

# debug cch323

To provide debugging output for various components within the H.323 subsystem, use the **debug cch323** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug cch323 {all | error | h225 | h245 | nxe | ras | rawmsg | session }
```

```
no debug cch323
```

## Syntax Description

<b>all</b>	Enables all <b>debug cch323</b> commands.
<b>error</b>	Traces errors encountered in the H.323 subsystem and can be used to help troubleshoot problems with H.323 calls.
<b>h225</b>	Traces the state transition of the H.225 state machine on the basis of the processed event.
<b>h245</b>	Traces the state transition of the H.245 state machine on the basis of the processed events.
<b>nxe</b>	Displays Annex E events that have been transmitted and received.
<b>ras</b>	Traces the state transition of the Registration, Admission, and Status (RAS) state machine on the basis of the processed events.
<b>rawmsg</b>	Troubleshoots raw message buffer problems.
<b>session</b>	Traces general H.323 events and can be used to troubleshoot H.323 problems.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
11.3(6)NA2	The <b>debug cch323</b> command and the following keywords were introduced: <b>h225</b> , <b>h245</b> , and <b>ras</b> .
12.2(2)XA	The <b>nxe</b> keyword was added.
12.2(4)T	The following keywords were introduced: <b>all</b> , <b>error</b> , <b>rawmsg</b> , and <b>session</b> . The <b>nxe</b> keyword was integrated into Cisco IOS Release 12.2(4)T on all Cisco H.323 platforms. This command does not support the Cisco access server platforms in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

**Usage Guidelines****The debug cch323 Command with the all Keyword**

When used with the **debug cch323** command, the **all** keyword provides debug output for various components within the H.323 subsystem.

The **debug cch323** command used with the **all** keyword enables the following **debug cch323** commands:

<b>error</b>	Enables a CCH323 Service Provider Interface (SPI) trace.
<b>h225</b>	Enables an H225 state machine debugging trace.
<b>h245</b>	Enables an H245 state machine debugging trace.
<b>nx</b>	Enables an Annex E debugging trace.
<b>ras</b>	Enables a RAS state machine debugging trace.
<b>rawmsg</b>	Enables a CCH323 RAWMSG debugging trace.
<b>session</b>	Enables a Session debugging trace.

**Caution**

Using the **debug cch323 all** command could slow your system and flood the TTY if there is significant call traffic.

**The debug cch323 Command with the error Keyword**

When used with the **debug cch323** command, the **error** keyword allows you to trace errors encountered in the H.323 subsystem.

**Note**

There is little or no output from this command when there is a stable H.323 network.

**The debug cch323 Command with the h225 Keyword**

When used with the **debug cch323** command, the **h225** keyword allows you to trace the state transition of the H.225 state machine on the basis of the processed event.

The definitions of the different states of the H.225 state machine follow:

- **H225\_IDLE**—This is the initial state of the H.225 state machine. The H.225 state machine is in this state before issuing a call setup request (for the outbound IP call case) or when ready to receive an incoming IP call.
- **H225\_SETUP**—This is the call setup state. The state machine changes to this state after sending out a call setup request or after receiving an incoming call indication.
- **H225\_ALERT**—This is the call alerting state. The state machine changes to this state after sending the alerting message or after receiving an alerting message from the peer.
- **H225\_CALLPROC**—This is the call proceeding state.
- **H225\_ACTIVE**—This is the call connected state. In this state, the call is active. The state machine changes to this state after sending the connect message to the peer or after receiving the connect message from the peer.
- **H225\_WAIT\_FOR\_ARQ**—This is the state in which the H.225 state machine is waiting for the completion of the Admission Request (ARQ) process from the RAS state machine.

- H225\_WAIT\_FOR\_DRQ—This is the state in which the H.225 state machine is waiting for the completion of the Disengage Request (DRQ) process from the RAS state machine.
- H225\_WAIT\_FOR\_H245—This is the state in which the H.225 state machine is waiting for the success or failure from the H.245 state machine.

The definitions of the different events of the H.225 state machine follow:

- H225\_EVENT\_NONE—There is no event.
- H225\_EVENT\_ALERT—This event instructs the H.225 state machine to send an alert message to the peer.
- H225\_EVENT\_ALERT\_IND—This event indicates to the H.225 state machine that an alert message arrived from the peer.
- H225\_EVENT\_CALLPROC—This event instructs the H.225 state machine to send a call proceeding message to the peer.
- H225\_EVENT\_CALLPROC\_IND—This event indicates to the H.225 state machine that a call proceeding message has been received from the peer.
- H225\_EVENT\_REJECT—This event instructs the H.225 state machine to reject the call setup request from the peer.
- H225\_EVENT\_REJECT\_IND—This event indicates to the H.225 state machine that a call setup request to the peer has been rejected.
- H225\_EVENT\_RELEASE—This event instructs the H.225 state machine to send a release complete message to the peer.
- H225\_EVENT\_RELEASE\_IND—This event indicates to the H.225 state machine that a release complete message has been received from the peer.
- H225\_EVENT\_SETUP—This event instructs the H.225 state machine to send a setup message to the peer.
- H225\_EVENT\_SETUP\_IND—This event indicates to the H.225 state machine that a setup message has been received from the peer.
- H225\_EVENT\_SETUP\_CFM—This event instructs the H.225 state machine to send a connect message to the peer.
- H225\_EVENT\_SETUP\_CFM\_IND—This event indicates to the H.225 state machine that a connect message arrived from the peer.
- H225\_EVENT\_RAS\_SUCCESS—This event indicates to the H.225 state machine that the pending RAS operation succeeded.
- H225\_EVENT\_RAS\_FAILED—This event indicates to the H.225 state machine that the pending RAS operation failed.
- H225\_EVENT\_H245\_SUCCESS—This event indicates to the H.225 state machine that the pending H.245 operation succeeded.
- H225\_EVENT\_H245\_FAILED—This event indicates to the H.225 state machine that the pending H.245 operation failed.

### The debug cch323 Command with the h245 Keyword

When used with the **debug cch323** command, the **h245** keyword allows you to trace the state transition of the H.245 state machine on the basis of the processed event.

The H.245 state machines include the following three state machines:

- Master slave determination (MSD) state machine
- Capability exchange (CAP) state machine
- Open logical channel (OLC) state machine

The state definitions follow:

- H245\_MS\_NONE—This is the initial state of the MSD state machine.
- H245\_MS\_WAIT—In this state, an MSD message is sent, and the device is waiting for the reply.
- H245\_MS\_DONE—The result is in.
- H245\_CAP\_NONE—This is the initial state of the CAP state machine.
- H245\_CAP\_WAIT—In this state, a CAP message is sent, and the device is waiting for the reply.
- H245\_CAP\_DONE—The result is in.
- H245\_OLC\_NONE—This is the initial state of the OLC state machine.
- H245\_OLC\_WAIT—In this state, an OLC message is sent, and the device is waiting for the reply.
- H245\_OLC\_DONE—The result is in.

The event definitions follow:

- H245\_EVENT\_MSD—Send MSD message.
- H245\_EVENT\_MS\_CFM—Send MSD acknowledge message.
- H245\_EVENT\_MS\_REJ—Send MSD reject message.
- H245\_EVENT\_MS\_IND—Received MSD message.
- H245\_EVENT\_CAP—Send CAP message.
- H245\_EVENT\_CAP\_CFM—Send CAP acknowledge message.
- H245\_EVENT\_CAP\_REJ—Send CAP reject message.
- H245\_EVENT\_CAP\_IND—Received CAP message.
- H245\_EVENT\_OLC—Send OLC message.
- H245\_EVENT\_OLC\_CFM—Send OLC acknowledge message.
- H245\_EVENT\_OLC\_REJ—Send OLC reject message.
- H245\_EVENT\_OLC\_IND—Received OLC message.

### The debug cch323 Command with the nxe Keyword

When used with the **debug cch323** command, the **nxe** keyword allows you to display the Annex E events that have been transmitted and received.

### The debug cch323 Command with the ras Keyword

When used with the **debug cch323** command, the **ras** keyword allows you to trace the state transition of the RAS state machine based on the processed events.

RAS operates in two state machines. One global state machine controls the overall RAS operation of the gateway. The other state machine is a per-call state machine that controls the active calls.

The definitions of the different states of the RAS state machine follow:

- CCH323\_RAS\_STATE\_NONE—This is the initial state of the RAS state machine.
- CCH323\_RAS\_STATE\_GRQ—The state machine is in the Gatekeeper Request (GRQ) state. In this state, the gateway is discovering a gatekeeper.
- CCH323\_RAS\_STATE\_RRQ—The state machine is in the Registration Request (RRQ) state. In this state, the gateway is registering with a gatekeeper.
- CCH323\_RAS\_STATE\_IDLE—The global state machine is in the idle state.
- CCH323\_RAS\_STATE\_URQ—The state machine is in the Unregistration Request (URQ) state. In this state, the gateway is in the process of unregistering with a gatekeeper.
- CCH323\_RAS\_STATE\_ARQ—The per-call state machine is in the process of admitting a new call.
- CCH323\_RAS\_STATE\_ACTIVE—The per-call state machine is in the call active state.
- CCH323\_RAS\_STATE\_DRQ—The per-call state machine is in the process of disengaging an active call.

The definitions of the different events of the RAS state machine follow:

- CCH323\_RAS\_EVENT\_NONE—Nothing.
- CCH323\_RAS\_EVENT\_GWUP—Gateway is coming up.
- CCH323\_RAS\_EVENT\_GWDWN—Gateway is going down.
- CCH323\_RAS\_EVENT\_NEWCALL—New call.
- CCH323\_RAS\_EVENT\_CALLDISC—Call disconnect.
- CCH323\_RAS\_EVENT\_GCF—Received Gatekeeper Confirmation (GCF).
- CCH323\_RAS\_EVENT\_GRJ—Received Gatekeeper Rejection (GRJ).
- CCH323\_RAS\_EVENT\_ACF—Received Admission Confirmation (ACF).
- CCH323\_RAS\_EVENT\_ARJ—Received Admission Reject (ARJ).
- CCH323\_RAS\_EVENT\_SEND\_RRQ—Send Registration Request (RRQ).
- CCH323\_RAS\_EVENT\_RCF—Received Registration Confirmation (RCF).
- CCH323\_RAS\_EVENT\_RRJ—Received Registration Rejection (RRJ).
- CCH323\_RAS\_EVENT\_SEND\_URQ—Send Unregistration Request (URQ).
- CCH323\_RAS\_EVENT\_URQ—Received URQ.
- CCH323\_RAS\_EVENT\_UCF—Received Unregister Confirmation (UCF).
- CCH323\_RAS\_EVENT\_SEND\_UCF—Send UCF.
- CCH323\_RAS\_EVENT\_URJ—Received Unregister Reject (URJ).
- CCH323\_RAS\_EVENT\_BCF—Received Bandwidth Confirm (BCF).
- CCH323\_RAS\_EVENT\_BRJ—Received Bandwidth Rejection (BRJ).
- CCH323\_RAS\_EVENT\_DRQ—Received Disengage Request (DRQ).

- CCH323\_RAS\_EVENT\_DCF—Received Disengage Confirm (DCF).
- CCH323\_RAS\_EVENT\_SEND\_DCF—Send DCF.
- CCH323\_RAS\_EVENT\_DRJ—Received Disengage Reject (DRJ).
- CCH323\_RAS\_EVENT\_IRQ—Received Interrupt Request (IRQ).
- CCH323\_RAS\_EVENT\_IRR—Send Information Request (IRR).
- CCH323\_RAS\_EVENT\_TIMEOUT—Message timeout.

#### The debug cch323 Command with the rawmsg Keyword

When used with the **debug cch323** command, the **rawmsg** keyword allows you to troubleshoot raw message buffer problems.



#### Caution

Using the **debug cch323** command with the **rawmsg** keyword could slow your system and flood the TTY if there is significant call traffic.

#### The debug cch323 Command with the session Keyword

Used with the **debug cch323** command, the **session** keyword allows you to trace general H.323 events.



#### Caution

Using the **debug cch323 session** command could slow your system and flood the TTY if there is significant call traffic.

## Examples

#### The debug cch323 Command with the all Keyword Example

The **debug cch323 all** command and keyword combination provides output for the following keywords: **error**, **h225**, **h245**, **nx**, **ras**, **rawmsg**, and **session**. Examples of output for each keyword follow.

#### The debug cch323 Command with the error Keyword Example

The following is sample output from a typical **debug cch323 error** request on a Cisco 3640 router:

```
Router# debug cch323 error

cch323_h225_receiver:received msg of unknown type 5
```

#### The debug cch323 Command with the h225 Keyword Example

The following is sample output from a typical **debug cch323 h225** request on a Cisco 3640 router:

```
Router# debug cch323 h225

20:59:17:Set new event H225_EVENT_SETUP
20:59:17:H225 FSM:received event H225_EVENT_SETUP while at state H225_IDLE
20:59:17:Changing from H225_IDLE state to H225_SETUP state
20:59:17:cch323_h225_receiver:received msg of type SETUPCFM_CHOSEN
20:59:17:H225 FSM:received event H225_EVENT_SETUP_CFM_IND while at state
H225_SETUP
20:59:17:Changing from H225_SETUP state to H225_ACTIVE state
20:59:17:Set new event H225_EVENT_H245_SUCCESS
20:59:17:H225 FSM:received event H225_EVENT_H245_SUCCESS while at state
H225_ACTIVE
20:59:20:Set new event H225_EVENT_RELEASE
20:59:20:H225 FSM:received event H225_EVENT_RELEASE while at state
H225_ACTIVE
20:59:20:Changing from H225_ACTIVE state to H225_WAIT_FOR_DRQ state
```

```

20:59:20:Set new event H225_EVENT_RAS_SUCCESS
20:59:20:H225 FSM:received event H225_EVENT_RAS_SUCCESS while at state
H225_WAIT_FOR_DRQ
20:59:20:Changing from H225_WAIT_FOR_DRQ state to H225_IDLE state

```

Table 32 describes the significant fields shown in the display.

**Table 32** *debug cch323 h225 Field Descriptions*

Field	Description
H225_EVENT_SETUP	This event instructs the H.225 state machine to send a setup message to the peer.
H225_IDLE	The initial state of the H.225 state machine. The H.225 state machine is in this state before issuing a call setup request (for the outbound IP call case) or when ready to receive an incoming IP call.
H225_SETUP	The call setup state. The state machine changes to this state after sending out a call setup request or after receiving an incoming call indication.
SETUPCFM_CHOSEN	The H225 connect message that has been received from a remote H323 endpoint.
H225_EVENT_SETUP_CFM_IND	This event indicates to the H.225 state machine that a connect message arrived from the peer.
H225_ACTIVE	The call connected state. In this state, the call is active. The state machine changes to this state after sending the connect message to the peer or after receiving the connect message from the peer.
H225_EVENT_H425_SUCCESS	This event indicates to the H.225 state machine that the pending H.245 operation succeeded.
H225_EVENT_RELEASE	This event instructs the H.225 state machine to send a release complete message to the peer.
H225_WAIT_FOR_DRQ	The state in which the H.225 state machine is waiting for the completion of the DRQ process from the RAS state machine.
H225_EVENT_RAS_SUCCESS	This event indicates to the H.225 state machine that the pending RAS operation succeeded.
H225 FSM	The finite state machine.

#### The debug cch323 Command with the h245 Keyword Example

The following is sample output from a typical **debug cch323 h245** request on a Cisco 3640 router:

```

Router# debug cch323 h245

20:58:23:Changing to new event H245_EVENT_MSD
20:58:23:H245 MS FSM:received event H245_EVENT_MSD while at state
H245_MS_NONE
20:58:23:changing from H245_MS_NONE state to H245_MS_WAIT state
20:58:23:Changing to new event H245_EVENT_CAP
20:58:23:H245 CAP FSM:received event H245_EVENT_CAP while at state
H245_CAP_NONE

```

```

20:58:23:changing from H245_CAP_NONE state to H245_CAP_WAIT state
20:58:23:cch323_h245_receiver:received msg of type
M_H245_MS_DETERMINE_INDICATION
20:58:23:Changing to new event H245_EVENT_MS_IND
20:58:23:H245 MS FSM:received event H245_EVENT_MS_IND while at state
H245_MS_WAIT
20:58:23:cch323_h245_receiver:received msg of type
M_H245_CAP_TRANSFER_INDICATION
20:58:23:Changing to new event H245_EVENT_CAP_IND
20:58:23:H245 CAP FSM:received event H245_EVENT_CAP_IND while at state
H245_CAP_WAIT
20:58:23:cch323_h245_receiver:received msg of type
M_H245_MS_DETERMINE_CONFIRM
20:58:23:Changing to new event H245_EVENT_MS_CFM
20:58:23:H245 MS FSM:received event H245_EVENT_MS_CFM while at state
H245_MS_WAIT
20:58:23:changing from H245_MS_WAIT state to H245_MS_DONE state
0:58:23:cch323_h245_receiver:received msg of type M_H245_CAP_TRANSFER_CONFIRM
20:58:23:Changing to new event H245_EVENT_CAP_CFM
20:58:23:H245 CAP FSM:received event H245_EVENT_CAP_CFM while at state
H245_CAP_WAIT
20:58:23:changing from H245_CAP_WAIT state to H245_CAP_DONE state
20:58:23:Changing to new event H245_EVENT_OLC
20:58:23:H245 OLC FSM:received event H245_EVENT_OLC while at state
H245_OLC_NONE
20:58:23:changing from H245_OLC_NONE state to H245_OLC_WAIT state
20:58:23:cch323_h245_receiver:received msg of type
M_H245_UCHAN_ESTABLISH_INDICATION
20:58:23:Changing to new event H245_EVENT_OLC_IND
20:58:23:H245 OLC FSM:received event H245_EVENT_OLC_IND while at state
H245_OLC_WAIT
20:58:23:cch323_h245_receiver:received msg of type M_H245_UCHAN_ESTAB_ACK
20:58:23:Changing to new event H245_EVENT_OLC_CFM
20:58:23:H245 OLC FSM:received event H245_EVENT_OLC_CFM while at state
H245_OLC_WAIT
20:58:23:changing from H245_OLC_WAIT state to H245_OLC_DONE state

```

Table 33 describes the significant fields shown in the display.

**Table 33** *debug cch323 h245 Field Descriptions*

Field	Description
H245_EVENT_MSD	Send MSD event message to the state machine.
H245 MS FSM	An H225 master slave determination finite state machine.
H245_MS_NONE	The initial state of the MSD state machine.
H245_MS_WAIT	In this state, a MSD message is sent, and the device is waiting for the reply.
H245_EVENT_CAP	Send CAP event message.
H245 CAP FSM	This is the H245 terminal CAP finite state machine.
H245_CAP_NONE	The initial state of the CAP state machine.
H245_CAP_WAIT	In this state, a CAP message is sent, and the device is waiting for the reply.

**Table 33** *debug cch323 h245 Field Descriptions (continued)*

Field	Description
M_H245_MS_DETERMINE_INDICATION	The MSD message that has been received by an H245 terminal from a remote H323 endpoint.
H245_EVENT_MS_IND	Received MSD event message.
M_H245_CAP_TRANSFER_INDICATION	A CAP message that has been received by the H245 terminal from an H323 remote endpoint.
H245_EVENT_CAP_IND	Received CAP event message.
M_H245_MS_DETERMINE_CONFIRM	A confirmation message that the H245 master slave termination message was sent.
H245_EVENT_MS_CFM	Send MSD acknowledge event message.
H245_MS_DONE	The result is in.
M_H245_CAP_TRANSFER_CONFIRM	An indication to the H245 terminal that the CAP message was sent.
H245_EVENT_CAP_CFM	Send CAP acknowledge event message.
H245_CAP_DONE	The result is in.
H245_EVENT_OLC	Send OLC event message.
H245_OLC_NONE	The initial state of the OLC state machine.
H245_OLC_WAIT	In this state, an OLC message is sent, and the device is waiting for the reply.
M_H245_UCHAN_ESTABLISH_INDICATION	The OLC message received by an H245 terminal from a remote H323 endpoint.
H245_EVENT_OLC_IND	Received OLC event message.
M_H245_UCHAN_ESTAB_ACK	The OLC message acknowledgement received by an H245 terminal from a remote H323 endpoint.
H245_EVENT_OLC_CFM	Send OLC acknowledge event message.
H245_OLC_FSM	The OLC finite state machine of the H245 terminal.
H245_EVENT_OLC_CFM	Send OLC acknowledge event message.
H245_OLC_DONE	The result is in.

**The debug cch323 Command with the nxe Keyword Example**

The following is sample output from a **debug cch323 nxe** request:

```
Router# debug cch323 nxe

00:15:54:nxe_handle_usrmsg_to_remote:User Message size is 227
00:15:54:nxe_msg_send_possible:Msg put in the active Q for CRV [3, direction flag 0]
00:15:54:nxe_send_msg:H323chan returns bytes sent=241, the actual len=241, to IPAddr
[0xA4D4A02], Port [2517]
00:15:54:nxe_handle_usrmsg_to_remote:Usr Msg sent for IPAddr [0xA4D4A02], Port [2517], CRV
[3, direction flag 0]
00:15:54:nxe_parse_msg_from_remote:Msg received from IP [0xA4D4A02], Port [2517]
00:15:54:nxe_parse_msg_from_remote:Value of PDU flags = 0x2
00:15:54:nxe_parse_payload:Transport msg type, Payload flag = 0x0
00:15:54:nxe_receive_ack:Ack received for 1 pdu
00:15:54:nxe_receive_ack:Ack received for seqnum=13 from IPAddr [0xA4D4A02], Port [2517]
```

```

00:15:54:nxe_parse_msg_from_remote:Msg received from IP [0xA4D4A02], Port [2517]
00:15:54:nxe_parse_msg_from_remote:Value of PDU flags = 0x3
00:15:54:nxe_parse_payload:Static msg type, Payload flag = 0xA0
00:15:54:nxe_parse_x_static:Rx H225 msg from IPaddr [0xA4D4A02], Port [2517], CRV [3,
direction flag 0]
00:15:54:nxe_make_ackmsg:NXE ACK Msg made to ack seqnum=14
00:15:54:nxe_send_msg:H323chan returns bytes sent=16, the actual len=16, to IPaddr
[0xA4D4A02], Port [2517]
00:15:54:nxe_parse_msg_from_remote:Ack sent for Destination IPaddr [0xA4D4A02], Port
[2517]
00:15:54:nxe_parse_msg_from_remote:Msg received from IP [0xA4D4A02], Port [2517]
00:15:54:nxe_parse_msg_from_remote:Value of PDU flags = 0x3
00:15:54:nxe_parse_payload:Static msg type, Payload flag = 0xA0
00:15:54:nxe_parse_x_static:Rx H225 msg from IPaddr [0xA4D4A02], Port [2517], CRV [3,
direction flag 0]

```

### The debug cch323 Command with the ras Keyword Example

The following is sample output from a typical **debug cch323 ras** request on a Cisco 3640 router:

```

Router# debug cch323 ras

20:58:49:Changing to new event CCH323_RAS_EVENT_SEND_RRQ
cch323_run_ras_sm:received event CCH323_RAS_EVENT_SEND_RRQ while at CCH323_RAS_STATE_IDLE
state
cch323_run_ras_sm:changing to CCH323_RAS_STATE_RRQ state
cch323_ras_receiver:received msg of type RCF_CHOSEN
cch323_run_ras_sm:received event CCH323_RAS_EVENT_RCF while at CCH323_RAS_STATE_RRQ state
cch323_run_ras_sm:changing to CCH323_RAS_STATE_IDLE state
20:58:59:cch323_percall_ras_sm:received event CCH323_RAS_EVENT_NEWCALL while at
CCH323_RAS_STATE_IDLE state
20:58:59:cch323_percall_ras_sm:changing to new state CCH323_RAS_STATE_ARQ
cch323_ras_receiver:received msg of type ACF_CHOSEN
20:58:59:cch323_percall_ras_sm:received event CCH323_RAS_EVENT_ACF while at
CCH323_RAS_STATE_ARQ state
20:58:59:cch323_percall_ras_sm:changing to new state
CCH323_RAS_STATE_ACTIVE
20:59:02:cch323_percall_ras_sm:received event CCH323_RAS_EVENT_CALLDISC while
at CCH323_RAS_STATE_ACTIVE state
20:59:02:cch323_percall_ras_sm:changing to new state CCH323_RAS_STATE_DRQ
cch323_ras_receiver:received msg of type DCF_CHOSEN
20:59:02:cch323_percall_ras_sm:received event CCH323_RAS_EVENT_DCF while at
CCH323_RAS_STATE_DRQ state
20:59:02:cch323_percall_ras_sm:changing to new state CCH323_RAS_STATE_IDLE
20:59:04:cch323_percall_ras_sm:received event CCH323_RAS_EVENT_IRR while at
CCH323_RAS_STATE_ACTIVE state
20:59:04:cch323_percall_ras_sm:changing to new state
CCH323_RAS_STATE_ACTIVE

```

Table 34 describes the significant fields shown in the display.

**Table 34** debug cch323 ras Field Descriptions

Field	Description
CCH323_RAS_EVENT_SEND_RRQ	Send RRQ event message.
CCH323_RAS_STATE_IDLE	The global state machine is in the idle state.
CCH323_RAS_STATE_RRQ	The state machine is in the RRQ state. In this state, the gateway is registering with a gatekeeper.
RCF_CHOSEN	A registration confirm message that has been received from a gatekeeper.



```

00:33:49:cch323_get_peer_info:preffered_codec set to G729IETF with Bytes = 20
00:33:49:cch323_get_peer_info:peer:81FC0D14, peer->voice_peer_tag:12D, ccb:81D12D2C
00:33:49:Call_setup Playout Mode:0,Init 60, Min 40, Max 200
00:33:49:No account/pin number available
00:33:49:cch323_call_setup_normal:for callID 10

00:33:49:timer (0x81D130D4)starts - delay (15000)
00:33:49:cch323_ct_main:SOCK 1 Event 0x1
00:33:49:timer(0x81D130D4) stops
00:33:49:Near-end Pref Codecs = G.729 IETF
00:33:49: generic_open_logical_channel:codec is g729

00:33:49:cch323_generic_open_logical_channel:Filling in qosCapability field to 0

00:33:49:timer (0x81D130D4)starts - delay (15000)
00:33:49:cch323_ct_main:SOCK 1 Event 0x1
00:33:49:cch323_ct_main:SOCK 1 Event 0x1
00:33:49:      [1]townner_data=0x81D13C88, len=105, msgPtr=0x81D07608

00:33:49:cch323_gw_process_read_socket:received msg for H.225

00:33:49:timer(0x81D130D4) stops
00:33:49:timer (0x81D130D4)starts - delay (180000)
00:33:49:Codec:loc(16), rem(16),
Bytes:loc(20), Fwd(20), Rev(20)
00:33:49:cch323_rtp_open_notify:
00:33:50:cch323_ct_main:SOCK 1 Event 0x1
00:33:50:      [1]townner_data=0x81D13C88, len=71, msgPtr=0x81F1F2E0

00:33:50:cch323_gw_process_read_socket:received msg for H.225

00:33:50:cch323_caps_ind:cap_modem_proto:0, cap_modem_codec:0, cap_modem_redundancy:0
payload 100
00:33:50:cch323_caps_ind:Load DSP with Negotiated codec(16) g729r8, Bytes=20
00:33:50:cch323_caps_ind:set DSP for dtmf-relay = CC_CAP_DTMF_RELAY_INBAND_VOICE

```

The following is sample output from a typical **debug cch323** session request for a call setup on a terminating gateway:

Router# **debug cch323 session**

```

00:23:27:cch323_ct_main:SOCK 0 Event 0x1
00:23:27:cch323_ct_main:SOCK 1 Event 0x1
00:23:27:      [1]townner_data=0x81F9CA9C, len=179, msgPtr=0x81D15C6C

00:23:27:cch323_gw_process_read_socket:received msg for H.225

00:23:27:cch323_h225_receiver CCB not existing already

00:23:27:cch323_get_new_ccb:ccb (0x81F90184) is in use
00:23:27:cch323_h225_receiver Got a new CCB for call id -2115467564

00:23:27:cch323_h225_setup_ind
00:23:27:Not using Voice Class Codec

00:23:27:cch323_set_peer:peer:81FB3228, peer->voice_peer_tag:12C, ccb:81F90184
00:23:27:Near-end Pref Codecs = G.729 IETF
00:23:27:Codec:loc(16), rem(16),
Bytes:loc(20), Fwd(20), Rev(20)

00:23:27:cch323_build_fastStart_cap_response:Retrieved qosCapability of 0

```

00:23:27:cch323\_build\_fastStart\_cap\_response:In Response Filling in qosCapability field to 0

00:23:27:Not using Voice Class Codec

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear h323 gateway</b>	Clears the H.323 gateway counters.
<b>debug h323-annexg</b>	Displays all pertinent AnnexG messages that have been transmitted and received.
<b>debug voip rawmsg</b>	Displays the raw message owner, length, and pointer.
<b>show h323 gateway</b>	Displays statistics for H.323 gateway messages that have been sent and received and displays the reasons for which H.323 calls have been disconnected.

# debug cch323 capacity

To track the call capacity of the gatekeeper, use the **debug cch323 capacity** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug cch323 capacity**

**no debug cch323 capacity**

**Syntax Description** This command has no keywords or arguments.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

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

**Usage Guidelines** Use the **debug cch323 capacity** command to track the maximum and current call capacity values in the Registration, Admission, and Status (RAS) Protocol messages and to debug capacity-related problems while sending RAS messages. This command is entered on the gateway to monitor the call capacity of the gatekeeper.

The command lists the values for current and maximum call capacity provided by the trunk group capacity resource manager if and when the H.323 Service Provider Interface (SPI) requests the information for all or specific groups of circuits.

**Examples** The following is sample output from the **debug cch323 capacity** command:

```
Router# debug cch323 capacity

Call Capacity Information tracing is enabled

5d00h: cch323_process_carrier_update: Registered = 1,Event = 1,Reason = 1
5d00h: cch323_process_carrier_update: CarrierId = CARRIERA_NEWENGLAND
5d00h: cch323_fill_crm_CallCapacities: Reason = 1, GroupID = CARRIERA_NEWENGLAND
5d00h: Capacity Details:                Maximum Channels in Group:    23
      Max. Voice Calls(In) :           23,      Max. Voice Calls(Out):    23
      Active Voice Calls(In):           5,      Active Voice Calls(Out):    7
      Max. Voice Calls(to GK):          23,      Avail. Voice Calls(to GK):  11
```

The gatekeeper displays this output when trunk groups are added, deleted, or modified or when circuits in a trunk group are deactivated or activated (similar to ISDN layer 2 down/up).

```
5d00h: cch323_process_carrier_update: Registered = 1,Event = 1,Reason = 1
5d00h: cch323_process_carrier_update: CarrierId = CARRIERA_NEWENGLAND
```

Table 35 describes the significant fields shown in the display.

**Table 35** debug cch323 capacity Update Field Descriptions

Field	Description
Registered	Gateway registration: <ul style="list-style-type: none"> <li>0=Gateway is not registered to the gatekeeper</li> <li>1=Gateway is registered to the gatekeeper at the time of the change</li> </ul>
Event	Carriers updated: <ul style="list-style-type: none"> <li>0=All carriers updated</li> <li>1=Single carrier updated</li> </ul>
Reason	Reason for the update notification: <ul style="list-style-type: none"> <li>0=CURRENT_CAPACITY_UPDATE</li> <li>1=MAX_CAPACITY_UPDATE</li> <li>2=BOTH_CAPACITY_UPDATE</li> </ul>
CarrierID	ID of the trunk group or carrier to which the change applies.

The gatekeeper displays this output whenever call capacity information is sent to the gatekeeper.

```
5d00h: cch323_fill_crm_CallCapacities: Reason = 1, GroupID = CARRIERA_NEWENGLAND
5d00h: Capacity Details:           Maximum Channels in Group:    23
    Max. Voice Calls(In) :      23,      Max. Voice Calls(Out):    23
    Active Voice Calls(In):     5,      Active Voice Calls(Out):    7
    Max. Voice Calls(to GK):    23,      Avail. Voice Calls(to GK):  11
```

Table 36 describes the significant fields shown in the display.

**Table 36** debug cch323 capacity Call Capacity Field Descriptions

Field	Description
GroupID	The circuit's carrier identification (ID) or trunk group label.
Maximum Channels in Group	Maximum number of physical (or configured) circuits.
Max. Voice Calls(In)	Maximum number of allowed incoming voice and data calls.
Max. Voice Calls(Out)	Maximum number of allowed outgoing voice and data calls.
Active Voice Calls(In)	Current number of active incoming voice and data calls.
Active Voice Calls(Out)	Current number of active outgoing voice and data calls.
Max. Voice Calls(to GK)	Maximum call capacity value to be sent to the gatekeeper in the RAS message.
Avail. Voice Calls(to GK)	Available call capacity value to be sent to the gatekeeper in the RAS message.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>endpoint circuit-id h323id</b>	Associates a carrier with a non-Cisco endpoint.

# debug cch323 h225

To provide the trace of the state transition of the H.225 state machine based on the processed events, use the **debug cch323 h225** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug cch323 h225
```

```
no debug cch323 h225
```

**Syntax Description** This command has no keywords or arguments.

**Defaults** Disabled

**Command Modes** Privileged EXEC

## Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

## Usage Guidelines

### State Descriptions

The state definitions of the different states of the H.225 state machine are as follows:

- **H225\_IDLE**—This is the initial state of the H.225 state machine. The H.225 state machine is in this state before issuing a call setup request (for the outbound IP call case) or ready to receive an incoming IP call.
- **H225\_SETUP**—This is the call setup state. The state machine transitions to this state after sending out a call setup request, or after the reception of an incoming call indication.
- **H225\_ALERT**—This is the call alerting state. The state machine transitions to this state after sending the *alerting* message or after the reception of an *alerting* message from the peer.
- **H225\_CALLPROC**—This is the *call proceeding state*.
- **H225\_ACTIVE**—This is the Call connected state. In this state, the call is active. The state machine transitions to this state after sending the *connect* message to the peer or after the reception of the *connect* message from the peer.
- **H225\_WAIT\_FOR\_ARQ**—This is the state where the H.225 state machine is waiting for the completion of the ARQ process from the Registration, Admission, and Status Protocol (RAS) state machine.
- **H225\_WAIT\_FOR\_DRQ**—This is the state where the H.225 state machine is waiting for the completion of the DRQ process from the RAS state machine.
- **H225\_WAIT\_FOR\_H245**—This is the state where the H.225 state machine is waiting for the success or failure from the H.245 state machine.

### Events Description

The event definitions of the different events of the H.225 state machine are as follows:

- H225\_EVENT\_NONE— No event.
- H225\_EVENT\_ALERT—This event indicates the H.225 state machine to send an *alerting* message to the peer.
- H225\_EVENT\_ALERT\_IND—This event indicates the H.225 state machine that an *alerting* message is received from the peer.
- H225\_EVENT\_CALLPROC—This event indicates the H.225 state machine to send a *call proceeding* message to the peer.
- H225\_EVENT\_CALLPROC\_IND—This event indicates the H.225 state machine that a *call proceeding* message is received from the peer.
- H225\_EVENT\_REJECT—This event indicates the H.225 state machine to reject the *call setup* request from the peer.
- H225\_EVENT\_REJECT\_IND—This event indicates the H.225 state machine that a *call setup* request to the peer is rejected.
- H225\_EVENT\_RELEASE—This event indicates the H.225 state machine to send a *release complete* message to the peer.
- H225\_EVENT\_RELEASE\_IND—This event indicates the H.225 state machine that a *release complete* message is received from the peer.
- H225\_EVENT\_SETUP—This event indicates the H.225 state machine to send a *setup* message to the peer.
- H225\_EVENT\_SETUP\_IND—This event indicates the H.225 state machine that a *setup* message is received from the peer.
- H225\_EVENT\_SETUP\_CFM—This event indicates the H.225 state machine to send a *connect* message to the peer.
- H225\_EVENT\_SETUP\_CFM\_IND—This event indicates the H.225 state machine that a *connect* message from the peer.
- H225\_EVENT\_RAS\_SUCCESS—This event indicates the H.225 state machine that the pending RAS operation is successful.
- H225\_EVENT\_RAS\_FAILED—This event indicates the H.225 state machine that the pending RAS operation failed.
- H225\_EVENT\_H245\_SUCCESS—This event indicates the H.225 state machine that the pending H.245 operation is successful.
- H225\_EVENT\_H245\_FAILED—This event indicates the H.225 state machine that the pending H.245 operation failed.

### Examples

The following is sample output from the **debug cch323 h225** command:

```
Router# debug cch323 h225

20:59:17:Set new event H225_EVENT_SETUP
20:59:17:H225 FSM:received event H225_EVENT_SETUP while at state H225_IDLE
20:59:17:Changing from H225_IDLE state to H225_SETUP state
20:59:17:cch323_h225_receiver:received msg of type SETUPCFM_CHOSEN
20:59:17:H225 FSM:received event H225_EVENT_SETUP_CFM_IND while at state
H225_SETUP
```

```
20:59:17:Changing from H225_SETUP state to H225_ACTIVE state
20:59:17:Set new event H225_EVENT_H245_SUCCESS
20:59:17:H225 FSM:received event H225_EVENT_H245_SUCCESS while at state
H225_ACTIVE
20:59:20:Set new event H225_EVENT_RELEASE
20:59:20:H225 FSM:received event H225_EVENT_RELEASE while at state
H225_ACTIVE
20:59:20:Changing from H225_ACTIVE state to H225_WAIT_FOR_DRQ state
20:59:20:Set new event H225_EVENT_RAS_SUCCESS
20:59:20:H225 FSM:received event H225_EVENT_RAS_SUCCESS while at state
H225_WAIT_FOR_DRQ
20:59:20:Changing from H225_WAIT_FOR_DRQ state to H225_IDLE state
```

# debug cch323 h245

To provide the trace of the state transition of the H.245 state machine based on the processed events, use the **debug cch323 h245** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug cch323 h245
```

```
no debug cch323 h245
```

**Syntax Description** This command has no keywords or arguments.

**Defaults** Disabled

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.3(6)NA2	This command was introduced.
	12.2(2)XB1	This command was implemented on the Cisco AS5850.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

**Usage Guidelines** The H.245 state machines include the following three state machines:

- Master SlaveDetermination (MSD) state machine
- Capability Exchange (CAP) state machine
- Open Logical Channel (OLC) state machine

### State Definitions

The definitions are as follows:

- H245\_MS\_NONE— This is the initial state of the master slave determination state machine.
- H245\_MS\_WAIT—In this state, a Master Slave Determination message is sent, waiting for the reply.
- H245\_MS\_DONE— The result is in.
- H245\_CAP\_NONE—This is the initial state of the capabilities exchange state machine.
- H245\_CAP\_WAIT—In this state, a *cap exchange message* is sent, waiting for reply.
- H245\_CAP\_DONE—The result is in.
- H245\_OLC\_NONE—This is the initial state of the open logical channel state machine.
- H245\_OLC\_WAIT: OLC message sent, waiting for reply.
- H245\_OLC\_DONE: OLC done.

**Event definitions**

- H245\_EVENT\_MSD—Send MSD message
- H245\_EVENT\_MS\_CFM—Send MSD acknowledge message
- H245\_EVENT\_MS\_REJ—Send MSD reject message
- H245\_EVENT\_MS\_IND— Received MSD message
- H245\_EVENT\_CAP—Send CAP message
- H245\_EVENT\_CAP\_CFM—Send CAP acknowledge message
- H245\_EVENT\_CAP\_REJ—Send CAP reject
- H245\_EVENT\_CAP\_IND—Received CAP message
- H245\_EVENT\_OLC—Send OLC message
- H245\_EVENT\_OLC\_CFM—Send OLC acknowledge message
- H245\_EVENT\_OLC\_REJ—Send OLC reject message
- H245\_EVENT\_OLC\_IND—Received OLC message

**Examples**

The following is sample output from the **debug cch323 h245** command:

```
Router# debug cch323 h245

20:58:23:Changing to new event H245_EVENT_MSD
20:58:23:H245 MS FSM:received event H245_EVENT_MSD while at state
H245_MS_NONE
20:58:23:changing from H245_MS_NONE state to H245_MS_WAIT state
20:58:23:Changing to new event H245_EVENT_CAP
20:58:23:H245 CAP FSM:received event H245_EVENT_CAP while at state
H245_CAP_NONE
20:58:23:changing from H245_CAP_NONE state to H245_CAP_WAIT state
20:58:23:cch323_h245_receiver:received msg of type
M_H245_MS_DETERMINE_INDICATION
20:58:23:Changing to new event H245_EVENT_MS_IND
20:58:23:H245 MS FSM:received event H245_EVENT_MS_IND while at state
H245_MS_WAIT
20:58:23:cch323_h245_receiver:received msg of type
M_H245_CAP_TRANSFER_INDICATION
20:58:23:Changing to new event H245_EVENT_CAP_IND
20:58:23:H245 CAP FSM:received event H245_EVENT_CAP_IND while at state
H245_CAP_WAIT
20:58:23:cch323_h245_receiver:received msg of type
M_H245_MS_DETERMINE_CONFIRM
20:58:23:Changing to new event H245_EVENT_MS_CFM
20:58:23:H245 MS FSM:received event H245_EVENT_MS_CFM while at state
H245_MS_WAIT
20:58:23:changing from H245_MS_WAIT state to H245_MS_DONE state
0:58:23:cch323_h245_receiver:received msg of type M_H245_CAP_TRANSFER_CONFIRM
20:58:23:Changing to new event H245_EVENT_CAP_CFM
20:58:23:H245 CAP FSM:received event H245_EVENT_CAP_CFM while at state
H245_CAP_WAIT
20:58:23:changing from H245_CAP_WAIT state to H245_CAP_DONE state
20:58:23:Changing to new event H245_EVENT_OLC
20:58:23:H245 OLC FSM:received event H245_EVENT_OLC while at state
H245_OLC_NONE
20:58:23:changing from H245_OLC_NONE state to H245_OLC_WAIT state
20:58:23:cch323_h245_receiver:received msg of type
M_H245_UCHAN_ESTABLISH_INDICATION
20:58:23:Changing to new event H245_EVENT_OLC_IND
```

```
20:58:23:H245 OLC FSM:received event H245_EVENT_OLC_IND while at state
H245_OLC_WAIT
20:58:23:cch323_h245_receiver:received msg of type M_H245_UCHAN_ESTAB_ACK
20:58:23:Changing to new event H245_EVENT_OLC_CFM
20:58:23:H245 OLC FSM:received event H245_EVENT_OLC_CFM while at state
H245_OLC_WAIT
20:58:23:changing from H245_OLC_WAIT state to H245_OLC_DONE state
```

# debug cch323 preauth

To enable diagnostic reporting of authentication, authorization, and accounting (AAA) call preauthentication for H.323 calls, use the **debug cch323 preauth** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug cch323 preauth**

**no debug cch323 preauth**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

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

**Examples** The following is debugging output for a single H.323 call:

```
Router# debug cch323 preauth

CCH323 preauth tracing is enabled
cch323_is_preauth_reqd is TRUE
Jan 23 18:39:56.393: In cch323_send_preauth_req for preauth_id = -1
Jan 23 18:39:56.393: Entering rpms_proc_print_preauth_req

Jan 23 18:39:56.393: Request = 0
Jan 23 18:39:56.393: Preauth id = 86514
Jan 23 18:39:56.393: EndPt Type = 1
Jan 23 18:39:56.393: EndPt = 192.168.81.102
Jan 23 18:39:56.393: Resource Service = 1
Jan 23 18:39:56.393: Call_origin = answer
Jan 23 18:39:56.393: Call_type = voip
Jan 23 18:39:56.393: Calling_num = 2230001
Jan 23 18:39:56.393: Called_num = 1#1130001
Jan 23 18:39:56.393: Protocol = 0
Jan 23 18:39:56.393: cch323_insert_preauth_tree:Created node with preauth_id = 86514 ,ccb
6852D5BC , node 651F87FC
Jan 23 18:39:56.393:rpms_proc_create_node:Created node with preauth_id = 86514
Jan 23 18:39:56.393:rpms_proc_send_aaa_req:uid got is 466725
Jan 23 18:39:56.397:rpms_proc_preauth_response:Context is for preauth_id 86514, aaa_uid
466725
Jan 23 18:39:56.397: Entering Function cch323_rpms_proc_callback_func
```

```
Jan 23 18:39:56.397:cch323_rpms_proc_callback_func:PREAUTH_SUCCESS for preauth id 86514
aaa_uid 466725 auth_serv 1688218168
```

```
Jan 23 18:39:56.397:rpms_proc_preauth_response:Deleting Tree node for preauth id 86514 uid
466725
```

```
Jan 23 18:39:56.397:cch323_get_ccb_and_delete_from_preauth_tree:Preauth_id=86514
cch323_get_ccb_and_delete_from_preauth_tree:651F87FC node and 6852D5BC ccb
```

Table 37 describes the significant fields shown in the display.

**Table 37** *debug cch323 preauth Field Descriptions*

Field	Description
Request	Request Type—0 for preauthentication, 1 for disconnect.
Preauth id	Identifier for the preauthentication request.
EndPt Type	Call Origin End Point Type—1 for IP address, 2 for IZCT value.
EndPt	Call Origin End Point Value—An IP address or IZCT value.
Resource Service	Resource Service Type—1 for Reservation, 2 for Query.
Call_origin	Answer.
Call_type	Voice over IP (VoIP).
Calling_num	Calling Party Number (CLID).
Called_num	Called Party Number (DNIS).
Protocol	0 for H.323, 1 for SIP.
function reports	Various identifiers and status reports for executed functions.

# debug cch323 ras

To provide the trace of the state transition of the Registration, Admission, and Status (RAS) Protocol state machine based on the processed events, use the **debug cch323 ras** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug cch323 ras**

**no debug cch323 ras**

**Syntax Description** This command has no keywords or arguments.

**Defaults** Disabled

**Command Modes** Privileged EXEC

## Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

## Usage Guidelines

RAS operates in two state machines. One global state machine controls the overall RAS operation of the Gateway. The other state machine is a per call state machine that controls the active calls.

### State definitions

The state definitions of the different states of the RAS state machine follow:

- CCH323\_RAS\_STATE\_NONE—This is the initial state of the RAS state machine.
- CCH323\_RAS\_STATE\_GRQ—The state machine is in the Gatekeeper Request (GRQ) state. In this state, the gateway is in the process of discovering a gatekeeper.
- CCH323\_RAS\_STATE\_RRQ—The state machine is in the Registration Request (RRQ) state. In this state, the gateway is in the process of registering with a gatekeeper.
- CCH323\_RAS\_STATE\_IDLE—The global state machine is in the idle state.
- CCH323\_RAS\_STATE\_URQ—The state machine is in the Unregistration Request (URQ) state. In this state, the gateway is in the process of unregistering with a gatekeeper.
- CCH323\_RAS\_STATE\_ARQ—The per call state machine is in the process of admitting a new call.
- CCH323\_RAS\_STATE\_ACTIVE—The per call state machine is in the call active state.
- CCH323\_RAS\_STATE\_DRQ—The per call state machine is in the process of disengaging an active call.

### Event Definitions

These are the event definitions of the different states of the RAS state machine:

- CCH323\_RAS\_EVENT\_NONE—Nothing.
- CCH323\_RAS\_EVENT\_GWUP—Gateway is coming up.
- CCH323\_RAS\_EVENT\_GWDWN—Gateway is going down.
- CCH323\_RAS\_EVENT\_NEWCALL—New call.
- CCH323\_RAS\_EVENT\_CALLDISC—Call disconnect.
- CCH323\_RAS\_EVENT\_GCF—Received Gatekeeper Confirmation (GCF).
- CCH323\_RAS\_EVENT\_GRJ—Received Gatekeeper Rejection (GRJ).
- CCH323\_RAS\_EVENT\_ACF—Received Admission Confirmation (ACF).
- CCH323\_RAS\_EVENT\_ARJ—Received Admission Rejection (ARJ).
- CCH323\_RAS\_EVENT\_SEND\_RRQ—Send Registration Request (RRQ).
- CCH323\_RAS\_EVENT\_RCF—Received Registration Confirmation (RCF).
- CCH323\_RAS\_EVENT\_RRJ—Received Registration Rejection (RRJ).
- CCH323\_RAS\_EVENT\_SEND\_URQ—Send URQ.
- CCH323\_RAS\_EVENT\_URQ—Received URQ.
- CCH323\_RAS\_EVENT\_UCF—Received Unregister Confirmation (UCF).
- CCH323\_RAS\_EVENT\_SEND\_UCF—Send Unregister Confirmation (UCF).
- CCH323\_RAS\_EVENT\_URJ—Received Unregister Reject (URJ).
- CCH323\_RAS\_EVENT\_BCF—Received Bandwidth Confirm (BCF).
- CCH323\_RAS\_EVENT\_BRJ—Received Bandwidth Rejection (BRJ).
- CCH323\_RAS\_EVENT\_DRQ—Received Disengage Request (DRQ).
- CCH323\_RAS\_EVENT\_DCF—Received Disengage Confirm (DCF).
- CCH323\_RAS\_EVENT\_SEND\_DCF—Send Disengage Confirm (DCF).
- CCH323\_RAS\_EVENT\_DRJ—Received Disengage Reject (DRJ).
- CCH323\_RAS\_EVENT\_IRQ—Received Interrupt Request (IRQ).
- CCH323\_RAS\_EVENT\_IRR—Send Information Request (IRR).
- CCH323\_RAS\_EVENT\_TIMEOUT—Message timeout.

### Examples

The following is sample output from the **debug cch323 preauth** command:

```
Router# debug cch323 preauth

20:58:49:Changing to new event CCH323_RAS_EVENT_SEND_RRQ
cch323_run_ras_sm:received event CCH323_RAS_EVENT_SEND_RRQ while at CCH323_RAS_STATE_IDLE
state
cch323_run_ras_sm:changing to CCH323_RAS_STATE_RRQ state
cch323_ras_receiver:received msg of type RCF_CHOSEN
cch323_run_ras_sm:received event CCH323_RAS_EVENT_RCF while at CCH323_RAS_STATE_RRQ state
cch323_run_ras_sm:changing to CCH323_RAS_STATE_IDLE state
20:58:59:cch323_percall_ras_sm:received event CCH323_RAS_EVENT_NEWCALL while at
CCH323_RAS_STATE_IDLE state
20:58:59:cch323_percall_ras_sm:changing to new state CCH323_RAS_STATE_ARQ
```

```
cch323_ras_receiver:received msg of type ACF_CHOSEN
20:58:59:cch323_percall_ras_sm:received event CCH323_RAS_EVENT_ACF while at
CCH323_RAS_STATE_ARQ state
20:58:59:cch323_percall_ras_sm:changing to new state
CCH323_RAS_STATE_ACTIVE
20:59:02:cch323_percall_ras_sm:received event CCH323_RAS_EVENT_CALLDISC while
at CCH323_RAS_STATE_ACTIVE state
20:59:02:cch323_percall_ras_sm:changing to new state CCH323_RAS_STATE_DRQ
cch323_ras_receiver:received msg of type DCF_CHOSEN
20:59:02:cch323_percall_ras_sm:received event CCH323_RAS_EVENT_DCF while at
CCH323_RAS_STATE_DRQ state
20:59:02:cch323_percall_ras_sm:changing to new state CCH323_RAS_STATE_IDLE
20:59:04:cch323_percall_ras_sm:received event CCH323_RAS_EVENT_IRR while at
CCH323_RAS_STATE_ACTIVE state
20:59:04:cch323_percall_ras_sm:changing to new state
CCH323_RAS_STATE_ACTIVE
```

# debug ccm-manager

To display debugging information about the Cisco CallManager (CCM), use the **debug ccm-manager** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ccm-manager {backhaul {events | errors} | config-download {all | errors | events |
packets | xml} | errors | events | music-on-hold {errors | events | packets} | packets}
```

```
no debug ccm-manager
```

Syntax Description	
<b>backhaul</b>	(Optional) Enables debugging of the CCM backhaul. The keywords are as follows: <ul style="list-style-type: none"> <li><b>events</b>—Displays CCM backhaul events.</li> <li><b>errors</b>—Displays CCM backhaul errors.</li> </ul>
<b>config-download</b>	Enables debugging of the CCM configuration download. The keywords are as follows: <ul style="list-style-type: none"> <li><b>all</b>—Displays all CCM configuration parameters.</li> <li><b>errors</b>—Displays CCM configuration errors.</li> <li><b>events</b>—Displays CCM configuration events.</li> <li><b>packets</b>—Displays CCM configuration packets.</li> <li><b>xml</b>—Displays the CCM configuration eXtensible Markup Language (XML) parser.</li> </ul>
<b>errors</b>	(Optional) Displays errors related to CCM.
<b>events</b>	(Optional) Displays CCM events, such as when the primary CCM server fails and control is switched to the backup CCM server.
<b>music-on-hold</b>	(Optional) Displays music-on-hold (MOH). The keywords are as follows: <ul style="list-style-type: none"> <li><b>errors</b>—Displays MOH errors.</li> <li><b>events</b>—Displays MOH events.</li> <li><b>packets</b>—Displays MOH packets.</li> </ul>
<b>packets</b>	(Optional) Displays CCM packets.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced for Cisco CallManager Version 3.0 and the Cisco Voice Gateway 200 (Cisco VG200).
	12.2(2)XA	This command was implemented on Cisco 2600 series and Cisco 3600 series routers.

Release	Modification
12.2(2)XN	Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series routers, Cisco 3600 series routers, and the Cisco Voice Gateway 200 (Cisco VG200).
12.2(11)T	This command was implemented on the Cisco IAD2420 series.

**Examples**

The following is sample output from the **debug ccm-manager events** command:

```
Router# debug ccm-manager events

*Feb 28 22:56:05.873: cmapp_mgcpapp_go_down: Setting mgc status to NO_RESPONSE
*Feb 28 22:56:05.873: cmapp_host_fsm: New state DOWN for host 0 (172.20.71.38)
*Feb 28 22:56:05.873: cmapp_mgr_process_ev_active_host_failed: Active host 0
(172.20.71.38) failed
*Feb 28 22:56:05.873: cmapp_mgr_check_hostlist: Active host is 0 (172.20.71.38)
*Feb 28 22:56:05.877: cmapp_mgr_switchover: New actv host will be 1 (172.20.71.44)
*Feb 28 22:56:05.877: cmapp_host_fsm: Processing event GO_STANDBY for host 0
(172.20.71.38) in state DOWN
*Feb 28 22:56:05.877: cmapp_open_new_link: Open link for [0]:172.20.71.38
*Feb 28 22:56:05.877: cmbh_open_tcp_link: Opening TCP link with Rem IP 172.20.71.38, Local
IP 172.20.71.19, port 2428
*Feb 28 22:56:05.881: cmapp_open_new_link: Open initiated OK: Host 0 (172.20.71.38),
session_id=8186DEE4
*Feb 28 22:56:05.881: cmapp_start_open_link_tmr: Host 0 (172.20.71.38), tmr 0
*Feb 28 22:56:05.881: cmapp_host_fsm: New state STANDBY_OPENING for host 0 (172.20.71.38)
*Feb 28 22:56:05.881: cmapp_host_fsm: Processing event GO_ACTIVE for host 1 (172.20.71.44)
in state STANDBY_READY
*Feb 28 22:56:05.885: cmapp_mgr_send_rehome: new addr=172.20.71.44,port=2427
*Feb 28 22:56:05.885: cmapp_host_fsm: New state REGISTERING for host 1 (172.20.71.44)
```

Table 38 describes the significant fields shown in the display.

**Table 38 debug ccm-manager Field Description**

Field	Description
<i>nn:nn:nn</i>	Time stamp that indicates when the Cisco CallManager event occurred.
CMAPP: <i>error message</i>	The Cisco CallManager routine in which the error event occurred.

**Related Commands**

Command	Description
<b>show ccm-manager</b>	Displays a list of Cisco CallManager servers, their current status, and their availability.

# debug ccsip all

To enable all Session Initiation Protocol (SIP)-related debugging, use the **debug ccsip all** command in privileged EXEC 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.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History		
12.1(1)T		This command was introduced.
12.1.(3)T		The output of this command was changed.
12.2(2)XA		Support was added for the Cisco AS5350 and Cisco AS5400 universal gateways.
12.2(2)XB1		This command was implemented on the Cisco AS5850 universal gateway.
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		This command was integrated into Cisco IOS Release 12.2(11)T. Support for the Cisco AS5300 universal access server, Cisco AS5350, Cisco AS5400, and Cisco AS5850 universal gateway is not included in this release.

**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** The following example displays debug output from one side of the call:

```
Router# 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 1993 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 1993 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_sentinvite_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)
*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 1993 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 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 1993 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 1993 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 1993 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
*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 1993 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 Playout: 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

```

The following example displays debug output from the other side of the call:

Router# **debug ccsip all**

```

All SIP call tracing enabled
3660-2#
*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 1993 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 1993 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
*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_recdinvite_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 1993 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 1993 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 1993 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 1993 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 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 1993 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**

<b>Command</b>	<b>Description</b>
<a href="#">debug ccsip calls</a>	Shows all SIP SPI call tracing.
<a href="#">debug ccsip error</a>	Shows SIP SPI errors.
<a href="#">debug ccsip events</a>	Shows all SIP SPI events tracing.
<a href="#">debug ccsip info</a>	Shows all SIP SPI message tracing.
<a href="#">debug ccsip states</a>	Shows all SIP SPI state tracing.

# debug ccsip calls

To show all Session Initiation Protocol (SIP) Service Provider Interface (SPI) call tracing, use the **debug ccsip calls** command in privileged EXEC 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.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History		
12.1(1)T		This command was introduced.
12.1(3)T		The output of this command was changed.
12.2(2)XA		Support was added for the Cisco AS5350 and Cisco AS5400 universal gateways.
12.2(2)XB1		This command was introduced on the Cisco AS5850 universal gateway.
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		This command was integrated into Cisco IOS Release 12.2(11)T. Support for the Cisco AS5300 universal access server, Cisco AS5350, Cisco AS5400, and Cisco AS5850 universal gateway is not included in this release.

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

**Examples** The following example displays debug output from one side of the call:

```
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

```

The following example displays debug output from the other side of the call:

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**

<b>Command</b>	<b>Description</b>
<a href="#">debug ccsip all</a>	Enables all SIP-related debugging.
<a href="#">debug ccsip error</a>	Shows SIP SPI errors.
<a href="#">debug ccsip events</a>	Shows all SIP SPI events tracing.
<a href="#">debug ccsip info</a>	Shows all SIP SPI message tracing.
<a href="#">debug ccsip states</a>	Shows all SIP SPI state tracing.

# debug ccsip error

To show Session Initiation Protocol (SIP) Service Provider Interface (SPI) errors, use the **debug ccsip error** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ccsip error**

**no debug ccsip error**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Version	Description
	12.1(1)T	This command was introduced.
	12.2(2)XA	Support was added for the Cisco AS5350 and Cisco AS5400 universal gateways.
	12.2(2)XB1	This command was implemented on the Cisco AS5850 universal gateway.
	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	This command was integrated into Cisco IOS Release 12.2(11)T. Support for the Cisco AS5300 universal access server, Cisco AS5350, Cisco AS5400, and Cisco AS5850 universal gateway is not included in this release.

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

**Examples** The following example displays debug output from one side of the call:

```
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
*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: HandleSIPlxxRinging: 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

```

The following example displays debug output from the other side of the call:

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_recdinvite_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_recdinvite_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 Playout: 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**

<b>Command</b>	<b>Description</b>
<a href="#">debug ccsip all</a>	Enables all SIP-related debugging.
<a href="#">debug ccsip calls</a>	Shows all SIP SPI call tracing.
<a href="#">debug ccsip events</a>	Shows all SIP SPI events tracing.
<a href="#">debug ccsip info</a>	Shows all SIP SPI message tracing.
<a href="#">debug ccsip states</a>	Shows all SIP SPI state tracing.

# debug ccsip events

To enable tracing of events that are specific to service provider interface (SPI), use the **debug ccsip events** command in privileged EXEC 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.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Version	Description
	12.1(1)T	This command was introduced.
	12.2(2)XA	Support was added for the Cisco AS5350 and Cisco AS5400 universal gateways.
	12.2(2)XB1	This command was introduced on the Cisco AS5850 universal gateway.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
	12.2(15)T	Much of the information formerly found in the output of the <b>debug ccsip events</b> command is now reported in the output of the <b>debug ccsip info</b> and <b>debug ccsip media</b> commands. The <b>debug ccsip events</b> command now displays only the debugging information specifically related to SIP events.

**Usage Guidelines** This command previously traced all events posted to Session Limitation Protocol (SIP) SPI from all interfaces and also provided general SIP SPI information. Beginning with Cisco IOS Release 12.2(15)T, the **debug ccsip events** command displays only debugging information specifically related to SIP SPI events. Media stream and SIP SPI information is now reported in the **debug ccsip media** and **debug ccsip info** command output.



**Note**

This command is intended for use by Cisco technicians only.

**Examples** The following is sample output from the **debug ccsip events** command for a Cisco 3660:

```
Router# debug ccsip events

SIP Call events tracing is enabled
Router#
Nov 15 18:20:25.779: Queued event from SIP SPI : SIPSPI_EV_CC_CALL_SETUP
Nov 15 18:20:25.779: Queued event from SIP SPI : SIPSPI_EV_CREATE_CONNECTION
Nov 15 18:20:25.783: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
```

```

Nov 15 18:20:25.815: Queued event from SIP SPI : SIPSPI_EV_CREATE_CONNECTION
Nov 15 18:20:25.819: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
Nov 15 18:20:28.339: Queued event from SIP SPI : SIPSPI_EV_CLOSE_CONNECTION
Nov 15 18:20:28.339: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
Nov 15 18:20:50.844: Queued event from SIP SPI : SIPSPI_EV_CLOSE_CONNECTION
Nov 15 18:20:50.844: Queued event from SIP SPI : SIPSPI_EV_SEND_MESSAGE
Nov 15 18:20:50.848: Queued event from SIP SPI : SIPSPI_EV_CC_CALL_DISCONNECT

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug ccsip all</b>	Enables all SIP-related debugging.
<b>debug ccsip info</b>	Enables tracing of general SIP SPI information.
<b>debug ccsip media</b>	Enables tracing of SIP call media streams.

# debug ccsip info

To enable tracing of general service provider interface (SPI) information, use the **debug ccsip info** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ccsip info**

**no debug ccsip info**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.

**Usage Guidelines** Beginning in Cisco IOS Release 12.2(15)T, the **debug ccsip info** command is a separate option that displays general SIP SPI information for debug purposes. In past releases, this output was part of the **debug ccsip events** command.



**Note** This command is intended for use by Cisco technicians only.

**Examples** The following is sample output from the **debug ccsip info** command for a Cisco 3660:

```
Router# debug ccsip info

SIP Call info tracing is enabled
Router#
Nov 15 18:19:22.670: ****Adding to UAC table
Nov 15 18:19:22.670: adding call id E to table
Nov 15 18:19:22.670: CCSIP-SPI-CONTROL: act_idle_call_setup
Nov 15 18:19:22.670: act_idle_call_setup:Not using Voice Class Codec
Nov 15 18:19:22.670: act_idle_call_setup: preferred_codec set[0] type :g729r8 bytes: 20
Nov 15 18:19:22.670: sipSPICopyPeerDataToCCB: From CLI: Modem NSE payload = 100,
Passthrough = 0,Modem relay = 0, Gw-Xid = 1
SPRT latency 200, SPRT Retries = 12, Dict Size = 1024
String Len = 32, Compress dir = 3
Nov 15 18:19:22.670: ****Deleting from UAC table
Nov 15 18:19:22.670: ****Adding to UAC table
Nov 15 18:19:22.670: sipSPIUsetBillingProfile: sipCallId for billing records =
20A40C3B-D92C11D5-8015E1CC-C91F3F10@12.18.195.49
Nov 15 18:19:22.674: CCSIP-SPI-CONTROL: act_idle_connection_created
Nov 15 18:19:22.674: CCSIP-SPI-CONTROL: act_idle_connection_created: Connid(1) created to
172.18.193.190:5060, local_port 56981
Nov 15 18:19:22.674: CCSIP-SPI-CONTROL: sipSPIOutgoingCallSDP
Nov 15 18:19:22.674: convert_codec_bytes_to_ptime: Values :Codec: g729r8 codecbytes :20,
ptime: 10
Nov 15 18:19:22.674: sip_generate_sdp_xcaps_list: Modem Relay disabled. X-cap not needed
```

```

Nov 15 18:19:22.674: sipSPIAddLocalContact
Nov 15 18:19:22.674: sip_stats_method
Nov 15 18:19:22.690: HandleUdpSocketReads :Msg enqueued for SPI with IPAddr:
172.18.193.190:5060
Nov 15 18:19:22.690: CCSIP-SPI-CONTROL: act_sentininvite_new_message
Nov 15 18:19:22.690: CCSIP-SPI-CONTROL: sipSPICheckResponse
Nov 15 18:19:22.690: sip_stats_status_code
Nov 15 18:19:22.690: Roundtrip delay 16 milliseconds for method INVITE
Nov 15 18:19:22.706: HandleUdpSocketReads :Msg enqueued for SPI with IPAddr:
172.18.193.190:5060
Nov 15 18:19:22.706: CCSIP-SPI-CONTROL: act_recdproc_new_message
Nov 15 18:19:22.706: CCSIP-SPI-CONTROL: sipSPICheckResponse
Nov 15 18:19:22.706: sip_stats_status_code
Nov 15 18:19:22.706: Roundtrip delay 32 milliseconds for method INVITE
Nov 15 18:19:22.706: sipSPIGetSdpBody : Parse incoming session description
Nov 15 18:19:22.706: HandleSIP1xxSessionProgress: Content-Disposition received in 18x
response:session;handling=required
Nov 15 18:19:22.706: sipSPIDoMediaNegotiation: number of m lines is 1
Nov 15 18:19:22.706: sipSPIDoAudioNegotiation: Codec (g729r8) Negotiation Successful on
Static Payload
Nov 15 18:19:22.706: sipSPIDoPtimeNegotiation: One ptime attribute found - value:10
Nov 15 18:19:22.706: convert_ptime_to_codec_bytes: Values :Codec: g729r8 ptime :10,
codecbytes: 20
Nov 15 18:19:22.710: convert_codec_bytes_to_ptime: Values :Codec: g729r8 codecbytes :20,
ptime: 10
Nov 15 18:19:22.710: sipSPIDoDTMFRelayNegotiation: m-line index 1
Nov 15 18:19:22.710: sipSPIDoDTMFRelayNegotiation: Requested DTMF-RELAY option(s) not
found in Preferred DTMF-RELAY option list!
Nov 15 18:19:22.710: sip_sdp_get_modem_relay_cap_params:
Nov 15 18:19:22.710: sip_sdp_get_modem_relay_cap_params: NSE payload from X-cap = 0
Nov 15 18:19:22.710: sip_do_nse_negotiation: NSE Payload 100 found in SDP
Nov 15 18:19:22.710: sip_do_nse_negotiation: Remote NSE payload = local one = 100, Use it
Nov 15 18:19:22.710: sip_select_modem_relay_params: X-tmr not present in SDP. Disable
modem relay
Nov 15 18:19:22.710: sipSPIDoQoSNegotiation - SDP body with media description
Nov 15 18:19:22.710: ccsip_process_response_contact_record_route
Nov 15 18:19:22.710: CCSIP-SPI-CONTROL: ccsip_bridge: confID = 4, srcCallID = 14,
dstCallID = 13
Nov 15 18:19:22.710: sipSPIUpdateCcCallIds: old src/dest ccCallids: -1/-1, new src/dest
ccCallids: 14/13
Nov 15 18:19:22.710: sipSPIUpdateCcCallIds: old streamcallid=-1, new streamcallid=14
Nov 15 18:19:22.710: CCSIP-SPI-CONTROL: ccsip_caps_ind
Nov 15 18:19:22.710: ccsip_get_rtcp_session_parameters: CURRENT VALUES: stream_callid=14,
current_seq_num=0x1B1B
Nov 15 18:19:22.710: ccsip_get_rtcp_session_parameters: NEW VALUES: stream_callid=14,
current_seq_num=0x180C
Nov 15 18:19:22.710: ccsip_caps_ind: Load DSP with negotiated codec : g729r8, Bytes=20
Nov 15 18:19:22.710: ccsip_caps_ind: set forking flag to 0x0
Nov 15 18:19:22.710: sipSPISetDTMFRelayMode: set DSP for dtmf-relay =
CC_CAP_DTMF_RELAY_INBAND_VOICE_AND_OOB
Nov 15 18:19:22.710: sip_set_modem_caps: Negotiation already Done. Set negotiated Modem
caps
Nov 15 18:19:22.710: sip_set_modem_caps: Modem Relay & Passthru both disabled
Nov 15 18:19:22.710: sip_set_modem_caps: nse payload = 100, ptru mode = 0, ptru-codec=0,
redundancy=0, xid=0, relay=0, sprt-retry=12, latecncy=200, compres-dir=3, dict=1024,
strnlen=32
Nov 15 18:19:22.710: ccsip_caps_ind: Load DSP with codec : g729r8, Bytes=20
Nov 15 18:19:22.710: CCSIP-SPI-CONTROL: ccsip_caps_ack
Nov 15 18:19:22.710: ccsip_caps_ack: set forking flag to 0x60FD1EAC
Nov 15 18:19:22.710: CCSIP-SPI-CONTROL: act_recdproc_connection_created
Nov 15 18:19:22.710: CCSIP-SPI-CONTROL: sipSPICheckSocketConnection: Connid(2) created to
172.18.193.190:5060, local_port 51663
Nov 15 18:19:22.714: sip_stats_method

```

```

Nov 15 18:19:22.722: HandleUdpSocketReads :Msg enqueued for SPI with IPAddr:
172.18.193.190:5060
Nov 15 18:19:22.722: CCSIP-SPI-CONTROL: act_recdproc_new_message
Nov 15 18:19:22.722: CCSIP-SPI-CONTROL: sipSPICheckResponse
Nov 15 18:19:22.722: sip_stats_status_code
Nov 15 18:19:22.722: Roundtrip delay 48 milliseconds for method PRACK
Nov 15 18:19:24.706: HandleUdpSocketReads :Msg enqueued for SPI with IPAddr:
172.18.193.190:5060
Nov 15 18:19:24.706: CCSIP-SPI-CONTROL: act_recdproc_new_message
Nov 15 18:19:24.706: CCSIP-SPI-CONTROL: sipSPICheckResponse
Nov 15 18:19:24.706: sip_stats_status_code
Nov 15 18:19:24.706: Roundtrip delay 2032 milliseconds for method PRACK
Nov 15 18:19:24.706: sipSPIGetSdpBody : Parse incoming session description
Nov 15 18:19:24.710: CCSIP-SPI-CONTROL: sipSPIUACSessionTimer
Nov 15 18:19:24.710: CCSIP-SPI-CONTROL: act_recdproc_continue_200_processing
Nov 15 18:19:24.710: CCSIP-SPI-CONTROL: act_recdproc_continue_200_processing: *** This ccb
is the parent
Nov 15 18:19:24.710: sipSPICompareRespMediaInfo
Nov 15 18:19:24.710: sipSPIDoMediaNegotiation: number of m lines is 1
Nov 15 18:19:24.710: sipSPIDoAudioNegotiation: Codec (g729r8) Negotiation Successful on
Static Payload
Nov 15 18:19:24.710: sipSPIDoPtimeNegotiation: One ptime attribute found - value:10
Nov 15 18:19:24.710: convert_ptime_to_codec_bytes: Values :Codec: g729r8 ptime :10,
codecbytes: 20
Nov 15 18:19:24.710: convert_codec_bytes_to_ptime: Values :Codec: g729r8 codecbytes :20,
ptime: 10
Nov 15 18:19:24.710: sipSPIDoDTMFRelayNegotiation: m-line index 1
Nov 15 18:19:24.710: sipSPIDoDTMFRelayNegotiation: Requested DTMF-RELAY option(s) not
found in Preferred DTMF-RELAY option list!
Nov 15 18:19:24.710: sip_sdp_get_modem_relay_cap_params:
Nov 15 18:19:24.710: sip_sdp_get_modem_relay_cap_params: NSE payload from X-cap = 0
Nov 15 18:19:24.710: sip_do_nse_negotiation: NSE Payload 100 found in SDP
Nov 15 18:19:24.710: sip_do_nse_negotiation: Remote NSE payload = local one = 100, Use it
Nov 15 18:19:24.710: sip_select_modem_relay_params: X-tmr not present in SDP. Disable
modem relay
Nov 15 18:19:24.710: sipSPIProcessMediaChanges
Nov 15 18:19:24.710: ccsip_process_response_contact_record_route
Nov 15 18:19:24.710: CCSIP-SPI-CONTROL: sipSPIProcess200OKforinvite
Nov 15 18:19:24.710: sip_stats_method
Nov 15 18:19:24.710: udpsock_close_connect: Socket fd: 1 closed for connid 1 with remote
port: 5060
Nov 15 18:19:37.479: HandleUdpSocketReads :Msg enqueued for SPI with IPAddr:
172.18.193.190:52180
Nov 15 18:19:37.483: ****Found CCB in UAC table
Nov 15 18:19:37.483: CCSIP-SPI-CONTROL: act_active_new_message
Nov 15 18:19:37.483: CCSIP-SPI-CONTROL: sact_active_new_message_request
Nov 15 18:19:37.483: sip_stats_method
Nov 15 18:19:37.483: sip_stats_status_code
Nov 15 18:19:37.483: CCSIP-SPI-CONTROL: sipSPIInitiateCallDisconnect : Initiate call
disconnect(16) for outgoing call
Nov 15 18:19:37.483: udpsock_cclose_connect: Socket fd: 2 closed for connid 2 with remote
port: 5060
Nov 15 18:19:37.483: CCSIP-SPI-CONTROL: act_disconnecting_disconnect
Nov 15 18:19:37.483: CCSIP-SPI-CONTROL: sipSPICallCleanup
Nov 15 18:19:37.483: sipSPIIcpifUpdate :CallState: 4 Playout: 10230 DiscTime:1745148
ConnTime 1743871
Nov 15 18:19:37.483: ****Deleting from UAC table
Nov 15 18:19:37.483: Removing call id E
Nov 15 18:19:37.483: freeing ccb 63330954

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug ccsip all</b>	Enables all SIP-related debugging.
<b>debug ccsip events</b>	Enables tracing of events that are specific to SIP SPI.
<b>debug ccsip media</b>	Enables tracing of SIP call media streams.

# debug ccsip media

To enable tracing of Session Limitation Protocol (SIP) call media streams, use the **debug ccsip media** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ccsip media**

**no debug ccsip media**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.

**Usage Guidelines** Beginning in Cisco IOS Release 12.2(15)T, the **debug ccsip media** command is a separate option that displays debugging information specific to SIP media stream processing. In past releases, this output was part of the **debug ccsip events** command.



**Note**

This command is intended for use by Cisco technicians only.

**Examples** The following is sample output from the **debug ccsip media** command for a Cisco 3660:

```
Router# debug ccsip media

SIP Call media tracing is enabled
Router#
Nov 15 18:19:53.835: sipSPISetMediaSrcAddr: media src addr for stream 1 = 172.18.195.49
Nov 15 18:19:53.835: sipSPIReserveRtpPort: reserved port 16500 for stream 1
Nov 15 18:19:53.867: sipSPIReplaceSDP
Nov 15 18:19:53.871: sipSPICopySdpInfo
Nov 15 18:19:53.871: sipSPIUpdCallWithSdpInfo:
Preferred Codec : g729r8, bytes :20
Preferred DTMF relay : inband-voice
Preferred NTE payload : 101
Early Media : No
Delayed Media : No
Bridge Done : No
New Media : No
DSP DNLD Reqd : No
Nov 15 18:19:53.871: sipSPISetMediaSrcAddr: media src addr for stream 1 = 172.18.195.49
Nov 15 18:19:53.871: sipSPIUpdCallWithSdpInfo:
M-line Index : 1
State : STREAM_ADDING (3)
Callid : -1
Negotiated Codec : g729r8, bytes :20
Negotiated DTMF relay : inband-voice
```

```

Negotiated NTE payload : 0
Media Srce Addr/Port : 172.18.195.49:16500
Media Dest Addr/Port : 172.18.193.190:19148
Nov 15 18:19:53.871: sipSPIProcessRtpSessions
Nov 15 18:19:53.871: sipSPIAddStream: Adding stream 1 (callid 16) to the VOIP RTP library
Nov 15 18:19:53.871: sipSPISetMediaSrcAddr: media src addr for stream 1 = 172.18.195.49
Nov 15 18:19:53.871: sipSPIUpdateRtcpSession: for m-line 1
Nov 15 18:19:53.871: sipSPIUpdateRtcpSession: rtcp_session info
laddr = 172.18.195.49, lport = 16500, raddr = 172.18.193.190, rport=19148
Nov 15 18:19:53.871: sipSPIUpdateRtcpSession: No rtp session, creating a new one
Nov 15 18:19:53.871: sipSPISetStreamInfo: num_streams = 1
Nov 15 18:19:53.871: sipSPISetStreamInfo: adding stream type 0 from mline 1
Nov 15 18:19:53.871: sipSPISetStreamInfo: caps.stream_count=1,
caps.stream_list[0].stream_type=0x1, caps.stream_list.xmitFunc=voip_rtp_xmit,
caps.stream_list.context=0x634F1F2C (gccb)
Nov 15 18:19:55.555: sipSPICompareSDP
Nov 15 18:19:55.555: sipSPICompareStreams: stream 1 dest_port: old=19148 new=19148
Nov 15 18:19:55.555: sipSPICompareStreams: Flags set for stream 1: RTP_CHANGE=No
CAPS_CHANGE=No
Nov 15 18:19:55.555: sipSPICompareSDP: Flags set for call: NEW_MEDIA=No DSPDNLD_REQD=No
Nov 15 18:19:55.555: sipSPIReplaceSDP
Nov 15 18:19:55.555: sipSPICopySdpInfo
Nov 15 18:19:55.555: sipSPIUpdCallWithSdpInfo:
Preferred Codec : g729r8, bytes :20
Preferred DTMF relay : inband-voice
Preferred NTE payload : 101
Early Media : No
Delayed Media : No
Bridge Done : Yes
New Media : No
DSP DNLD Reqd : No
Nov 15 18:19:55.555: sipSPISetMediaSrcAddr: media src addr for stream 1 = 172.18.195.49
Nov 15 18:19:55.555: sipSPIUpdCallWithSdpInfo:
M-line Index : 1
State : STREAM_ACTIVE (3)
Callid : 16
Negotiated Codec : g729r8, bytes :20
Negotiated DTMF relay : inband-voice
Negotiated NTE payload : 0
Media Srce Addr/Port : 172.18.195.49:16500
Media Dest Addr/Port : 172.18.193.190:19148

```

---

**Related Commands**

Command	Description
<b>debug ccsip all</b>	Enables all SIP-related debugging.
<b>debug ccsip events</b>	Enables tracing of events that are specific to SIP SPI.
<b>debug ccsip info</b>	Enables tracing of general SIP SPI events.

---

# debug ccsip messages

To show all Session Initiation Protocol (SIP) Service Provider Interface (SPI) message tracing, use the **debug ccsip messages** command in privileged EXEC 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.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Version	Description
	12.1(1)T	This command was introduced.
	12.1(3)T	The output of this command was changed.
	12.2(2)XA	Support was added for the Cisco AS5350 and Cisco AS5400 universal gateways.
	12.2(2)XB1	This command was implemented on the Cisco AS5850 universal gateway.
	12.2(8)T	This command was implemented on Cisco 7200 series routers.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support for the Cisco AS5300 universal access server, Cisco AS5350, Cisco AS5400, and Cisco AS5850 universal gateway is not included in this release.

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

**Examples** The following example shows debug output from one side of the call:

```
Router1# debug ccsip messages

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 1993 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 1993 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 1993 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 1993 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 1993 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 1993 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 1993 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

```

The following example show debug output from the other side of the call:

```
Router2# debug ccsip messages
```

```

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 1993 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 1993 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 1993 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 1993 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 1993 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 1993 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 1993 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**

<b>debug ccsip all</b>	Enables all SIP-related debugging.
<b>debug ccsip calls</b>	Shows all SIP SPI call tracing.
<b>debug ccsip error</b>	Shows SIP SPI errors.
<b>debug ccsip events</b>	Shows all SIP SPI events tracing.
<b>debug ccsip states</b>	Shows all SIP SPI state tracing.

# debug ccsip preauth

To enable diagnostic reporting of authentication, authorization, and accounting (AAA) preauthentication for Session Initiation Protocol (SIP) calls, use the **debug ccsip preauth** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ccsip preauth**

**no debug ccsip preauth**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

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

**Examples** The following example shows debug output for a single SIP call:

```
Router# debug ccsip preauth

SIP Call preauth tracing is enabled
Jan 23 18:43:17.898::Preauth Required
Jan 23 18:43:17.898: In sipSPISendPreauthReq for preauth_id = 86515, ccb = 67AF4E10
Jan 23 18:43:17.898: Entering rpms_proc_print_preauth_req

Jan 23 18:43:17.898: Request = 0
Jan 23 18:43:17.898: Preauth id = 86515
Jan 23 18:43:17.898: EndPt Type = 1
Jan 23 18:43:17.898: EndPt = 192.168.80.70
Jan 23 18:43:17.898: Resource Service = 1
Jan 23 18:43:17.898: Call_origin = answer
Jan 23 18:43:17.898: Call_type = voip
Jan 23 18:43:17.898: Calling_num = 2270001
Jan 23 18:43:17.898: Called_num = 1170001
Jan 23 18:43:17.898: Protocol = 1
Jan 23 18:43:17.898:sipSPISendPreauthReq:Created node with preauth_id = 86515, ccb
67AF4E10 , node 6709C280
Jan 23 18:43:17.898:rpms_proc_create_node:Created node with preauth_id = 86515
Jan 23 18:43:17.898:rpms_proc_send_aaa_req:uid got is 466728
Jan 23 18:43:17.902:rpms_proc_preauth_response:Context is for preauth_id 86515, aaa_uid
466728
Jan 23 18:43:17.902:rpms_proc_preauth_response:Deleting Tree node for preauth id 86515 uid
466728
Jan 23 18:43:17.902:sipSPIGetNodeForPreauth:Preauth_id=86515
```

```
Jan 23 18:43:17.902: ccsip_spi_process_preauth_event:67AF4E10 ccb & 6709C280 node
Jan 23 18:43:17.902: In act_preauth_response:67AF4E10 ccb
Jan 23 18:43:17.902: act_preauth_response:Deleting node 6709C280 from tree
```

Table 39 describes the significant fields shown in the display.

**Table 39** *debug ccsip preauth Field Descriptions*

Field	Description
Request	Request Type—0 for preauthentication, 1 for disconnect.
Preauth id	Identifier for the preauthentication request.
EndPt Type	Call Origin End Point Type—1 for IP address, 2 for Interzone ClearToken (IZCT) value.
EndPt	Call Origin End Point Value—An IP address or IZCT value.
Resource Service	Resource Service Type—1 for Reservation, 2 for Query.
Call_origin	Answer.
Call_type	Voice over IP (VoIP).
Calling_num	Calling Party Number (CLID).
Called_num	Called Party Number (DNIS).
Protocol	0 for H.323, 1 for SIP.
function reports	Various identifiers and status reports for executed functions.

# debug ccsip states

To show all Session Initiation Protocol (SIP) Service Provider Interface (SPI) state tracing, use the **debug ccsip states** command in privileged EXEC 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.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History		
12.1(1)T		This command was introduced.
12.2(2)XA		Support was added for the Cisco AS5350 and Cisco AS5400 universal gateways.
12.2(2)XB1		This command was implemented on the Cisco AS5850 universal gateway.
12.2(8)T		This command was implemented on Cisco 7200 series routers.
12.2(11)T		This command was integrated into Cisco IOS Release 12.2(11)T. Support for the Cisco AS5300 universal access server, Cisco AS5350, Cisco AS5400, and Cisco AS5850 universal gateway is not included in this release.

**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
<a href="#">debug ccsip all</a>	Enables all SIP-related debugging.
<a href="#">debug ccsip calls</a>	Shows all SIP SPI call tracing.
<a href="#">debug ccsip error</a>	Shows SIP SPI errors.
<a href="#">debug ccsip events</a>	Shows all SIP SPI events tracing.
<a href="#">debug ccsip info</a>	Shows all SIP SPI message tracing.

# debug ccswwoice vo-debug

To display detailed debugging information related to ccswwoice function calls during call setup and teardown, use the **debug ccswwoice vo-debug** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ccswwoice vo-debug**

**no debug ccswwoice vo-debug**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 networking device.
	12.0(7)XK	This command was implemented on the Cisco 3600 series router.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

**Usage Guidelines** Use this command when attempting to troubleshoot a Vo call that uses the “cisco-switched” session protocol. This command provides the same information as the **debug ccswwoice vo-session** command, but includes additional debugging information relating to the calls.

**Examples** The following shows sample output from the **debug ccswwoice vo-debug** command:

```
Router# debug ccswwoice vo-debug

2w2d: ccswwoice: callID 529927 pvcid -1 cid -1 state NULL event O/G SETUP
2w2d: ccswwoice_out_callinit_setup: callID 529927 using pvcid 1 cid 15
2w2d: ccswwoice: callID 529927 pvcid 1 cid 15 state O/G INIT event I/C PROC
2w2d: ccswwoice: callID 529927 pvcid 1 cid 15 state O/G PROC event I/C
ALERTccfrf11_caps_ind: codec(preferred) = 1

2w2d: ccswwoice: callID 529927 pvcid 1 cid 15 state O/G ALERT event I/C CONN
2w2d: ccswwoice_bridge_drop: dropping bridge calls src 529927 dst 529926 pvcid 1 cid 15
state ACTIVE
2w2d: ccswwoice: callID 529927 pvcid 1 cid 15 state ACTIVE event O/G REL
2w2d: ccswwoice: callID 529927 pvcid 1 cid 15 state RELEASE event I/C RELCOMP
2w2d: ccswwoice_store_call_history_entry: cause=10 tcause=10 cause_text=normal call
clearing.
```

Related Commands	Command	Description
	<b>debug ccswwoice vo-session</b>	Displays the first 10 bytes (including header) of selected VoFR subframes for the interface.

# debug ccswwoice vofr-debug

To display the ccswwoice function calls during call setup and teardown, use the **debug ccswwoice vofr-debug** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ccswwoice vofr-debug**

**no debug ccswwoice vofr-debug**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco 2600 and Cisco 3600 series routers.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
	12.0(7)XK	This command was implemented on the Cisco MC3810 networking device.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

**Usage Guidelines** Use this command when troubleshooting a VoFR call that uses the “cisco-switched” session protocol. This command provides the same information as the **debug ccswwoice vofr-session** command, but includes additional debugging information relating to the calls.

**Examples** The following shows sample output from the **debug ccswwoice vofr-debug** command:

```
Router# debug ccswwoice vofr-debug
```

```
CALL TEARDOWN:
3640_vofr(config-voiceport)#
*Mar  1 03:02:08.719:ccswvofr_bridge_drop:dropping bridge calls src 17 dst 16 dlci 100
      cid 9 state ACTIVE
*Mar  1 03:02:08.727:ccswvofr:callID 17 dlci 100 cid 9 state ACTIVE event O/G REL
*Mar  1 03:02:08.735:ccswvofr:callID 17 dlci 100 cid 9 state RELEASE event I/C RELCOMP
*Mar  1 03:02:08.735:ccswvofr_store_call_history_entry:cause=22 tcause=22
      cause_text=no circuit.
3640_vofr(config-voiceport)#
```

```
CALL SETUP (outgoing):
*Mar  1 03:03:22.651:ccswvofr:callID 23 dlci -1 cid -1 state NULL event O/G SETUP
*Mar  1 03:03:22.651:ccswvofr_out_callinit_setup:callID 23 using dlci 100 cid 10
*Mar  1 03:03:22.659:ccswvofr:callID 23 dlci 100 cid 10 state O/G INIT event I/C PROC
*Mar  1 03:03:22.667:ccswvofr:callID 23 dlci 100 cid 10 state O/G PROC event I/C CONN
ccfrf11_caps_ind:codec(preferred) = 0
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">debug cch323</a>	Displays the ccfrf11 function calls during call setup and teardown.
<a href="#">debug ccsvoice vo-debug</a>	Displays the ccsvoice function calls during call setup and teardown.
<b>debug vtsp session</b>	Displays the first 10 bytes (including header) of selected VoFR subframes for the interface.

# debug ccswwoice vofr-session

To display the ccswwoice function calls during call setup and teardown, use the **debug ccswwoice vofr-session** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ccswwoice vofr-session**

**no debug ccswwoice vofr-session**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(3)XG	This command was introduced on the Cisco 2600 and Cisco 3600 series routers.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
	12.0(7)XK	This command was implemented on the Cisco MC3810 networking device.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

**Usage Guidelines** Use this command to show the state transitions of the cisco-switched-vofr state machine as a call is processed, and when attempting to troubleshoot a VoFR call that uses the “cisco-switched” session protocol.

**Examples** The following shows sample output from the **debug ccswwoice vofr-session** command:

```
Router# debug ccswwoice vofr-session

CALL TEARDOWN:
3640_vofr(config-voiceport)#
*Mar  1 02:58:13.203:ccswvofr:callID 14 dlci 100 cid 8 state ACTIVE event O/G REL
*Mar  1 02:58:13.215:ccswvofr:callID 14 dlci 100 cid 8 state RELEASE event I/C RELCOMP
3640_vofr(config-voiceport)#

CALL SETUP (outgoing):
*Mar  1 02:59:46.551:ccswvofr:callID 17 dlci -1 cid -1 state NULL event O/G SETUP
*Mar  1 02:59:46.559:ccswvofr:callID 17 dlci 100 cid 9 state O/G INIT event I/C PROC
*Mar  1 02:59:46.567:ccswvofr:callID 17 dlci 100 cid 9 state O/G PROC event I/C CONN
3640_vofr(config-voiceport)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">debug cch323</a>	Displays the ccfrf11 function calls during call setup and teardown.
<b>debug call rsvp-sync events</b>	Displays events that occur during RSVP setup.
<b>debug vtsp session</b>	Displays the first 10 bytes (including header) of selected VoFR subframes for the interface.

# debug ccswwoice vo-session

To display the first 10 bytes (including header) of selected VoFR subframes for the interface, use the **debug ccswwoice vo-session** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ccswwoice vo-session**

**no debug ccswwoice vo-session**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.3(1)MA	This command was introduced on the Cisco MC3810 networking device.
	12.0(7)XK	This command was implemented on the Cisco 3600 series router.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

**Usage Guidelines** Use this command to show the state transitions of the cisco-switched-vo state machine as a call is processed. This command should be used when attempting to troubleshoot a Vo call that uses the “cisco-switched” session protocol.

**Examples** The following shows sample output from the **debug ccswwoice vo-session** command:

```
Router# debug ccswwoice vo-session

2w2d: ccswwoice: callID 529919 pvcid -1 cid -1 state NULL event O/G SETUP
2w2d: ccswwoice: callID 529919 pvcid 1 cid 11 state O/G INIT event I/C PROC
2w2d: ccswwoice: callID 529919 pvcid 1 cid 11 state O/G PROC event I/C ALERT
2w2d: ccswwoice: callID 529919 pvcid 1 cid 11 state O/G ALERT event I/C CONN
2w2d: ccswwoice: callID 529919 pvcid 1 cid 11 state ACTIVE event O/G REL
2w2d: ccswwoice: callID 529919 pvcid 1 cid 11 state RELEASE event I/C RELCOMP
```

Related Commands	Command	Description
	<b>debug ccswwoice vo-debug</b>	Displays detailed debugging information related to ccswwoice function calls during call setup and teardown.

# debug cdapi

To display information about the call distributor application programming interface (CDAPI), use the **debug cdapi** command in privileged EXEC mode.

```
debug cdapi {detail | events}
```

Syntax Description	<i>detail</i>	Displays when applications register or unregister with CDAPI, when calls are added or deleted from the CDAPI routing table, and when CDAPI messages are created and freed. It is useful for determining if messages are being lost (or not freed) and the size of the raw messages passed between CDAPI and applications so that you can check that the correct number of bytes is being passed.
	<i>events</i>	Displays the events passing between CDAPI and an application or signalling stack. This debug is useful for determining if certain ISDN messages are not being received by an application and if calls are not being directed to an application.

**Defaults** Disabled

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(6)T	This command was introduced.

**Examples** The following example shows output for the **debug cdapi** command:

```
Router# debug cdapi

003909 ISDN Se123 RX <- SETUP pd = 8 callref = 0x06BB
003909     Bearer Capability i = 0x9090A2
003909     Channel ID i = 0xA18381
003909     Facility i =
0x9FAA068001008201008B0100A1180202274C020100800F534341524C415454492D3530303733
003909     Progress Ind i = 0x8183 - Origination address is non-ISDN
003909     Calling Party Number i = 0xA1, '50073'
003909     Called Party Number i = 0xC1, '3450070'
003909 CDAPI Se123 TX -> CDAPI_MSG_CONNECT_IND to TSP CDAPI Application call = 0x24
003909     From Appl/Stack = ISDN
003909     Call Type = VOICE
003909     B Channel = 0
003909     Cause = 0
003909     Calling Party Number = 50073
003909     Called Party Number = 3450070
003909 CDAPI Se123 TX -> CDAPI_MSG_CONNECT_RESP to ISDN call = 0x24
003909     From Appl/Stack = TSP CDAPI Application
003909     Call Type = VOICE
003909     B Channel = 0
```

```

003909      Cause      = 0
003909 CDAPI-ISDN Se123 RX <- CDAPI_MSG_CONNECT_RESP from TSP CDAPI Application call =
0x24
003909      Call Type = VOICE
003909      B Channel = 0
003909      Cause      = 0
003909 CDAPI Se123 TX -> CDAPI_MSG_SUBTYPE_CALL_PROC_REQ to ISDN call = 0x24
003909      From Appl/Stack = TSP CDAPI Application
003909      Call Type = VOICE
003909      B Channel = 0
003909      Cause      = 0
003909 CDAPI-ISDN Se123 RX <- CDAPI_MSG_SUBTYPE_CALL_PROC_REQ from TSP CDAPI Application
call = 0x24
003909      Call Type = VOICE
003909      B Channel = 0
003909      Cause      = 0
003909 ISDN Se123 TX -> CALL_PROC pd = 8  callref = 0x86BB
003909      Channel ID i = 0xA98381

```

**Related Commands**

Command	Description
debug voip rawmsg	Displays the raw message owner, length, and pointer.

# debug cdp

To enable debugging of the Cisco Discovery Protocol (CDP), use the **debug cdp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug cdp {packets | adjacency | events}
```

```
no debug cdp {packets | adjacency | events}
```

Syntax Description		
	<b>packets</b>	Enables packet-related debugging output.
	<b>adjacency</b>	Enables adjacency-related debugging output.
	<b>events</b>	Enables output related to error messages, such as detecting a bad checksum.

**Command Modes** Privileged EXEC

**Usage Guidelines** Use **debug cdp** commands to display information about CDP packet activity, activity between CDP neighbors, and various CDP events.

**Examples** The following is sample output from **debug cdp packets**, **debug cdp adjacency**, and **debug cdp events** commands:

```
Router# debug cdp packets
```

```
CDP packet info debugging is on
```

```
Router# debug cdp adjacency
```

```
CDP neighbor info debugging is on
```

```
Router# debug cdp events
```

```
CDP events debugging is on
```

```
CDP-PA: Packet sent out on Ethernet0
```

```
CDP-PA: Packet received from gray.cisco.com on interface Ethernet0
```

```
CDP-AD: Deleted table entry for violet.cisco.com, interface Ethernet0
```

```
CDP-AD: Interface Ethernet2 coming up
```

```
CDP-EV: Encapsulation on interface Serial2 failed
```

# debug cdp ip

To enable debug output for the IP routing information that is carried and processed by the Cisco Discovery Protocol (CDP), use the **debug cdp ip** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug cdp ip**

**no debug cdp ip**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

**Usage Guidelines** CDP is a media- and protocol-independent device-discovery protocol that runs on all Cisco routers.

You can use the **debug cdp ip** command to determine the IP network prefixes CDP is advertising and whether CDP is correctly receiving this information from neighboring routers.

Use the **debug cdp ip** command with the **debug ip routing** command to debug problems that occur when on-demand routing (ODR) routes are not installed in the routing table at a hub router. You can also use the **debug cdp ip** command with the **debug cdp packet** and **debug cdp adjacency** commands along with encapsulation-specific debug commands to debug problems that occur in the receipt of CDP IP information.

**Examples** The following is sample output from the **debug cdp ip** command. This example shows the transmission of IP-specific information in a CDP update. In this case, three network prefixes are being sent, each with a different network mask.

```
Router# debug cdp ip

CDP-IP: Writing prefix 172.1.69.232.112/28
CDP-IP: Writing prefix 172.19.89.0/24
CDP-IP: Writing prefix 11.0.0.0/8
```

In addition to these messages, you might see the following messages:

- This message indicates that CDP is attempting to install the prefix 172.16.1.0/24 into the IP routing table:

```
CDP-IP: Updating prefix 172.16.1.0/24 in routing table
```

- This message indicates a protocol error occurred during an attempt to decode an incoming CDP packet:

```
CDP-IP: IP TLV length (3) invalid
```

- This message indicates the receipt of the IP prefix 172.16.1.0/24 from a CDP neighbor connected via Ethernet interface 0/0. The neighbor IP address is 10.0.0.1.

```
CDP-IP: Reading prefix 172.16.1.0/24 source 10.0.0.1 via Ethernet0/0
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug ip routing</b>	Displays information on RIP routing table updates and route cache updates.

---

# debug ces-conn

To display information from circuit emulation service (CES) clients, use the **debug ces-conn** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ces-conn** [**all** | **errors** | **events**]

**no debug ces-conn**

## Syntax Description

<b>all</b>	(Optional) Displays all error and event information.
<b>errors</b>	(Optional) Displays only error information.
<b>events</b>	(Optional) Displays only event information.

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(5)XM	This command is supported on Cisco 3600 series routers.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

## Examples

The following example shows debug output for a CES connection:

```
Router# debug ces-conn all

CES all debugging is on
Router#

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# connect conn1 t1 3/0 1 atm1/0 1/100

Router(config-ces-conn)# exit

Router(config)#
*Mar  6 18:32:27:CES_CLIENT:vc QoS parameters are PCR = 590, CDV =
5000, CAS_ENABLED = 1,partial fill = 0, multiplier = 8, cbr rate = 64,
clock recovery = 0,service_type = 3, error method = 0,sdt_size = 196,
billing count = 0
*Mar  6 18:32:27:CES_CLIENT:attempt 1 to activate segment>
```

# debug channel events

To display processing events on Cisco 7000 series routers that occur on the channel adapter interfaces of all installed adapters, use the **debug channel events** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug channel events**

**no debug channel events**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(3)T	This command was introduced.

**Usage Guidelines** This command displays CMCC adapter events that occur on the Channel Interface Processor (CIP) or Channel Port Adapter (CPA) and is useful for diagnosing problems in an IBM channel attach network. It provides an overall picture of the stability of the network. In a stable network, the **debug channel events** command does not return any information. If the command generates numerous messages, the messages can indicate the possible source of the problems. To observe the statistic message (cip\_love\_letter) sent every 10 seconds, use the **debug channel love** command.

When configuring or making changes to a router or interface that supports IBM channel attach, enable the **debug channel events** command. Doing so alerts you to the progress of the changes or to any errors that might result. Also use this command periodically when you suspect network problems.

**Examples** The following sample output is from the **debug channel events** command:

```
Router# debug channel events

Channel3/0: cip_reset(), state administratively down
Channel3/0: cip_reset(), state up
Channel3/0: sending nodeid
Channel3/0: sending command for vc 0, CLAW path C700, device C0
```

The following line indicates that the CIP is being reset to an administrative down state:

```
Channel3/0: cip_reset(), state administratively down
```

The following line indicates that the CIP is being reset to an administrative up state:

```
Channel3/0: cip_reset(), state up
```

The following line indicates that the node ID is being sent to the CIP. This information is the same as the “Local Node” information under the **show extended channel slot/port subchannels** command. The CIP needs to send this information to the host mainframe.

```
Channel3/0: sending nodeid
```

The following line indicates that a Common Link Access for Workstations (CLAW) subchannel command is being sent from the Route Processor (RP) to the CIP. The value vc 0 indicates that the CIP will use virtual circuit number 0 with this device. The virtual circuit number also shows up when you use the **debug channel packets** command.

```
Channel13/0: sending command for vc 0, CLAW path C700, device C0
```

The following is a sample output that is generated by the **debug channel events** command when a CMPC+ IP TG connection is activated with the host:

```
1d05h:Channel14/2:Received route UP for tg (768)
1d05h:Adding STATIC ROUTE for vc:768
```

The following is a sample output from the **debug channel events** command when a CMPC+ IP TG connection is deactivated:

```
1d05h:Channel14/2:Received route DOWN for tg (768)
1d05h:Deleting STATIC ROUTE for vc:768
```

**Related Commands**

Command	Description
<a href="#">debug channel ilan</a>	Displays CIP love letter events.
<a href="#">debug channel packets</a>	Displays per-packet debugging output.

# debug channel ilan

To display messages relating to configuration and bridging using CMCC internal LANs and to help debug source-route bridging (SRB) problems related to CMCC internal LANs, use the **debug channel ilan** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug channel ilan**

**no debug channel ilan**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.0(3)	This command was introduced.

**Usage Guidelines** The **debug channel ilan** command displays events related to CMCC internal LANs. This command is useful for debugging problems associated with CMCC internal LAN configuration. It is also useful for debugging problems related to SRB packet flows through internal LANs.

**Examples** The following sample output is from the **debug channel ilan** command:

```
Router# debug channel ilan
```

```
Channel internal LANs debugging is on
```

The following line indicates that a packet destined for the CMCC via a configured internal MAC adapter configured on an internal LAN was dropped because the Logical Link Control (LLC) end station in Cisco IOS software did not exist:

```
CIP ILAN(Channel13/2-Token): Packet dropped - NULL LLC
```

The following line indicates that a packet destined for the CMCC via a configured internal MAC adapter configured on an internal LAN was dropped because the CMCC had not yet acknowledged the internal MAC adapter configuration command:

```
Channel13/2: ILAN Token-Ring 3 - CIP internal MAC adapter not acknowledged
DMAC(4000.7000.0001) SMAC(0c00.8123.0023)
```

Related Commands	Command	Description
	<b>debug channel events</b>	Displays processing that occurs on the channel adapter interfaces of all installed adapters.
	<b>debug source bridge</b>	Displays information about packets and frames transferred across a source-route bridge.

# debug channel love

To display Channel Interface Processor (CIP) love letter events, use the **debug channel love** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug channel love**

**no debug channel love**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

**Usage Guidelines** This command displays CIP love letter events (an operating status or configuration message) that occur on the CIP interface processor and is useful for diagnosing problems in an IBM channel attach network. It provides an overall picture of the stability of the network. In a stable network, the **debug channel love** command returns a statistic message (cip\_love\_letter) that is sent every 10 seconds. This command is valid for the Cisco 7000 series routers only.

**Examples** The following is sample output from the **debug channel love** command:

```
Router# debug channel love

Channel3/1: love letter received, bytes 3308
Channel3/0: love letter received, bytes 3336
cip_love_letter: received 11, but no cip_info
```

The following line indicates that data was received on the CIP:

```
Channel3/1: love letter received, bytes 3308
```

The following line indicates that the interface is enabled, but there is no configuration for it. It does not normally indicate a problem, just that the Route Processor (RP) got statistics from the CIP but has no place to store them.

```
cip_love_letter: received 11, but no cip_info
```

## Related Commands

Command	Description
<a href="#">debug channel events</a>	Displays processing that occurs on the channel adapter interfaces of all installed adapters.
<a href="#">debug channel packets</a>	Displays per-packet debugging output.

# debug channel packets

To display per-packet debugging output, use the **debug channel packets** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug channel packets**

**no debug channel packets**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

**Usage Guidelines** The **debug channel packets** command displays all process-level Channel Interface Processor (CIP) packets for both outbound and inbound packets. The output reports information when a packet is received or a transmission is attempted. You will need to disable fast switching and autonomous switching to obtain debugging output. This command is useful for determining whether packets are received or sent correctly.

This command is valid for the Cisco 7000 series routers only.

**Examples** The following is sample output from the **debug channel packets** command:

```
Router# debug channel packets

(Channel3/0)-out size = 104, vc = 0000, type = 0800, src 172.24.0.11, dst 172.24.1.58
(Channel3/0)-in size = 48, vc = 0000, type = 0800, src 172.24.1.58, dst 172.24.15.197
(Channel3/0)-in size = 48, vc = 0000, type = 0800, src 172.24.1.58, dst 172.24.15.197
(Channel3/0)-out size = 71, vc = 0000, type = 0800, src 172.24.15.197, dst 172.24.1.58
(Channel3/0)-in size = 44, vc = 0000, type = 0800, src 172.24.1.58, dst 172.24.15.197
```

[Table 40](#) describes the significant fields shown in the display.

**Table 40** *debug channel packets Field Descriptions*

Field	Description
(Channel3/0)	Interface slot and port.
in/out	“In” is a packet from the mainframe to the router. “Out” is a packet from the router to the mainframe.
size =	Number of bytes in the packet, including internal overhead.
vc =	Value from 0 to 511 that maps to the <b>claw</b> interface configuration command. This information is from the MAC layer.
type =	Encapsulation type in the MAC layer. The value 0800 indicates an IP datagram.
src	Origin, or source, of the packet, as opposed to the previous hop address.
dst	Destination of the packet, as opposed to the next-hop address.