  8 17:42:39: sact_idle_new_message_invite: Preferred codec[0] type: g711ulaw Bytes
:160
*Mar  8 17:42:39: sact_idle_new_message_invite: Media Negotiation successful for an
incoming call

*Mar  8 17:42:39: sact_idle_new_message_invite: Negotiated Codec      : g711ulaw, bytes
:160
Preferred Codec      : g711ulaw, bytes :160

*Mar  8 17:42:39: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar  8 17:42:39: Num of Contact Locations 1 3660110 166.34.245.230 5060

*Mar  8 17:42:39: CCSIP-SPI-CONTROL: act_recdininvite_proceeding
*Mar  8 17:42:39: CCSIP-SPI-CONTROL: ccsip_caps_ind
*Mar  8 17:42:39: ccsip_caps_ind: codec(negotiated) = 5(Bytes 160)
*Mar  8 17:42:39: ccsip_caps_ind: Load DSP with codec (5) g711ulaw, Bytes=160
*Mar  8 17:42:39: ccsip_caps_ind: set DSP for dtmf-relay = CC_CAP_DTMF_RELAY_INBAND_VOICE
*Mar  8 17:42:39: CCSIP-SPI-CONTROL: ccsip_caps_ack
*Mar  8 17:42:39: CCSIP-SPI-CONTROL: act_recdininvite_alerting
*Mar  8 17:42:39: 180 Ringing with SDP - not likely

*Mar  8 17:42:39: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar  8 17:42:42: CCSIP-SPI-CONTROL: act_sentalert_connect
*Mar  8 17:42:42: sipSPIAddLocalContact
*Mar  8 17:42:42: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar  8 17:42:42: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.230:55674
*Mar  8 17:42:42: CCSIP-SPI-CONTROL: act_sentsucc_new_message
*Mar  8 17:42:42: CCSIP-SPI-CONTROL: sip_stats_method
*Mar  8 17:42:47: CCSIP-SPI-CONTROL: act_active_disconnect
*Mar  8 17:42:47: REQUEST CONNECTION TO IP:166.34.245.230 PORT:5060

*Mar  8 17:42:47: CCSIP-SPI-CONTROL: act_active_connection_created
*Mar  8 17:42:47: CCSIP-SPI-CONTROL: sipSPICheckSocketConnection
*Mar  8 17:42:47: CCSIP-SPI-CONTROL: sipSPICheckSocketConnection: Connid(1) created to
166.34.245.230:5060, local_port 56101
*Mar  8 17:42:47: CCSIP-SPI-CONTROL: sip_stats_method
*Mar  8 17:42:47: HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
166.34.245.230:55674
*Mar  8 17:42:47: CCSIP-SPI-CONTROL: act_disconnecting_new_message
*Mar  8 17:42:47: CCSIP-SPI-CONTROL: sact_disconnecting_new_message_response
*Mar  8 17:42:47: CCSIP-SPI-CONTROL: sipSPICheckResponse
*Mar  8 17:42:47: CCSIP-SPI-CONTROL: sip_stats_status_code
*Mar  8 17:42:47: Roundtrip delay 0 milliseconds for method BYE

*Mar  8 17:42:47: CCSIP-SPI-CONTROL: sipSPICallCleanup
*Mar  8 17:42:47: CLOSE CONNECTION TO CONNID:1

*Mar  8 17:42:47: sipSPIIcpifUpdate :CallState: 4 Payout: 1255 DiscTime:66856757 ConnTime
66856294

*Mar  8 17:42:47: udpsock_close_connect: Socket fd: 1 closed for connid 1 with remote
port: 5060

```

Related Commands

Command	Description
debug ccsip all	Enables all SIP-related debugging.
debug ccsip calls	Shows all SIP Service Provider Interface (SPI) call tracing.
debug ccsip events	Shows all SIP SPI events tracing.

■ debug ccsip error

Command	Description
debug ccsip messages	Shows all SIP SPI message tracing.
debug ccsip states	Shows all SIP SPI state tracing.

debug ccsip events

To show all SIP SPI events tracing, enter the **debug ccsip events** command in privileged EXEC configuration mode. To disable debugging output, use the **no** form of this command.

debug ccsip events

no debug ccsip events

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	
12.1(1)T	This command was introduced.
12.1.(3)T	The output of the command was changed.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines This command traces the events posted to SIP SPI from all interfaces.

Examples From one side of the call, the debug output is as follows:

```
Router1# debug ccsip events

SIP Call events tracing is enabled
Router1#
*Mar 6 14:17:57: Queued event from SIP SPI : SIPSPI_EV_CC_CALL_SETUP
*Mar 6 14:17:57: Queued event from SIP SPI : SIPSPI_EV_CREATE_CONNECTION
*Mar 6 14:17:57: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 6 14:18:00: Queued event from SIP SPI : SIPSPI_EV_RECONNECT_CONNECTION
*Mar 6 14:18:00: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 6 14:18:04: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 6 14:18:04: Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_DISCONNECT
*Mar 6 14:18:04: Queued event from SIP SPI : SIPSPI_EV_CLOSE_CONNECTION
Router1#
```

From the other side of the call, the debug output is as follows:

```
Router2# debug ccsip events

SIP Call events tracing is enabled
Router2#
*Mar 8 17:43:55: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 8 17:43:55: Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_PROCEEDING
*Mar 8 17:43:55: Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_ALERTING
*Mar 8 17:43:55: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar 8 17:43:58: Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_CONNECT
```

■ debug ccsip events

```

*Mar  8 17:43:58: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar  8 17:44:01: Queued event From SIP SPI to CCAPI/DNS : SIPSPI_EV_CC_CALL_DISCONNECT
*Mar  8 17:44:01: Queued event from SIP SPI : SIPSPI_EV_CREATE_CONNECTION
*Mar  8 17:44:01: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
*Mar  8 17:44:01: Queued event from SIP SPI : SIPSPI_EV_CLOSE_CONNECTION

```

Related Commands

Command	Description
debug ccsip all	Enables all SIP-related debugging.
debug ccsip calls	Shows all SIP Service Provider Interface (SPI) call tracing.
debug ccsip error	Shows SIP SPI errors.
debug ccsip messages	Shows all SIP SPI message tracing.
debug ccsip states	Shows all SIP SPI state tracing.

debug ccsip messages

To show all SIP SPI message tracing, enter the **debug ccsip messages** command in privileged EXEC configuration mode. To disable debugging output, use the **no** form of this command.

debug ccsip messages

no debug ccsip messages

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	
12.1(1)T	This command was introduced.
12.1.(3)T	The output of the command was changed.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines This command traces the SIP messages exchanged between the SIP UA client (UAC) and the access server.

Examples From one side of the call, the debug output is as follows:

```
Router1# debug ccsip message

SIP Call messages tracing is enabled
Router1#
*Mar 6 14:19:14: Sent:
INVITE sip:3660210@166.34.245.231;user=phone;phone-context=unknown SIP/2.0
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Sat, 06 Mar 2002 19:19:14 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Cisco-Guid: 2881152943-2184249568-0-483551624
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Max-Forwards: 6
Timestamp: 731427554
Contact: <sip:3660110@166.34.245.230:5060;user=phone>
Expires: 180
Content-Type: application/sdp
Content-Length: 138

v=0
o=CiscoSystemsSIP-GW-UserAgent 5596 7982 IN IP4 166.34.245.230
s=SIP Call
t=0 0
```

```
c=IN IP4 166.34.245.230
m=audio 20762 RTP/AVP 0
```

```
*Mar 6 14:19:14: Received:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 2002 22:45:12 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Timestamp: 731427554
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Length: 0
```

```
*Mar 6 14:19:14: Received:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 2002 22:45:12 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Timestamp: 731427554
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 138
```

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 1193 7927 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20224 RTP/AVP 0
```

```
*Mar 6 14:19:16: Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27DBC6D8-1357
Date: Mon, 08 Mar 2002 22:45:12 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Timestamp: 731427554
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Contact: <sip:3660210@166.34.245.231:5060;user=phone>
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 138
```

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 1193 7927 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20224 RTP/AVP 0
```

```
*Mar 6 14:19:16: Sent:
ACK sip:3660210@166.34.245.231:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27DBC6D8-1357
Date: Sat, 06 Mar 2002 19:19:14 GMT
```

```

Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Max-Forwards: 6
Content-Type: application/sdp
Content-Length: 138
CSeq: 101 ACK

```

```

v=0
o=CiscoSystemsSIP-GW-UserAgent 5596 7982 IN IP4 166.34.245.230
s=SIP Call
t=0 0
c=IN IP4 166.34.245.230
m=audio 20762 RTP/AVP 0

```

```

*Mar 6 14:19:19: Received:
BYE sip:3660110@166.34.245.230:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 166.34.245.231:53600
From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27DBC6D8-1357
To: "3660110" <sip:3660110@166.34.245.230>
Date: Mon, 08 Mar 2002 22:45:14 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Max-Forwards: 6
Timestamp: 731612717
CSeq: 101 BYE
Content-Length: 0

```

```

*Mar 6 14:19:19: Sent:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 166.34.245.231:53600
From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27DBC6D8-1357
To: "3660110" <sip:3660110@166.34.245.230>
Date: Sat, 06 Mar 2002 19:19:19 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Timestamp: 731612717
Content-Length: 0
CSeq: 101 BYE

```

```
Router1#
```

From the other side of the call, the debug output is as follows:

```
Router2# debug ccsip message
```

```

SIP Call messages tracing is enabled
Router2#
*Mar 8 17:45:12: Received:
INVITE sip:3660210@166.34.245.231;user=phone;phone-context=unknown SIP/2.0
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Sat, 06 Mar 2002 19:19:14 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Cisco-Guid: 2881152943-2184249568-0-483551624
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Max-Forwards: 6
Timestamp: 731427554
Contact: <sip:3660110@166.34.245.230:5060;user=phone>
Expires: 180
Content-Type: application/sdp

```

Content-Length: 138

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 5596 7982 IN IP4 166.34.245.230
s=SIP Call
t=0 0
c=IN IP4 166.34.245.230
m=audio 20762 RTP/AVP 0
```

```
*Mar 8 17:45:12: Sent:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 2002 22:45:12 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Timestamp: 731427554
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Length: 0
```

```
*Mar 8 17:45:12: Sent:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>
Date: Mon, 08 Mar 2002 22:45:12 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Timestamp: 731427554
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 138
```

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 1193 7927 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20224 RTP/AVP 0
```

```
*Mar 8 17:45:14: Sent:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27DBC6D8-1357
Date: Mon, 08 Mar 2002 22:45:12 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Timestamp: 731427554
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Contact: <sip:3660210@166.34.245.231:5060;user=phone>
CSeq: 101 INVITE
Content-Type: application/sdp
Content-Length: 138
```

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 1193 7927 IN IP4 166.34.245.231
s=SIP Call
t=0 0
c=IN IP4 166.34.245.231
m=audio 20224 RTP/AVP 0
```

```

*Mar  8 17:45:14: Received:
ACK sip:3660210@166.34.245.231:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 166.34.245.230:55820
From: "3660110" <sip:3660110@166.34.245.230>
To: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27DBC6D8-1357
Date: Sat, 06 Mar 2002 19:19:14 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Max-Forwards: 6
Content-Type: application/sdp
Content-Length: 138
CSeq: 101 ACK

v=0
o=CiscoSystemsSIP-GW-UserAgent 5596 7982 IN IP4 166.34.245.230
s=SIP Call
t=0 0
c=IN IP4 166.34.245.230
m=audio 20762 RTP/AVP 0

*Mar  8 17:45:17: Sent:
BYE sip:3660110@166.34.245.230:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 166.34.245.231:53600
From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27DBC6D8-1357
To: "3660110" <sip:3660110@166.34.245.230>
Date: Mon, 08 Mar 2002 22:45:14 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
User-Agent: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Max-Forwards: 6
Timestamp: 731612717
CSeq: 101 BYE
Content-Length: 0

*Mar  8 17:45:17: Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 166.34.245.231:53600
From: <sip:3660210@166.34.245.231;user=phone;phone-context=unknown>;tag=27DBC6D8-1357
To: "3660110" <sip:3660110@166.34.245.230>
Date: Sat, 06 Mar 2002 19:19:19 GMT
Call-ID: ABBAE7AF-823100E2-0-1CD274BC@172.18.192.194
Server: Cisco VoIP Gateway/ IOS 12.x/ SIP enabled
Timestamp: 731612717
Content-Length: 0
CSeq: 101 BYE

```

Related Commands

Command	Description
debug ccsip all	Enables all SIP-related debugging.
debug ccsip calls	Shows all SIP Service Provider Interface (SPI) call tracing.
debug ccsip error	Shows SIP SPI errors.
debug ccsip events	Shows all SIP SPI events tracing.
debug ccsip states	Shows all SIP SPI state tracing.

debug ccsip states

To show all SIP SPI state tracing, enter the **debug ccsip states** command in privileged EXEC configuration mode. To disable debugging output, use the **no** form of this command.

debug ccsip states

no debug ccsip states

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	
12.1(1)T	This command was introduced.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines This command traces the state machine changes of SIP SPI and displays the state transitions.

Examples The following example shows all SIP SPI state tracing:

```
Router1# debug ccsip states

SIP Call states tracing is enabled
Router1#
*Jan 2 18:34:37.793:0x6220C634 :State change from (STATE_NONE, SUBSTATE_NONE) to
(STATE_IDLE, SUBSTATE_NONE)
*Jan 2 18:34:37.797:0x6220C634 :State change from (STATE_IDLE, SUBSTATE_NONE) to
(STATE_IDLE, SUBSTATE_CONNECTING)
*Jan 2 18:34:37.797:0x6220C634 :State change from (STATE_IDLE, SUBSTATE_CONNECTING) to
(STATE_IDLE, SUBSTATE_CONNECTING)
*Jan 2 18:34:37.801:0x6220C634 :State change from (STATE_IDLE, SUBSTATE_CONNECTING) to
(STATE_SENT_INVITE, SUBSTATE_NONE)
*Jan 2 18:34:37.809:0x6220C634 :State change from (STATE_SENT_INVITE, SUBSTATE_NONE) to
(STATE_REC'D_PROCEEDING, SUBSTATE_PROCEEDING_PROCEEDING)
*Jan 2 18:34:37.853:0x6220C634 :State change from (STATE_REC'D_PROCEEDING,
SUBSTATE_PROCEEDING_PROCEEDING) to (STATE_REC'D_PROCEEDING, SUBSTATE_PROCEEDING_ALERTING)
*Jan 2 18:34:38.261:0x6220C634 :State change from (STATE_REC'D_PROCEEDING,
SUBSTATE_PROCEEDING_ALERTING) to (STATE_ACTIVE, SUBSTATE_NONE)
*Jan 2 18:35:09.860:0x6220C634 :State change from (STATE_ACTIVE, SUBSTATE_NONE) to
(STATE_DISCONNECTING, SUBSTATE_NONE)
*Jan 2 18:35:09.868:0x6220C634 :State change from (STATE_DISCONNECTING, SUBSTATE_NONE) to
(STATE_DEAD, SUBSTATE_NONE)
*Jan 2 18:28:38.404: Queued event from SIP SPI :SIPSPI_EV_CLOSE_CONNECTION
```

Related Commands

Command	Description
debug ccsip all	Enables all SIP-related debugging.
debug ccsip calls	Shows all SIP Service Provider Interface (SPI) call tracing.
debug ccsip error	Shows SIP SPI errors.
debug ccsip events	Shows all SIP SPI events tracing.
debug ccsip messages	Shows all SIP SPI message tracing.

default

To reset the value of a SIP-related command to its default, enter the **default** command in SIP user agent configuration mode. To disable the default setting, use the **no** form of this command.

default { **inband-alerting** | **max-forwards** | **retry** { **invite** | **response** | **bye** | **cancel** } | **sip-server** | **timers** { *trying* | *connect* | *disconnect* | *expires* } || **transport** }

no default { **inband-alerting** | **max-forwards** | **retry** { **invite** | **response** | **bye** | **cancel** } | **sip-server** | **timers** { *trying* | *connect* | *disconnect* | *expires* } || **transport** }

Syntax Description

inband-alerting	Resets inband-alerting to its default, which means that tones are fed from the terminating gateway.
max-forwards	Resets max-forwards to its default of 6.
retry { invite response bye cancel }	Resets the specified retry to its default (6 for invite and response ; 10 for bye and cancel).
sip-server	Resets the sip-server to a null value.
timers { <i>trying</i> <i>connect</i> <i>disconnect</i> <i>expires</i> }	Resets the specified retry to its default (500 for trying, connect, and disconnect; 180000 for expires).
transport	Resets transport to the default of both UDP and TCP enabled.

Defaults

No default behavior or values.

Command Modes

SIP user agent configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example shows how to set inband-alerting to default value:

```
Router(config-sip-ua)# default inband-alerting
```

Related Commands

Command	Description
exit	Exits the SIP user agent configuration mode.
inband-alerting	Specifies an inband-alerting SIP header.
max-forwards	Specifies the maximum number of hops for a request.
no	Negates a command or set its defaults.

Command	Description
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a Session Initiation Protocol (SIP) INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
timers	Configures the SIP signaling timers.
transport	Enables SIP UA transport for TCP/UDP.

gw-accounting

To enable gateway-specific accounting, enter the **gw-accounting** command in global configuration mode. To disable gateway-specific accounting, use the **no** form of this command.

```
gw-accounting {h323 [vsa] | syslog | voip}
```

```
no gw-accounting {h323 [vsa] | syslog | voip}
```

Syntax Description	h323	Enables standard H.323 accounting using Internet Engineering Task Force (IETF) RADIUS attributes.
	vsa	(Optional) Enables H.323 accounting using RADIUS vendor-specific attributes (VSAs).
	syslog	Enables the system logging facility to output accounting information in the form of a system log message.
	voip	Enables generic gateway-specific accounting.

Defaults Disabled.

Command Modes Global configuration

Command History	Release	Modification
	11.3(6)NA2	This command was introduced.
	12.0(7)T	The vsa keyword was added.
	12.1(1)T	The voip keyword was added.
	12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
	12.2(2)XB1	This command was introduced on the Cisco AS5850.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers.
	12.2(11)T	Support was added for Cisco IOS Release 12.2(11)T.

Usage Guidelines There are three different methods of accounting:

- The **voip** method sends the call data record (CDR) to the RADIUS server. Use this method with the SIP feature.
- The **h323** method sends the CDR to the RADIUS server.
- The **syslog** method uses the system logging facility to record the CDRs.

Use this command if you configure the AAA accounting application. If you enable both **h323** and **syslog** simultaneously, CDRs are generated in both methods.

To collect basic start-stop connection accounting data, the gateway must be configured to support gateway-specific H.323 accounting functionality. The **gw-accounting** command enables you to send accounting data to the RADIUS server in one of four ways:

- Using standard IETF RADIUS accounting attribute/value (AV) pairs—This method is the basic method of gathering accounting data (connection accounting) according to the specifications defined by the IETF. Use the **gw-accounting h323** command to configure the standard IETF RADIUS method of applying H.323 gateway-specific accounting. [Table 4](#) shows the supported IETF RADIUS attributes.

Table 4 Supported IETF RADIUS Accounting Attributes

Number	Attribute	Description
30	Called-Station-Id	Allows the network access server to send the telephone number that the user called as part of the Access-Request packet (using Dialed Number Identification Service [DNIS] or similar technology). This attribute is supported only on ISDN and modem calls on the Cisco AS5200 and Cisco AS5300 universal access server if used with ISDN PRI.
31	Calling-Station-Id	Allows the network access server to send the telephone number that the call came from as part of the Access-Request packet (using Automatic Number Identification or similar technology). This attribute has the same value as “remote-addr” from TACACS+. This attribute is supported only on ISDN, and modem calls on the Cisco AS5200 and Cisco AS5300 universal access server if used with ISDN PRI.
42	Acct-Input-Octets	Indicates how many octets have been received from the port over the course of the accounting service being provided.
43	Acct-Output-Octets	Indicates how many octets have been sent to the port over the course of delivering the accounting service.
44	Acct-Session-Id	Indicates a unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session-Id numbers restart at 1 each time the router is power-cycled or the software is reloaded.
47	Acct-Input-Packets	Indicates how many packets have been received from the port over the course of this service being provided to a framed user.
48	Acct-Output-Packets	Indicates how many packets have been sent to the port in the course of delivering this service to a framed user.

For more information about RADIUS and the use of IETF-defined attributes, refer to the *Cisco IOS Security Configuration Guide*.

- Overloading the Acct-Session-Id field—Attributes that cannot be mapped to standard RADIUS are packed into the Acct-Session-Id attribute field as ASCII strings separated by the character “/”. The Acct-Session-Id attribute is defined to contain the RADIUS account session ID, which is a unique identifier that links accounting records associated with the same login session for a user. To support additional fields, we have defined the following string format for this field:

```
<session id>/<call leg setup time>/<gateway id>/<connection id>/<call origin>/
<call type>/<connect time>/<disconnect time>/<disconnect cause>/<remote ip address>
```

Table 5 shows the field attributes that you use with the overloaded session-ID method and a brief description of each.

Table 5 *Field Attributes in Overloaded Acct-Session-ID*

Field Attribute	Description
Session-Id	Specifies the standard RADIUS account session ID.
Setup-Time	Provides the Q.931 setup time for this connection in Network Time Protocol (NTP) format. NTP time formats are displayed as %H: %M: %S %k %Z %tw %tn %td %Y where: %H is hour (00 to 23). %M is minutes (00 to 59). %S is seconds (00 to 59). %k is milliseconds (000 to 999). %Z is timezone string. %tw is day of week (Saturday through Sunday). %tn is month name (January through December). %td is day of month (01 to 31). %Y is year including century (for example, 1998).
Gateway-Id	Indicates the name of the underlying gateway in the form "gateway.domain_name."
Call-Origin	Indicates the origin of the call relative to the gateway. Possible values are originate and answer .
Call-Type	Indicates the call leg type. Possible values are telephony and VoIP .
Connection-Id	Specifies the unique global identifier used to correlate call legs that belong to the same end-to-end call. The field consists of 4 long words (128 bits). Each long word is displayed as a hexadecimal value and is separated by a space character.
Connect-Time	Provides the Q.931 connect time for this call leg, in NTP format.
Disconnect-Time	Provides the Q.931 disconnect time for this call leg, in NTP format.
Disconnect-Cause	Specifies the reason a call was taken offline as defined in the Q.931 specification.
Remote-IP-Address	Indicates the address of the remote gateway port where the call is connected.

Because of the limited size of the Acct-Session-Id string, it is not possible to embed very many information elements in it. Therefore, this feature supports only a limited set of accounting information elements.

Use the **gw-accounting h323** command to configure the overloaded session ID method of applying H.323 gateway-specific accounting.

- Using vendor-specific RADIUS attributes—The IETF draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (Attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option has vendor-type 1, which is named “cisco-avpair.” The value is a string of the format:

```
protocol: attribute sep value *
```

“Protocol” is a value of the Cisco “protocol” attribute for a particular type of authorization. “Attribute” and “value” are an appropriate attribute/value (AV) pair defined in the Cisco TACACS+ specification, and “sep” is “=” for mandatory attributes and “*” for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

The VSA fields and their ASCII values are listed in [Table 6](#).

Table 6 VSA Fields and Their ASCII Values

IETF RADIUS Attribute	Vendor-Specific Company Code	Subtype Number	Attribute Name	Description
26	9	23	h323-remote-address	Indicates the IP address of the remote gateway.
26	9	24	h323-conf-id	Identifies the conference ID.
26	9	25	h323-setup-time	Indicates the setup time for this connection in Coordinated Universal Time (UTC) formerly known as Greenwich Mean Time (GMT) and Zulu time.
26	9	26	h323-call-origin	Indicates the origin of the call relative to the gateway. Possible values are originating and terminating (answer).
26	9	27	h323-call-type	Indicates the call leg type. Possible values are telephony and VoIP .
26	9	28	h323-connect-time	Indicates the connection time for this call leg in UTC.
26	9	29	h323-disconnect-time	Indicates the time this call leg was disconnected in UTC.
26	9	30	h323-disconnect-cause	Specifies the reason a connection was taken offline per the Q.931 specification.
26	9	31	h323-voice-quality	Specifies the impairment factor (ICPIF) affecting voice quality for a call.
26	9	33	h323-gw-id	Indicates the name of the underlying gateway.

Use the **gw-accounting h323 vsa** command to configure the VSA method of applying H.323 gateway-specific accounting.

- Using syslog records—The syslog accounting option exports the information elements associated with each call leg through a system log message, which can be captured by a syslog daemon on the network. The syslog output consists of the following:

```
<server timestamp> <gateway id> <message number> : <message label> : <list of AV pairs>
```

The syslog message fields are listed in [Table 7](#).

Table 7 Syslog Message Output Fields

Field	Description
server timestamp	The time stamp created by the server when it receives the message to log.
gateway id	The name of the gateway that emits the message.
message number	The number assigned to the message by the gateway.
message label	A string used to identify the message category.
list of AV pairs	A string that consists of <attribute name> <attribute value> pairs separated by commas.

Use the **gw-accounting syslog** command to configure the syslog record method of gathering H.323 accounting data.

Use this command if you configure the AAA accounting application.

If you enable both **h323** and **syslog** simultaneously, CDRs are generated in both methods.

Examples

The following example shows how to configure accounting using RADIUS to output accounting CDRs. Both H.323 and SIP protocols can use this method.

```
Router(config)# gw-accounting voip
```

The following example configures basic H.323 accounting using IETF RADIUS attributes:

```
gw-accounting h323
```

The following example configures H.323 accounting using VSA RADIUS attributes:

```
gw-accounting h323 vsa
```

The following example enables gateway-specific accounting and defines the accounting method as **voip**:

```
gw-accounting voip
```

Related Commands

Command	Description
inband-alerting	Enables inband alerting so that the originating gateway can open an early media path (upon receiving a 180 or 183 message with a SDP body).

inband-alerting

To enable inband alerting, enter the **inband-alerting** command in the SIP user agent configuration mode. Use the **no** form of this command to disable inband alerting.

[no] inband-alerting

Syntax Description There are no arguments or keywords for this command.

Defaults By default, inband alerting is enabled.

Command Modes SIP user agent configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.1(3)T	This command was limited to enabling and disabling inband alerting.
	12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
	12.2(2)XB1	This command was introduced on the Cisco AS5850.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines If inband alerting is enabled, the originating gateway can open an early media path (upon receiving a 180 or 183 message with a SDP body). This allows the terminating gateway or switch to feed tones or announcements before the call is connected. If inband-alerting is disabled, local alerting is generated on the originating gateway.

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

Examples The following example shows how to disable inband alerting:

```
Router(config)# sip-ua
Router(config-sip-ua)# no inband-alerting
```

Related Commands	Command	Description
	default	Sets a command to its default.
	exit	Exits the SIP user agent configuration mode.
	max-forwards	Specifies the maximum number of hops for a request.
	no	Negates a command or set its defaults.
	retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.

Command	Description
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a Session Initiation Protocol (SIP) INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
timers	Configures the SIP signaling timers.
transport	Enables SIP UA transport for TCP/UDP.

max-forwards

To set the maximum number of proxy or redirect servers that can forward a request, enter the **max-forwards** command in SIP user agent configuration mode. To reset this command to the default value, use the **no** form of this command.

max-forwards *number*

no max-forwards *number*

Syntax Description	<i>number</i>	Number of hops. Possible values are 1 through 15. The default is 6.
---------------------------	---------------	---

Defaults	The default number of hops is 6.
-----------------	----------------------------------

Command Modes	SIP user agent configuration
----------------------	------------------------------

Command History	Release	Modification
	12.1(3)T	This command was introduced.
	12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
	12.2(2)XB1	This command was supported on the Cisco AS5850.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines	To reset this command to the default value, you can also use the default command.
-------------------------	--

Examples	The following example shows how to set the number of proxy or redirect servers that can forward a request to two:
-----------------	---

```
Router(config)# sip-ua
Router(config-sip-ua)# max-forwards 2
```

Related Commands	Command	Description
	default	Sets a command to its default.
	exit	Exits the SIP user agent configuration mode.
	inband-alerting	Specifies an inband-alerting SIP header.
	no	Negates a command or set its defaults.

Command	Description
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a Session Initiation Protocol (SIP) INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry relxx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
timers	Configures the SIP signaling timers.
transport	Enables SIP UA transport for TCP/UDP.

max-redirects

To set the maximum number of redirect servers that a call can traverse, enter the **max-redirects** command in dial-peer configuration mode. To reset this command to the default value, use the **no** form of this command.

max-redirects *number*

no max-redirects *number*

Syntax Description	<i>number</i>	Maximum number of redirect servers that a call can traverse. Possible values are 1 through 10. The default is 1.
---------------------------	---------------	--

Defaults	The default number of redirects is 1.
-----------------	---------------------------------------

Command Modes	Dial-peer configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
	12.2(2)XB1	This command was introduced on the Cisco AS5850.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series. This command does not support the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
	12.2(11)T	Support was added for Cisco IOS Release 12.2(11)T.

Examples The following example shows how to set the number of redirect servers that a call can traverse to one:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# max-redirects 2
```

Related Commands	Command	Description
	default	Sets a command to its default.
	exit	Exits the SIP user agent configuration mode.
	inband-alerting	Specifies an inband-alerting SIP header.
	max-forwards	Specifies the maximum number of hops for a request.
	no	Negates a command or set its defaults.
	retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.

Command	Description
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a Session Initiation Protocol (SIP) INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
timers	Configures the SIP signaling timers.
transport	Enables SIP UA transport for TCP/UDP.

session protocol

To configure a VoIP dial peer to use either H323 or SIP as the session protocol for VoIP call signaling, enter the **session protocol** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

```
session protocol { aal2-trunk | cisco | sipv2 | smtp }
```

```
no session protocol
```

Syntax Description	Command	Description
	aal2-trunk	Dial peer uses ATM adaptation layer 2 (AAL2) nonswitched trunk session protocol.
	cisco	Configure the dial peer to use proprietary Cisco VoIP session protocol.
	sipv2	Configures the dial peer to use IETF SIP. SIP users should use this new option.
	smtp	Dial peer uses Simple Mail Transfer Protocol (SMTP) session protocol.

Defaults No default behavior or values.

Command Modes Dial-peer configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced.
	12.0(3)XG	The cisco option was added.
	12.0(4)XJ	This command was modified for store-and-forward fax on Cisco AS5300 universal access servers.
	12.1(1)XA	This command was implemented for VoATM dial peers on Cisco MC3810 multiservice access concentrators, and the aal2-trunk keyword was added.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T, and the sipv2 keyword was added.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
	12.2(2)T	This command was implemented on Cisco 7200 series routers.
	12.2(4)T	This command was introduced on Cisco 1750 access routers.
	12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
	12.2(2)XB1	This command was introduced on the Cisco AS5850.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. This command is not supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release. Note The aal2-trunk and smtp keywords are not supported on Cisco 7200 series routers.
	12.2(11)T	Support was added for Cisco IOS Release 12.2(11)T.

Usage Guidelines

The **cisco** keyword is applicable only to VoIP on the Cisco 1750, Cisco 1751, Cisco 3600 series, and Cisco 7200 series routers.

The **aal2-trunk** keyword is applicable only to VoATM on the Cisco MC3810 multiservice access concentrator and the Cisco 7200 series router.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example shows how to configure the dial peer to use IETF SIP:

```
Router(config)# dial-peer voice 102 voip
Router(config-dial-peer)# session protocol sipv2
```

The following example shows that AAL2 trunking has been configured as the session protocol:

```
dial-peer voice 10 voatm
 session protocol aal2-trunk
```

The following example shows that Cisco session protocol has been configured as the session protocol:

```
dial-peer voice 20 voip
 session protocol cisco
```

Related Commands

Command	Description
session target (VoIP)	Specifies a network-specific address for a dial peer.
session transport	Configures the VoIP dial peer to use TCP or UDP as the underlying transport layer protocol for SIP messages.

session target (VoIP)

To designate a network-specific address to receive calls from this VoIP dial peer, use the **session target** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 1751, Cisco 3725, Cisco 3745, Cisco AS5300

```
session target { ipv4:destination-address | dns:[$s$. | $d$. | $u$. | $e$.] host-name |
enum:table-num | loopback:rtp | ras | sip-server }
```

```
no session target
```

Cisco 2600 Series, Cisco 3600 Series, Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco MC8310

```
session target { ipv4:destination-address | dns:[$s$. | $d$. | $e$. | $u$.] host-name |
enum:table-num | loopback:rtp | ras | settlement provider-number | sip-server }
```

```
no session target
```

Cisco AS5800

```
session target { ipv4:destination-address | dns:[$s$. | $d$. | $e$. | $u$.] host-name |
enum:table-num | loopback:rtp }
```

```
no session target
```

Syntax Description

ipv4:destination-address	IP address of the dial peer to receive calls.
dns:[<i>\$s\$</i>...] host-name	The domain name server resolves the name of the dial peer to receive calls. Valid entries for this parameter are characters representing the name of the host device. (Optional) Use one of the following macros with this keyword when defining the session target for Voice over IP (VoIP) peers: <ul style="list-style-type: none"> <i>\$s\$</i>.—The source destination pattern is used as part of the domain name. <i>\$d\$</i>.—The destination number is used as part of the domain name. <i>\$e\$</i>.—The digits in the called number are reversed and periods are added between the digits of the called number. The resulting string is used as part of the domain name. <i>\$u\$</i>.—The unmatched portion of the destination pattern (such as a defined extension number) is used as part of the domain name. host-name—String that contains the complete host name to be associated with the target address; for example, serverA.mycompany.com.
enum:table-num	ENUM search table number. Range is 1 to 15.
loopback:rtp	All voice data is looped back to the source.
ras	Registration, admission, and status (RAS) signaling function protocol is being used, meaning that a gatekeeper is consulted to translate the E.164 address into an IP address.

settlement <i>provider-number</i>	The settlement server is the target to resolve the terminating gateway address. The argument is as follows: <ul style="list-style-type: none"> <i>provider-number</i>—Provider IP address.
sip-server	The global Session Initiation Protocol (SIP) server is the destination for calls from this dial peer.

Defaults

Enabled, with no IP address or domain name defined.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)T	This command was implemented on the Cisco AS5300. The ras keyword was introduced.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.1(1)T	The settlement <i>provider-number</i> keyword-argument pair and the sip-server keyword were introduced.
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 integrated into Cisco IOS Release 12.2(8)T. This command is not supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)T	Support was added for Cisco IOS Release 12.2(11)T on the Cisco AS5300, Cisco AS5350, and Cisco AS5400. The enum keyword was introduced.

Usage Guidelines

Use this command to specify a network-specific destination for a dial peer to receive calls from this dial peer. You can select an option to define a network-specific address or domain name as a target, or you can select one of several methods to automatically determine the destination for calls from this dial peer.

Use the **session target dns** command with or without the specified macros. Using the optional macros can reduce the number of VoIP dial peer session targets you must configure if you have groups of numbers associated with a particular router.

The **session target enum** command instructs the dial peer to use a table of translation rules to convert the dialed number identification service (DNIS) number into a number in E.164 format. This translated number is sent to a DNS server that contains a collection of URLs. These URLs identify each user as a destination for a call and may represent various access services, such as SIP, H.323, telephone, fax, email, instant messaging, and personal web pages. Before assigning the session target to the dial peer, configure an ENUM match table with the translation rules using the **voice enum-match-table** command in global configuration mode. The table is identified in **session target enum** as *table-num*.

Use the **session target loopback** command to test the voice transmission path of a call. The loopback point depends on the call origin.

Use the **session target ras** command to specify that the RAS protocol is being used to determine the IP address of the session target.

In Cisco IOS Release 12.1(1)T the **session target** command configuration cannot combine the target of RAS with the **settle-call** command.

If the **session target** type is **settlement** when the VoIP dial peers are configured for a settlement server, the *provider-number* parameter in the **session target** and **settle-call** commands should be identical.

Use the **session target sip-server** command to name the global SIP server interface as the destination for calls from this dial peer. You must first define the SIP server interface by using the **sip-server** command in SIP user-agent configuration mode. Then you can enter the **session target sip-server** option for each dial peer instead of having to enter the entire IP address for the SIP server interface under each dial peer.

Examples

The following example creates a session target using DNS for a host named “voice_router” in the domain cisco.com:

```
dial-peer voice 10 voip
 session target dns:voice_router.cisco.com
```

The following example creates a session target using DNS with the optional **\$u\$** macro. In this example, the destination pattern ends with four periods (.) to allow for any four-digit extension that has the leading numbers 1310222.

The optional macro **\$u\$** directs the gateway to use the unmatched portion of the dialed number—in this case, the four-digit extension—to identify a dial peer. As in the preceding example, the domain is “cisco.com.”

```
dial-peer voice 10 voip
 destination-pattern 1310222....
 session target dns:$u$.cisco.com
```

The following example creates a session target using DNS, with the optional **\$d\$** macro. In this example, the destination pattern has been configured for 13102221111. The optional macro **\$d\$** directs the gateway to use the destination pattern to identify a dial peer in the “cisco.com” domain.

```
dial-peer voice 10 voip
 destination-pattern 13102221111
 session target dns:$d$.cisco.com
```

The following example creates a session target using DNS, with the optional **\$e\$** macro. In this example, the destination pattern has been configured for 12345. The optional macro **\$e\$** directs the gateway to do the following: reverse the digits in the destination pattern, add periods between the digits, and use this reverse-exploded destination pattern to identify the dial peer in the “cisco.com” domain.

```
dial-peer voice 10 voip
 destination-pattern 12345
 session target dns:$e$.cisco.com
```

The following example creates a session target using an ENUM table. It indicates that calls made using dial peer 100 should use the preferential order of rules in enum match table 3.

```
dial-peer voice 101 voip
 session target enum: 3
```

The following example creates a session target using RAS:

```
dial-peer voice 11 voip
 destination-pattern 13102221111
 session target ras
```

The following example creates a session target using settlement:

■ session target (VoIP)

```
dial-peer voice 24 voip
  session target settlement:0
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.
settle-call	Specifies that settlement is to be used for the specified dial peer, regardless of session target type.
sip-server	Defines a network address for the SIP server interface.
voice enum-match-table	Initiates the ENUM match table definition.

session transport

To configure the VoIP dial peer to use TCP or UDP as the underlying transport layer protocol for SIP messages, enter the **session transport** command in dial-peer configuration mode. To reset the value of this command to the default, use the **no** form of this command.

```
session transport {udp | tcp}
```

```
no session transport {udp | tcp}
```

Syntax Description	Command	Description
	udp	Configures the SIP dial peer to use the UDP transport layer protocol. This is the default.
	tcp	Configures the SIP dial peer to use the TCP transport layer protocol.

Defaults

The default for this command is that the SIP dial peer uses UDP.



Note

The transport protocol specified with the **transport command** and the one specified with the **session transport** command must be the same.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Use the **show sip-ua status** command in privileged EXEC configuration mode to ensure that the transport protocol that you set using the **session transport** command matches the protocol set using the **transport** command. This command is used in a dial-peer configuration mode to specify the SIP transport method, either UDP or TCP.

Examples

The following example shows how to configure the SIP dial peer to use the UDP transport layer protocol:

```
Router(config)# dial-peer voice 102 voip
Router(dial-peer-config)# session transport udp
```

Related Commands	Command	Description
	session protocol	Configures a VoIP dial peer to use either H323 or SIP as the session protocol for VoIP call signaling
	session target (VoIP)	Specifies a network-specific address for a dial peer.

show sip-ua statistics

To display response, traffic, and retry SIP UA statistics, enter the **show sip-ua statistics** command in privileged EXEC configuration mode.

show sip-ua statistics

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced.
	12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
	12.2(2)XB	Command output was enhanced to display the following: BadRequest counter (400 class) now counts Malformed Via entries, Reliable provisional responses (PRACK/re1xx), Conditions met (COMET), and Notify responses.
	12.2(2)XB1	This command was introduced on the Cisco AS5850.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. This command is not supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms in this release. For the purposes of display, this command was separated from the generic show sip-ua command found previously in this reference.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines Use this command to verify SIP configurations.

Examples The following example shows response, traffic, and retry SIP UA statistics:

```
Router# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
Informational:
  Trying 0/0, Ringing 0/0,
  Forwarded 0/0, Queued 0/0,
  SessionProgress 0/0
Success:
  OkInvite 0/0, OkBye 0/0,
  OkCancel 0/0, OkOptions 0/0
Redirection (Inbound only):
  MultipleChoice 0, MovedPermanently 0,
```

■ show sip-ua statistics

```

MovedTemporarily 0, SeeOther 0,
UseProxy 0, AlternateService 0
Client Error:
BadRequest 0/0, Unauthorized 0/0,
PaymentRequired 0/0, Forbidden 0/0,
NotFound 0/0, MethodNotAllowed 0/0,
NotAcceptable 0/0, ProxyAuthReqd 0/0,
ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
LengthRequired 0/0, ReqEntityTooLarge 0/0,
ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
BadExtension 0/0, TempNotAvailable 0/0,
CallLegNonExistent 0/0, LoopDetected 0/0,
TooManyHops 0/0, AddrIncomplete 0/0,
Ambiguous 0/0, BusyHere 0/0
Server Error:
InternalServerError 0/0, NotImplemented 0/0,
BadGateway 0/0, ServiceUnavail 0/0,
GatewayTimeout 0/0, BadSipVer 0/0
Global Failure:
BusyEverywhere 0/0, Decline 0/0,
NoExistAnywhere 0/0, NotAcceptable 0/0

SIP Total Traffic Statistics (Inbound/Outbound)
Invite 0/0, Ack 0/0, Bye 0/0,
Cancel 0/0, Options 0/0

Retry Statistics
Invite 0, Bye 0, Cancel 0, Response 0

```

Table 8 show sip-ua statistics Field Descriptions

Field	Description
Note	When 0/0 is included in a field, the first number is an inbound count and the second number is an outbound count.
Note	For each field, the standard RFC2543 SIP response number and message are shown.
Ack 0/0	A confirmed final response received/sent.
Accepted 0/0	202 Indicates a successful response to a Refer request received/sent.
AddrIncomplete 0/0	484 Address supplied is incomplete.
AlternateService 0	380 Unsuccessful call; however, an alternate service is available.
Ambiguous 0/0	485 Address supplied is ambiguous.
BadExtension 0/0	420 Server could not understand the protocol extension in the Require header.
BadGateway 0/0	502 Network is out of order.
BadRequest	400 Bad Request (includes the malformed Via header).
BadSipVer 0/0	505 Requested SIP version is not supported.
BusyEverywhere 0/0	600 Called party is busy.
BusyHere 0/0	486 Called party is busy.
Bye 0	Number of times that a Bye request is retransmitted to the other user agent.
Bye 0/0	Terminated the session.

Table 8 *show sip-ua statistics Field Descriptions (continued)*

Field	Description
CallLegNonExistent 0/0	481 Server is ignoring the request, which was either a Bye request and there was not a matching leg ID, or a Cancel request and there was not a matching transaction.
Cancel 0	Number of times that a Cancel request is retransmitted to the other user agent.
Cancel 0/0	Terminated the pending request.
Client Error:	4xx Client error.
Comet 0	Number of times that a COMET request is retransmitted to the other user agent.
Comet 0/0	Conditions have been met.
Conflict 0/0	409 Temporary failure.
Decline 0/0	603 Call rejected.
Forbidden 0/0	403 IP server has the request, but cannot provide service.
Forwarded 0/0	181 Call has been forwarded.
GatewayTimeout 0/0	504 Server or gateway did not receive a timely response from another server (such as a location server).
Global Failure:	6xx Called party does not exist anywhere.
Gone 0/0	410 Resource is no longer available at the server, and no forwarding address is known.
Informational:	1xx b Informational response.
InternalError 0/0	500 Server or gateway encountered an unexpected error that prevented it from processing the request.
Invite 0	Number of times that an INVITE request is retransmitted to the other user agent.
Invite 0/0	Initiated a call.
LengthRequired 0/0	411 A content length is required.
LoopDetected 0/0	482 A loop—server received a request that included itself in the path.
MethodNotAllowed 0/0	405 Method specified in the request is not allowed.
MovedPermanently 0	301 User is no longer available at this location.
MovedTemporarily 0	302 User is temporarily unavailable.
MultipleChoice 0	300 Address resolves to more than one location.
NotAcceptable 0/0	406/606 Call was contacted, but some aspect of the session description was unacceptable.
NotAcceptableMedia 0/0	406 Call was contacted, but some aspect of the session description was unacceptable.
NotExistAnywhere 0/0	604 Server has authoritative information that the called party does not exist in the network.
NotFound 0/0	404 Called party does not exist in the specified domain.

Table 8 *show sip-ua statistics Field Descriptions (continued)*

Field	Description
Notify 0	Number of times that a Notify is retransmitted to the other user agent.
Notify 0/0	Number of Notify messages received/sent.
NotImplemented 0/0	501 Service or option not implemented in the server or gateway.
OkBye 0/0	200 A successful response to a Bye request.
OkCancel 0/0	200 A successful response to a Cancel request.
OkInvite 0/0	200 A successful response to an INVITE request.
OkNotify 0/0	200 A successful response to a Notify request.
OkOptions 0/0	200 A successful response to an Options request.
OkPrack 0/0	200 A successful response to a PRACK request.
OkPreconditionMet 0/0	200 A successful response to a PreconditionMet request.
Options 0/0	Query the receiving/sending server as to its capabilities.
PaymentRequired 0/0	402 Payment is required to complete the call.
Prack 0	Number of times that a PRACK request is retransmitted to the other user agent.
Prack 0/0	Provisional response received/sent.
PreCondFailure 0/0	580 Session could not be established because of failure to meet required preconditions.
ProxyAuthReqd 0/0	407 Rejected for proxy authentication.
Queued 0/0	182 Until the called party is available, the message is queued.
Redirection (Inbound only):	3xx Called party is not available at the address used in the request; reissue.
Refer 0/0	Number of Refer requests received/sent.
Reliable1xx 0	Number of times the Reliable 1xx response is retransmitted to the other user agent.
ReqEntityTooLarge 0/0	413 Server refuses to process request because the request is larger than is acceptable.
ReqURITooLarge 0/0	414 Server refuses to process, because the URI (URL) request is larger than is acceptable.
ReqTimeout 0/0	408 Server could not produce a response before the Expires timeout.
RequestCancel 0/0	Request has been cancelled.
Response 0	Number of Response retries.
Retry Statistics	One of the three categories of response statistics.
Ringling 0/0	180 Called party has been located and is being notified of the call.
SeeOther 0	303 Transfer to another address.
Server Error:	5xx Server error.
ServiceUnavail 0/0	503 Service option is not available because of an overload or maintenance problem.

Table 8 *show sip-ua statistics Field Descriptions (continued)*

Field	Description
SessionProgress 0/0	183 Indicates inband alerting.
SIP Response Statistics (Inbound/Outbound)	One of the three categories of response statistics.
SIP Total Traffic Statistics (Inbound/Outbound)	One of the three categories of response statistics.
Success	2xx Request understood and performed.
TempNotAvailable 0/0	480 Called party did not respond.
TooManyHops 0/0	483 Server received a request that required more hops than is allowed by the Max-Forward header.
Trying 0/0	100 Action is being taken with no resolution.
Unauthorized 0/0	401 Request requires user authentication.
UnsupportedMediaType 0/0	415 Server refuses to process a request because the service option is not available on the destination endpoint.
UseProxy 0	305 Caller must use a proxy to contact called party.

Related Commands

Command	Description
show sip-ua status	Displays SIP UA status.
show sip-ua timers	Displays the current settings for SIP UA timers.

show sip-ua status

To display SIP UA status, enter the **show sip-ua status** command in privileged EXEC configuration mode to display SIP status.

show sip-ua status

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.1(3)T	The statistics portion of the output was removed and is now included in the show sip-ua statistics command.
	12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
	12.2(2)XB1	This command was introduced on the Cisco AS5850.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. This command is not supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms in this release. For the purposes of display, this command was separated from the generic show sip-ua command found previously in this reference.
	12.2(11)T	This command was supported in Cisco IOS Release 12.2(11)T.

Usage Guidelines Use this command to verify SIP configurations.

Examples The following example displays SIP UA status:

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP max-forwards :6
```

Table 9 describes significant fields in this output.

Table 9 *show sip-ua status Field Descriptions*

Field	Description
SIP User Agent Status	UA status.
SIP User Agent for UDP	UDP is enabled or disabled.
SIP User Agent for TCP	TCP is enabled or disabled.
SIP User Agent bind status (signaling)	Binding for signaling is enabled or disabled.
SIP User Agent bind status (media)	Binding for media is enabled or disabled.
SIP max-forwards	Value of max-forwards of SIP messages.
SIP DNS SRV version	Style of DNS SRV query: 1 for RFC 2052 or 2 for RFC 2782.

Related Commands

Command	Description
show sip-ua statistics	Displays response, traffic, and retry SIP UA statistics.
show sip-ua timers	Displays the current settings for SIP UA timers.

show sip-ua timers

To display the current settings for SIP UA timers, enter the **show sip-ua timers** command in privileged EXEC configuration mode.

show sip-ua timers

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.1(3)T	The output of this command was changed to reflect the changes in the timers command.
	12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
	12.2(2)XB	Command output was enhanced to display the following: Reliable provisional responses (PRACK/rel 1xx), Conditions met (COMET), and Notify responses.
	12.2(2)XB1	This command was introduced on the Cisco AS5850.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. This command is not supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms in this release. For the purposes of display, this command was separated from the generic show sip-ua command found previously in this reference.
	12.2(11)T	This command was supported in Cisco IOS Release 12.2(11)T.

Examples The following examples displays SIP UA timers values:

```
Router# show sip-ua timers

SIP UA Timer Values (milliseconds)
trying 500, expires 150000, connect 500, disconnect 500
comet 500, prack 500, rel1xx 500, notify 500
```

Table 10 describes significant fields in this output.

Table 10 *show sip-ua timers Field Descriptions*

Field	Description
SIP UA Timer Values (milliseconds)	SIP UA timer status.
trying	Time to wait before a Trying message is retransmitted.
expires	Time to wait before an Expires message is retransmitted.
connect	Time to wait before a Connect message is retransmitted.
disconnect	Time to wait before a Disconnect message is retransmitted.
comet	Time to wait before a COMET message is retransmitted.
prack	Time to wait before a PRACK acknowledgment is retransmitted.
rel1xx	Time to wait before a Rel1xx response is retransmitted.
notify	Time to wait before a Notify response is retransmitted.

Related Commands

Command	Description
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP status.
show sip-ua retry	Displays SIP retry statistics.
sip-ua	Enables the SIP user-agent configuration commands.
timers comet	Sets the amount of time that the user agent should wait before retransmitting COMET requests.
timers prack	Sets the amount of time that the user agent should wait before retransmitting the PRACK requests.
timers rel1xx	Sets the amount of time that the user agent should wait before retransmitting the reliable 1xx responses.

sip-server

To configure a network address for the SIP server interface, enter the **sip-server** command in SIP user agent configuration mode. To disable, use the **no** form of this command.

```
sip-server { dns:[host-name] | ipv4:ipaddr [:port-num]}
```

```
no sip-server { dns:[host-name] | ipv4:ipaddr [:port-num]}
```

Syntax Description

dns:	Sets the global SIP server interface to a DNS host name. If you do not specify a host name, the default DNS defined by the ip name-server command is used.
<i>host-name</i>	Specifies the DNS host name. A DNS host name takes the following format: name.gateway.xyz
ipv4:ipaddr	Sets the global SIP server interface to an IP address. A valid IP address takes the following format: xxx.xxx.xxx.xxx
<i>:port-num</i>	(Optional) Specifies the port number for the SIP server.

Defaults

The default for this command is a null value.

Command Modes

SIP user agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on Cisco 7200 series routers. This command is not supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms in this release.
12.2(11)T	This command was supported in Cisco IOS Release 12.2(11)T.

Usage Guidelines

You can specify **session target sip-server** for each dial peer instead of repeatedly entering the SIP server interface address for each dial peer. To reset this command to a null value, use the **default** command.

Examples

The following example shows how to set the global SIP server interface to a DNS host name and specify an IP address. If you do not specify a host name, the default DNS defined by the **ip name-server** command is used.

```
Router(config)# sip-ua  
Router(config-sip-ua)# sip-server dns:UA-1-f0.sip.com
```

Related Commands

Command	Description
sip-ua	Enables the sip-ua configuration commands to configure the user agent.

sip-ua

To enable the sip-ua configuration commands to configure the user agent, enter the **sip-ua** command in global configuration mode. To reset all 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.

Defaults No default behavior or values.

Command Modes Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Use the **sip-ua** command to enter the SIP user agent-configuration sub-mode. The table below lists the sub-mode configuration commands.

Sub-Mode Command	Description
default	Sets a command to its default.
exit	Exits the SIP user agent configuration mode.
inband-alerting	Specifies an inband-alerting SIP header.
max-forwards	Specifies the maximum number of hops for a request.
no	Negates a command or set its defaults.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
retry invite	Configures the number of times that a Session Initiation Protocol (SIP) INVITE request is retransmitted to the other user agent.
retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.

Sub-Mode Command	Description
retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
sip-server	Configures a SIP server interface.
timers	Configures the SIP signaling timers configuration.
transport	Enables SIP UA transport for TCP/UDP.

Examples

The following example shows sub-command options available in config-sip-ua configuration mode:

```
Router(config)# sip-ua
Router(config-sip-ua)# ?
```

SIP UA configuration commands:

```
default      Set a command to its defaults
exit         Exit from sip-ua configuration mode
inband-alerting Specify an Inband-alerting SIP header
max-forwards Change number of max-forwards for SIP Methods
no           Negate a command or set its defaults
retry        Change default retries for each SIP Method
sip-server   Configure a SIP Server Interface
timers       SIP Signaling Timers Configuration
transport    Enable SIP UA transport for TCP/UDP
```

Related Commands

Command	Description
sip-server	Configures a network address for the SIP server interface.

timers

To configure the SIP signaling timers, enter the **timers** command in SIP user agent configuration mode. To reset to the default value, use the **no** form of this command.

timers { *trying number* | *connect number* | *disconnect number* | *expires number* }

no timers

Syntax Description

<i>trying number</i>	Time (in milliseconds) to wait for a 100 response to an INVITE request. Possible values are 100 through 1000. The default is 500.
<i>connect number</i>	Time (in milliseconds) to wait for a 200 response to an ACK request. Possible values are 100 through 1000. The default is 500.
<i>disconnect number</i>	Time (in milliseconds) to wait for a 200 response to a BYE request. Possible values are 100 through 1000. The default is 500.
<i>expires number</i>	Time (in milliseconds) for which an INVITE request is valid. Possible values are 60000 through 300000. The default is 180000.

Defaults

The default for trying, connect, and disconnect is 500. The default for expires is 180,000.

Command Modes

SIP user agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.1(3)T	This command was modified. The names of the parameters were changed. Two of the keywords (<i>invite-wait-180</i> and <i>invite-wait-200</i>) were combined into one (<i>trying</i>).
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

If you used an earlier version of this command to configure timers, the timer settings are maintained. The output of the **show running configuration** command reflects both previous and current timers.

To reset this command to the default value, you can also use the **default** command.

Examples

The following example sets the trying timers to the default of 500.

```
Router(config)# sip-ua
Router(config-sip-ua)# timers trying 500
```

Related Commands	Command	Description
	default	Sets a command to its default.
	exit	Exits the SIP user agent configuration mode.
	inband-alerting	Specifies an inband-alerting SIP header.
	max-forwards	Specifies the maximum number of hops for a request.
	no	Negates a command or set its defaults.
	retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
	retry cancel	Configures the number of times that a CANCEL request is retransmitted to the other user agent.
	retry comet	Configures the number of times that a COMET request is retransmitted to the other user agent.
	retry invite	Configures the number of times that a Session Initiation Protocol (SIP) INVITE request is retransmitted to the other user agent.
	retry notify	Configures the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request.
	retry prack	Configures the number of times that the PRACK request is retransmitted to the other user agent.
	retry rel1xx	Configures the number of times that the reliable 1xx response is retransmitted to the other user agent.
	retry response	Configures the number of times that the RESPONSE message is retransmitted to the other user agent.
	transport	Enables SIP UA transport for TCP/UDP.

transport

To configure the SIP user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP or UDP socket, enter the **transport** command in SIP user agent configuration mode. To block reception of SIP signaling messages on a particular socket, use the **no** form of this command.

transport {udp | tcp}

no transport {udp | tcp}

Syntax Description

udp	Configures the SIP user agent to receive SIP messages on UDP port 5060.
tcp	Configures the SIP user agent to receive SIP messages on TCP port 5060.

Defaults

By default, both UDP and TCP transport protocols are enabled.

Command Modes

SIP user agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XA	Support was added for the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was introduced on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

This command controls whether messages reach the SIP service provider interface (SPI). To reset this command to the default value, use the **default** command.

Examples

The following example shows how to block reception of SIP signaling messages on a TCP port:

```
Router(config)# sip-ua
Router(config-sip-ua)# no transport tcp
```

Related Commands

Command	Description
sip-ua	Enables the sip-ua configuration commands to configure the user agent.
sip-server	Configures a network address for the SIP server interface.

Glossary

AAA—Authentication, Authorization, and Accounting. AAA is a suite of network security services that provides the primary framework through which access control can be set up on your Cisco router or access server.

ANI—Automatic number identification.

call—In SIP, a call consists of all participants in a conference invited by a common source. A SIP call is identified by a globally unique call ID. A point-to-point IP telephony conversation maps into a single SIP call. For a multicast session, each participant in the session constitutes a unique call. Each call involves a UAC and a UAS application.

CAS—Channel associated signaling.

CCAPI—Call control applications programming interface.

CLI—Command line interface.

CO—Central office.

CPE—Customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at the customer sites, and connected to the telephone company network.

CSM—Call switching module.

dial peer—An addressable call endpoint. In Voice over IP (VoIP), there are two types of dial peers: POTS and VoIP.

DNS—Domain name system used to address translation to convert H.323 IDs, URLs, or e-mail IDs to IP addresses. DNS is also used to assist in the locating remote gatekeepers and to reverse-map raw IP addresses to host names of administrative domains.

DNIS—Dialed number identification service (the called number).

DSP—Digital signal processor.

DTMF—Dual tone multi-frequency.

E.164—The international public telecommunications numbering plan. A standard set by ITU-T which addresses telephone numbers.

E&M—Ear and mouth RBS signaling.

endpoint—A H.323 terminal or gateway. An endpoint can call and be called. It generates and/or terminates the information stream.

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

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

H.323 RAS—Registration, admission, and status. The RAS signaling function performs registration, admissions, bandwidth changes, status and disengage procedures between the VoIP gateway and the gatekeeper.

IPSEC—An IETF standard that is used to provide security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (“peers”), such as Cisco routers.

IVR—Integrated voice response. When someone dials in, IVR responds with a prompt to get a personal identification number (PIN), and so on.

LEC—Local exchange carrier.

Location Server—A SIP redirect or proxy server uses a location service to get information about a caller's location(s). Location services are offered by location servers.

MF—Multi-frequency tones are made of six frequencies that provide 15 two frequency combinations for indication digits 0-9 and KP/ST signals.

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

multipoint-unicast—A process of transferring PDUs (Protocol Data Units) where an endpoint sends more than one copy of a media stream to different endpoints. This can be necessary in networks which do not support multicast.

node—A H.323 entity that uses RAS to communicate with the gatekeeper, for example, an endpoint such as a terminal, proxy, or gateway.

PDU—Protocol data units used by bridges to transfer connectivity information.

POTS—Plain old telephone service. Basic telephone service supplying standard single line telephones, telephone lines, and access to the PSTN.

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

PSTN—Public switched telephone network. PSTN refers to the local telephone company.

QoS—Quality of Service. Measure of performance for a transmission system that reflects its transmission quality and service availability. QoS refers to the ability of a network to provide better service to selected network traffic over various underlying technologies. QoS is not inherent in a network infrastructure. Rather, you must institute QoS by strategically deploying features that implement it throughout the network.

Redirect Server—A redirect server is a server that accepts a SIP request, maps the address into zero or more new addresses and returns these addresses to the client. It does not initiate its own SIP request nor accept calls.

Registrar—A registrar is a server that accepts REGISTER requests. A registrar is typically co-located with a proxy or redirect server and MAY offer location services.

RAS—Registration, admission, and status protocol. This is the protocol that is used between endpoints and the gatekeeper to perform management functions.

RBS—Robbed bit signaling.

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

SIP—Session Initiation Protocol. This is an application-layer protocol developed by the IETF MMUSIC Working Group to equip platforms to signal the setup of voice and multimedia calls over IP networks. SIP features are compliant with IETF RFC 2543, published in March 1999.

SPI—Service provider interface.

TDM—Time division multiplexing. Technique in which information from multiple channels can be allocated bandwidth on a single wire based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

User Agent—see **UAS and UAC**.

UAC—User Agent Client: A user agent client is a client application that initiates the SIP request.

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

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

