show mrcp client session active through show sip dhcp

show monitor event-trace voip ccsip (EXEC)

To display the captured Voice over IP (VoIP) Call-Control Session Initiation Protocol (CCSIP) event-traces on console, use the **show monitor event-trace voip ccsip** command in user EXEC or privileged EXEC mode.

show monitor event-trace voip ccsip {**api** | **fsm** | **global** | **history** | **merged** | **misc** | **msg** | **summary**} [**filter** {**call-id** | **called-num** | **calling-num** | **sip-call-id**} *filter*] {**all** | **back** *duration* | **clock** *time* | **from-boot** *seconds* | **latest**}

Syntax Description

api	Displays information about event tracing for VOIP CCSIP API events.
fsm	Displays information about event tracing for Finite State Machine (FSM) and Communicating Nested FSM (CNFSM) events.
global	Displays information about event tracing for global events.
history	Displays information about all completed calls.
merged	Displays information about merged events.
misc	Displays information about miscellaneous events.
msg	Displays information about event tracing message events.
summary	Displays a summary of all captured information.
filter	(Optional) Filters information to be displayed based on the selected filter options.
call-id *filter*	Displays information related to the specified call ID.
called-num *filter*	Displays information related to the specified called number.
calling-num *filter*	Displays information related to the specified calling number.
sip-call-id *filter*	Displays information related to the specified SIP call-id.
all	Displays all event trace information in the current buffer.
back *duration*	Displays all event trace information from the current time going backwards for the duration specified.

clock *time*	Displays information from the specified time until the current time.
from-boot *seconds*	Displays information from this many seconds after boot.
latest	Displays the latest trace events since the last display.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Use the **monitor event-trace voip ccsip** command to control what, when, and how event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace voip ccsip** command in global configuration mode.

Use the **show monitor event-trace voip ccsip** command to display event traces for the configured events.

Use the **filter** keyword to limit traces for specific SIP based parameters, this ensures that only relevant traces are displayed on the console.

Example

The following example shows how to display a summary of statistics for active call traces:

```
Device# show monitor event-trace voip ccsip summary
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4

--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
```

The following example shows how to display information about all miscellaneous event traces:

```
Device# show monitor event-trace voip ccsip misc all
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
```

```
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4
--------------------------------
*Jul  2 13:16:30.118: Inbound dial-peer matched : tag = 11111
*Jul  2 13:16:30.119: Media Stream Index = 1, Media Stream Type = voice-only Stream State
= STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.120: Media Stream Index = 1, Media Stream Type = voice-only Stream State
= STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.131: Media Stream Index = 1, Media Stream Type = voice-only Stream State
= STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
--------------------------------
*Jul  2 13:16:30.122: Outbound dial-peer matched : tag = 22222
*Jul  2 13:16:30.123: Media Stream Index = 1, Media Stream Type = voice-only Stream State
= STREAM_ADDING
        Negotiated Codec = No Codec    Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.129: Media Stream Index = 1, Media Stream Type = voice-only Stream State
= STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
```

The following example displays the captured event traces for Finite State Machine (FSM) and Communicating Nested FSM (CNFSM) events:

```
Device# show monitor event-trace voip ccsip fsm all
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4
--------------------------------
*Jul  2 13:16:30.116: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_NONE Next State
 = STATE_IDLE Current Substate = STATE_NONE Next Substate = STATE_IDLE
*Jul  2 13:16:30.118: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_INVITE_SDP_RCVD,
     Current State = S_SIP_EARLY_DIALOG_IDLE,    Next State = S_SIP_EARLY_DIALOG_OFFER_RCVD
*Jul  2 13:16:30.118: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_RCVD_SDP,
Current State = S_SIP_IWF_SDP_IDLE, Next State = S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT
*Jul  2 13:16:30.119: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_IDLE Next State
 = STATE_RECD_INVITE Current Substate = STATE_IDLE Next Substate = STATE_RECD_INVITE
*Jul  2 13:16:30.121: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SET_MODE,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.122:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_CC_CALL_PROCEEDING
     Current State = STATE_RECD_INVITE
*Jul  2 13:16:30.122: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,   Current State = CNFSM_CONTAINER_STATE,
Next State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:16:30.127:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_CC_CALL_ALERTING
      Current State = STATE_RECD_INVITE
*Jul  2 13:16:30.127: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_RECD_INVITE Next
 State = STATE_SENT_ALERTING Current Substate = STATE_RECD_INVITE Next Substate =
STATE_SENT_ALERTING
```

```
*Jul  2 13:16:30.128: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PEER_CAPS,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_MULTIMEDIA_CHANNEL_ACK,     Current State =
S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT,        Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_PEER_CHNL_ACK, Current State = S_IPIP_MEDIA_SERV_STATE_IDLE,
Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.139: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_CONNECT,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.139:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_CC_CALL_CONNECT
      Current State = STATE_SENT_ALERTING
*Jul  2 13:16:30.139: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_INVITE_RESP_SDP_SENT,
  Current State = S_SIP_EARLY_DIALOG_OFFER_RCVD,      Next State =
S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE
*Jul  2 13:16:30.139: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SENT_SDP,
Current State = S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT,       Next State = S_SIP_IWF_SDP_DONE
*Jul  2 13:16:30.141: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_SENT_ALERTING
Next State = STATE_SENT_SUCCESS Current Substate = STATE_SENT_ALERTING Next Substate =
STATE_SENT_SUCCESS
*Jul  2 13:16:30.146:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
Current State = STATE_SENT_SUCCESS
*Jul  2 13:16:30.146: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_SENT_SUCCESS
Next State = STATE_ACTIVE Current Substate = STATE_SENT_SUCCESS Next Substate = STATE_ACTIVE
*Jul  2 13:16:30.146: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_DIALOG_ESTD,
Current State = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE,   Next State = S_SIP_MID_DIALOG_IDLE
*Jul  2 13:16:30.146: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_ACTIVE,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.147: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_CALL_ACTIVE,   Current State = CNFSM_CONTAINER_STATE,      Next State
 = CNFSM_NO_STATE_CHANGE
--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
--------------------------------
*Jul  2 13:16:30.121: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_NONE Next State
 = STATE_IDLE Current Substate = STATE_NONE Next Substate = STATE_IDLE
*Jul  2 13:16:30.121: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SET_MODE,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.121: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PRE_SETUP,
Current State = S_SIP_IWF_SDP_IDLE, Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.122: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_MULTIMEDIA_CHANNEL_IND,     Current State = S_SIP_IWF_SDP_IDLE,
Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.122: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_PEER_CHNL_IND, Current State = S_IPIP_MEDIA_SERV_STATE_IDLE,
Next State = S_IPIP_MEDIA_SERV_STATE_INIT_XCODER_RESERVED
*Jul  2 13:16:30.122: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CONTINUE_PRE_SETUP,
      Current State = S_SIP_IWF_SDP_IDLE,         Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,   Current State = CNFSM_CONTAINER_STATE,
Next State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:16:30.123: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_INIT_CALL_SETUP,
Current State = S_SIP_IWF_SDP_IDLE, Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_CC_CALL_SETUP
      Current State = STATE_IDLE
*Jul  2 13:16:30.124: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_INVITE_SDP_SENT,
     Current State = S_SIP_EARLY_DIALOG_IDLE,    Next State = S_SIP_EARLY_DIALOG_OFFER_SENT
*Jul  2 13:16:30.124: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SENT_SDP,
```

```
Current State = S_SIP_IWF_SDP_IDLE, Next State = S_SIP_IWF_SDP_SENT_AWAIT_SDP
*Jul  2 13:16:30.125: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_IDLE Next State
 = STATE_SENT_INVITE Current Substate = STATE_IDLE Next Substate = STATE_SENT_INVITE
*Jul  2 13:16:30.127:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
Current State = STATE_SENT_INVITE
*Jul  2 13:16:30.127: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_SENT_INVITE Next
 State = STATE_RECD_PROCEEDING Current Substate = STATE_SENT_INVITE Next Substate =
STATE_RECD_PROCEEDING
*Jul  2 13:16:30.128:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
Current State = STATE_RECD_PROCEEDING
*Jul  2 13:16:30.128: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_INVITE_RESP_SDP_RCVD,
  Current State = S_SIP_EARLY_DIALOG_OFFER_SENT,      Next State =
S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE
*Jul  2 13:16:30.128: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_RCVD_SDP,
Current State = S_SIP_IWF_SDP_SENT_AWAIT_SDP,       Next State = S_SIP_IWF_SDP_DONE
*Jul  2 13:16:30.129: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_RECD_PROCEEDING
 Next State = STATE_RECD_PROCEEDING Current Substate = STATE_RECD_PROCEEDING Next Substate
 = STATE_RECD_PROCEEDING
*Jul  2 13:16:30.129: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_RECD_PROCEEDING
 Next State = SIP_STATE_RECD_SUCCESS Current Substate = STATE_RECD_PROCEEDING Next Substate
 = SIP_STATE_RECD_SUCCESS
*Jul  2 13:16:30.129: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_DIALOG_ESTD,
Current State = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE,   Next State = S_SIP_MID_DIALOG_IDLE
*Jul  2 13:16:30.129: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_ACTIVE,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.129: FSM TYPE = SIP STATE TRANS FSM Current State = SIP_STATE_RECD_SUCCESS
 Next State = STATE_ACTIVE Current Substate = SIP_STATE_RECD_SUCCESS Next Substate =
STATE_ACTIVE
*Jul  2 13:16:30.129: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_UPDATE_STREAM_CONTEXT,
   Current State = S_SIP_IWF_SDP_DONE,         Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PEER_CAPS_ACK,,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PEER_CAPS_ACK,,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_CALL_ACTIVE,   Current State = CNFSM_CONTAINER_STATE,      Next State
 = CNFSM_NO_STATE_CHANGE
```

The following example shows how to display information about all API event traces:

```
Device# show monitor event-trace voip ccsip api all
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4
--------------------------------
*Jul  2 13:16:30.119: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:16:30.119: API Name = voip_rtp_allocate_port Port = 16384
*Jul  2 13:16:30.120: API Name = cc_api_call_setup_ind_with_callID Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.130: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.132: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.132: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.132: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.132: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.132: API Name = ccsip_bridge Ret_code= 0
```

```
--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
--------------------------------
*Jul  2 13:16:30.122: API Name = voip_rtp_allocate_port Port = 16386
*Jul  2 13:16:30.122: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.122: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.124: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:16:30.124: API Name = cc_api_call_proceeding Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.128: API Name = cc_api_call_alert Ret_code= 0
*Jul  2 13:16:30.128: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_caps_ind Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_call_connected Ret_code= 0
*Jul  2 13:16:30.129: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.131: API Name = ccsip_bridge Ret_code= 0
--------Cover buff----------
        buffer-id = 3   ccCallId = 3    PeerCallId = 4
        Called-Number = 44444   Calling-Number = 33333  Sip-Call-Id = 1-5682@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4
--------------------------------
*Jul  2 13:21:40.322: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:21:40.322: API Name = voip_rtp_allocate_port Port = 16388
*Jul  2 13:21:40.322: API Name = cc_api_call_setup_ind_with_callID Ret_code= 0
*Jul  2 13:21:40.324: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:21:40.324: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:21:40.324: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.330: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:21:40.331: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.333: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:21:40.334: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.334: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:21:40.332: API Name = ccsip_bridge Ret_code= 0
--------Cover buff----------
        buffer-id = 4   ccCallId = 4    PeerCallId = 3
        Called-Number = 44444   Calling-Number = 33333  Sip-Call-Id =
2A3AEE9D-FFFFFFFFE25111E2-FFFFFFFF800F8694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
--------------------------------
*Jul  2 13:21:40.324: API Name = voip_rtp_allocate_port Port = 16390
*Jul  2 13:21:40.326: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:21:40.326: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:21:40.326: API Name = voip_rtp_update_callinfo Ret_code= 0
```

```
*Jul  2 13:21:40.327: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:21:40.327: API Name = cc_api_call_proceeding Ret_code= 0
*Jul  2 13:21:40.328: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.327: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:21:40.327: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.329: API Name = cc_api_call_alert Ret_code= 0
*Jul  2 13:21:40.330: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:21:40.331: API Name = cc_api_caps_ind Ret_code= 0
*Jul  2 13:21:40.331: API Name = cc_api_call_connected Ret_code= 0
*Jul  2 13:21:40.331: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.333: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:21:40.333: API Name = ccsip_bridge Ret_code= 0
```

In the following example, there are two active calls on Cisco UBE. In the first call, the calling number is 1111 and it calls the number 22222. In the second call, the calling number is 33333 and it calls number 44444. The example shows how to filter the API event traces where the calling number is 11111:

```
Device# show monitor event-trace voip ccsip api filter calling-num 11111 all
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4
--------------------------------
*Jul  2 13:16:30.119: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:16:30.119: API Name = voip_rtp_allocate_port Port = 16384
*Jul  2 13:16:30.120: API Name = cc_api_call_setup_ind_with_callID Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.130: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.131: API Name = ccsip_bridge Ret_code= 0
--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
--------------------------------
*Jul  2 13:16:30.123: API Name = voip_rtp_allocate_port Port = 16386
*Jul  2 13:16:30.124: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.124: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.124: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.124: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:16:30.124: API Name = cc_api_call_proceeding Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_update_callinfo Ret_code= 0
```

```
*Jul  2 13:16:30.128: API Name = cc_api_call_alert Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.130: API Name = cc_api_caps_ind Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_call_connected Ret_code= 0
*Jul  2 13:16:30.129: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.131: API Name = ccsip_bridge Ret_code= 0
```

The following example shows how to display the traces captured for completed calls. The call could be a successful one or a failed one. The output displays all the traces (fsm, msg, misc, api) that were enabled at the time of call, arranged according to time stamp:

```
Device# show monitor event-trace voip ccsip history all
--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 9
sip_fsm: Enabled.. Total Traces logged = 31
sip_apis: Enabled.. Total Traces logged = 25
sip_misc: Enabled.. Total Traces logged = 3
--------------------------------
*Jul  2 13:16:30.122: sip_misc: Outbound dial-peer matched : tag = 22222
*Jul  2 13:16:30.122: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_NONE
Next State = STATE_IDLE Current Substate = STATE_NONE Next Substate = STATE_IDLE
*Jul  2 13:16:30.122: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SET_MODE,
      Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.122: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PRE_SETUP,
      Current State = S_SIP_IWF_SDP_IDLE,         Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_MULTIMEDIA_CHANNEL_IND,    Current State = S_SIP_IWF_SDP_IDLE,
Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123: sip_misc: Media Stream Index = 1, Media Stream Type = voice-only
Stream State = STREAM_ADDING
        Negotiated Codec = No Codec    Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.122: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_PEER_CHNL_IND,        Current State = S_IPIP_MEDIA_SERV_STATE_IDLE,
     Next State = S_IPIP_MEDIA_SERV_STATE_INIT_XCODER_RESERVED
*Jul  2 13:16:30.122: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_CONTINUE_PRE_SETUP,     Current State = S_SIP_IWF_SDP_IDLE,        Next State
 = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,  Current State = CNFSM_CONTAINER_STATE,     Next
 State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:16:30.124: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_INIT_CALL_SETUP,        Current State = S_SIP_IWF_SDP_IDLE,        Next State
 = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.124: sip_apis: API Name = voip_rtp_allocate_port Port = 16386
*Jul  2 13:16:30.124: sip_apis: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.124: sip_apis: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.124: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.124: sip_apis: API Name = cc_api_update_interface_cac_resource Ret_code=
0
*Jul  2 13:16:30.124: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_SETUP         Current State = STATE_IDLE
*Jul  2 13:16:30.124: sip_apis: API Name = cc_api_call_proceeding Ret_code= 0
*Jul  2 13:16:30.125: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event =
E_SIP_INVITE_SDP_SENT,      Current State = S_SIP_EARLY_DIALOG_IDLE,    Next State =
S_SIP_EARLY_DIALOG_OFFER_SENT
*Jul  2 13:16:30.125: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SENT_SDP,
```

```
     Current State = S_SIP_IWF_SDP_IDLE,        Next State = S_SIP_IWF_SDP_SENT_AWAIT_SDP
*Jul  2 13:16:30.126: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_IDLE
Next State = STATE_SENT_INVITE Current Substate = STATE_IDLE Next Substate = STATE_SENT_INVITE
*Jul  2 13:16:30.125: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.125: sip_apis: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.125: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.125: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 3, Last Fragment
 = No, Messages Direction = Sent, Message:
INVITE sip:22222@9.40.1.22:9632 SIP/2.0
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK07AC
Remote-Party-ID: "11111 " <sip:11111@9.40.1.30>;party=calling;screen=no;privacy=off
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507
To: <sip:22222@9.40.1.22>
Date: Tue, 02 Jul 2013 13:16:30 GMT
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE:  1800
Cisco-Guid: 1901362665-3796898274-2147649172-0547562766
--------

*Jul  2 13:16:30.126: sip_msgs: SIP_MSG: Fragment Number = 2,  Message Id = 3, Last Fragment
 = No, Messages Direction = Sent, Message:

User-Agent: Cisco-SIPGateway/IOS-15.3.20130514.122658.
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO,
REGISTER
CSeq: 101 INVITE
Timestamp: 1372770990
Contact: <sip:11111@9.40.1.30:5060>
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 69
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 206

v=0
o=CiscoSystemsSIP-GW-UserAgent 5243 1933 IN IP4 9.40.1.30
s=SIP Call
c=IN IP4 9.40.1.30
t=0
--------

*Jul  2 13:16:30.126: sip_msgs: SIP_MSG: Fragment Number = 3,  Message Id = 3, Last Fragment
 = Yes, Messages Direction = Sent, Message:
0
m=audio 16386 RTP/AVP 0 19
c=IN IP4 9.40.1.30
a=rtpmap:0 PCMU/8000
a=rtpmap:19 CN/8000
a=ptime:20

--------

*Jul  2 13:16:30.126: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 4, Last Fragment
 = Yes, Messages Direction = received, Message:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK07AC
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507
To: <sip:22222@9.40.1.22>;tag=4
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
CSeq: 101 INVITE
Contact: <sip:9.40.1.22:9632;transport=UDP>
Content-Length: 0
```

```
--------

*Jul  2 13:16:30.127: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
           Current State = STATE_SENT_INVITE
*Jul  2 13:16:30.127: sip_apis: API Name = cc_api_call_alert Ret_code= 0
*Jul  2 13:16:30.128: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_SENT_INVITE Next State = STATE_RECD_PROCEEDING Current Substate = STATE_SENT_INVITE
Next Substate = STATE_RECD_PROCEEDING
*Jul  2 13:16:30.128: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 6, Last Fragment
 = No, Messages Direction = received, Message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK07AC
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507
To: <sip:22222@9.40.1.22>;tag=4
Call-ID: 7155B639-FFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
CSeq: 101 INVITE
Contact: <sip:9.40.1.22:9632;transport=UDP>
Content-Type: application/sdp
Content-Length:   199

v=0

o=user1 53655765 2353687637 IN IP4 9.40.1.22
s=-
c=IN IP4 9.40.1.22
t=0 0
m=audio 9832 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephon
--------

*Jul  2 13:16:30.128: sip_msgs: SIP_MSG: Fragment Number = 2,  Message Id = 6, Last Fragment
 = Yes, Messages Direction = received, Message:
e-event/8000
a=fmtp:101 0-16
a=ptime:20


--------

*Jul  2 13:16:30.129: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
           Current State = STATE_RECD_PROCEEDING
*Jul  2 13:16:30.129: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event =
E_SIP_INVITE_RESP_SDP_RCVD, Current State = S_SIP_EARLY_DIALOG_OFFER_SENT,      Next State
 = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE
*Jul  2 13:16:30.129: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_RCVD_SDP,
      Current State = S_SIP_IWF_SDP_SENT_AWAIT_SDP,       Next State = S_SIP_IWF_SDP_DONE
*Jul  2 13:16:30.128: sip_misc: Media Stream Index = 1, Media Stream Type = voice-only
Stream State = STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.128: sip_apis: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.129: sip_apis: API Name = cc_api_caps_ind Ret_code= 0
*Jul  2 13:16:30.129: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_RECD_PROCEEDING Next State = STATE_RECD_PROCEEDING Current Substate =
STATE_RECD_PROCEEDING Next Substate = STATE_RECD_PROCEEDING
*Jul  2 13:16:30.130: sip_apis: API Name = cc_api_call_connected Ret_code= 0
*Jul  2 13:16:30.130: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_RECD_PROCEEDING Next State = SIP_STATE_RECD_SUCCESS Current Substate =
STATE_RECD_PROCEEDING Next Substate = SIP_STATE_RECD_SUCCESS
*Jul  2 13:16:30.130: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_DIALOG_ESTD,
  Current State = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE,   Next State =
```

```
S_SIP_MID_DIALOG_IDLE
*Jul  2 13:16:30.130: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_ACTIVE,
    Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
SIP_STATE_RECD_SUCCESS Next State = STATE_ACTIVE Current Substate = SIP_STATE_RECD_SUCCESS
 Next Substate = STATE_ACTIVE
*Jul  2 13:16:30.129: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_UPDATE_STREAM_CONTEXT,  Current State = S_SIP_IWF_SDP_DONE,        Next State
 = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.129: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.130: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_CAPS_ACK,, Current State = CNFSM_CONTAINER_STATE,      Next State =
CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_CAPS_ACK,, Current State = CNFSM_CONTAINER_STATE,      Next State =
CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.131: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_CALL_ACTIVE,  Current State = CNFSM_CONTAINER_STATE,      Next State
= CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.131: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 7, Last Fragment
 = Yes, Messages Direction = Sent, Message:
ACK sip:9.40.1.22:9632;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK113B1
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507
To: <sip:22222@9.40.1.22>;tag=4
Date: Tue, 02 Jul 2013 13:16:30 GMT
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
Max-Forwards: 70
CSeq: 101 ACK

Allow-Events: telephone-event
Content-Length: 0


--------

*Jul  2 13:16:30.132: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.132: sip_apis: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.132: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.132: sip_apis: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.132: sip_apis: API Name = ccsip_bridge Ret_code= 0
*Jul  2 13:32:52.831: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,  Current State = CNFSM_CONTAINER_STATE,      Next
 State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:32:52.831: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:32:52.832: sip_apis: API Name = cc_api_bridge_drop_done Ret_code= 0
*Jul  2 13:32:52.833: sip_apis: API Name = cc_api_update_interface_cac_resource Ret_code=
0
*Jul  2 13:32:52.833: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_DISCONNECT    Current State = STATE_ACTIVE
*Jul  2 13:32:52.833: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_ACTIVE
 Next State = STATE_DISCONNECTING Current Substate = STATE_ACTIVE Next Substate =
STATE_DISCONNECTING
*Jul  2 13:32:52.831: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 21, Last Fragment
 = Yes, Messages Direction = Sent, Message:
BYE sip:9.40.1.22:9632;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK4326
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507
To: <sip:22222@9.40.1.22>;tag=4
Date: Tue, 02 Jul 2013 13:16:30 GMT
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
User-Agent: Cisco-SIPGateway/IOS-15.3.20130514.122658.
Max-Forwards: 70
Timestamp: 1372771972
```

```
CSeq: 102 BYE
Reason: Q.850;cause=16
Content-Length: 0


--------

*Jul  2 13:32:52.839: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 22, Last Fragment
 = Yes, Messages Direction = received, Message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK4326
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507

To: <sip:22222@9.40.1.22>;tag=4;tag=4
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
CSeq: 102 BYE
Contact: <sip:9.40.1.22:9632;transport=UDP>


--------

*Jul  2 13:32:52.838: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
           Current State = STATE_DISCONNECTING
*Jul  2 13:32:52.838: sip_apis: API Name = voip_rtp_delete_dp_session Ret_code= 0
*Jul  2 13:32:52.851: sip_apis: API Name = ccsip_voip_rtp_fpi_event_handler Ret_code= 0
*Jul  2 13:32:52.851: sip_apis: API Name = cc_api_call_disconnect_done Ret_code= 0
*Jul  2 13:32:52.851: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_DISCONNECTING Next State = STATE_DEAD Current Substate = STATE_DISCONNECTING Next
Substate = STATE_DEAD
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 10
sip_fsm: Enabled.. Total Traces logged = 28
sip_apis: Enabled.. Total Traces logged = 23
sip_misc: Enabled.. Total Traces logged = 4
--------------------------------
*Jul  2 13:16:30.117: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 1, Last Fragment
 = No, Messages Direction = received, Message:
INVITE sip:22222@9.40.1.30:5060 SIP/2.0
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1-0
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>
Call-ID: 1-5671@9.40.1.22
CSeq: 1 INVITE
Contact: <sip:11111@9.40.1.22:9232>
Max-Forwards: 70
Subject: Call Spike Testing
Content-Length:  182
Content-Type: application/sdp

v=0
o=- 53655765 2353687637 IN IP4 9.40.1.22
s=-
c=IN IP4 9.40.1.22

t=0 0
m=audio 9432 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpm
--------

*Jul  2 13:16:30.115: sip_msgs: SIP_MSG: Fragment Number = 2,  Message Id = 1, Last Fragment
 = Yes, Messages Direction = received, Message:
```

```
ap: 101 telephone-event/8000
a=fmtp:101 0-16

--------

*Jul  2 13:16:30.115: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_NONE
Next State = STATE_IDLE Current Substate = STATE_NONE Next Substate = STATE_IDLE
*Jul  2 13:16:30.118: sip_misc: Inbound dial-peer matched : tag = 11111
*Jul  2 13:16:30.119: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event =
E_SIP_INVITE_SDP_RCVD,      Current State = S_SIP_EARLY_DIALOG_IDLE,    Next State =
S_SIP_EARLY_DIALOG_OFFER_RCVD
*Jul  2 13:16:30.119: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_RCVD_SDP,
      Current State = S_SIP_IWF_SDP_IDLE,         Next State =
S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT
*Jul  2 13:16:30.119: sip_misc: Media Stream Index = 1, Media Stream Type = voice-only
Stream State = STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.119: sip_apis: API Name = cc_api_update_interface_cac_resource Ret_code=
0
*Jul  2 13:16:30.119: sip_apis: API Name = voip_rtp_allocate_port Port = 16384
*Jul  2 13:16:30.120: sip_misc: Media Stream Index = 1, Media Stream Type = voice-only
Stream State = STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.119: sip_apis: API Name = cc_api_call_setup_ind_with_callID Ret_code= 0
*Jul  2 13:16:30.119: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_IDLE
Next State = STATE_RECD_INVITE Current Substate = STATE_IDLE Next Substate = STATE_RECD_INVITE
*Jul  2 13:16:30.121: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SET_MODE,
      Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123: sip_apis: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.123: sip_apis: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.123: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.123: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_PROCEEDING    Current State = STATE_RECD_INVITE
*Jul  2 13:16:30.123: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,  Current State = CNFSM_CONTAINER_STATE,      Next
 State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:16:30.126: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 2, Last Fragment
 = Yes, Messages Direction = Sent, Message:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1-0
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>
Date: Tue, 02 Jul 2013 13:16:30 GMT
Call-ID: 1-5671@9.40.1.22
CSeq: 1 INVITE
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-15.3.20130514.122658.
Content-Length: 0


--------

*Jul  2 13:16:30.127: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_ALERTING      Current State = STATE_RECD_INVITE
*Jul  2 13:16:30.127: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_RECD_INVITE Next State = STATE_SENT_ALERTING Current Substate = STATE_RECD_INVITE
Next Substate = STATE_SENT_ALERTING
*Jul  2 13:16:30.128: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 5, Last Fragment
 = No, Messages Direction = Sent, Message:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1-0
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>;tag=38C97-1057
Date: Tue, 02 Jul 2013 13:16:30 GMT
```

```
Call-ID: 1-5671@9.40.1.22
CSeq: 1 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO,
REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:22222@9.40.1.30>;party=called;screen=no;privacy=off
Contact: <sip:22222@9.40.1.30:5060>

--------

*Jul  2 13:16:30.128: sip_msgs: SIP_MSG: Fragment Number = 2,  Message Id = 5, Last Fragment
 = Yes, Messages Direction = Sent, Message:
Server: Cisco-SIPGateway/IOS-15.3.20130514.122658.
Content-Length: 0


--------

*Jul  2 13:16:30.129: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PEER_CAPS,
      Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.129: sip_apis: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.130: sip_apis: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.131: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_MULTIMEDIA_CHANNEL_ACK,    Current State =
S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT,        Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.131: sip_misc: Media Stream Index = 1, Media Stream Type = voice-only
Stream State = STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.131: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: sip_apis: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.131: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_PEER_CHNL_ACK,        Current State = S_IPIP_MEDIA_SERV_STATE_IDLE,
     Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.132: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: sip_apis: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.131: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: sip_apis: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.131: sip_apis: API Name = ccsip_bridge Ret_code= 0
*Jul  2 13:16:30.139: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_CONNECT,
   Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.140: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_CONNECT       Current State = STATE_SENT_ALERTING
*Jul  2 13:16:30.140: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event =
E_SIP_INVITE_RESP_SDP_SENT, Current State = S_SIP_EARLY_DIALOG_OFFER_RCVD,      Next State
 = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE
*Jul  2 13:16:30.140: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SENT_SDP,
      Current State = S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT,        Next State =
S_SIP_IWF_SDP_DONE
*Jul  2 13:16:30.141: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_SENT_ALERTING Next State = STATE_SENT_SUCCESS Current Substate = STATE_SENT_ALERTING
 Next Substate = STATE_SENT_SUCCESS
*Jul  2 13:16:30.141: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 8, Last Fragment
 = No, Messages Direction = Sent, Message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1-0
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>;tag=38C97-1057
Date: Tue, 02 Jul 2013 13:16:30 GMT
Call-ID: 1-5671@9.40.1.22
CSeq: 1 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO,
REGISTER
Allow-Events: telephone-event
```

```
Remote-Party-ID: <sip:22222@9.40.1.30>;party=called;screen=no;privacy=off
Contact: <sip:22222@9.40.1.30:5060>
Suppo
--------

*Jul  2 13:16:30.142: sip_msgs: SIP_MSG: Fragment Number = 2,  Message Id = 8, Last Fragment
 = Yes, Messages Direction = Sent, Message:
rted: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.3.20130514.122658.
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 182

v=0
o=CiscoSystemsSIP-GW-UserAgent 8289 9144 IN IP4 9.40.1.30
s=SIP Call
c=IN IP4 9.40.1.30
t=0 0
m=audio 16384 RTP/AVP 0
c=IN IP4 9.40.1.30

a=rtpmap:0 PCMU/8000
a=ptime:20

--------

*Jul  2 13:16:30.146: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 9, Last Fragment
 = Yes, Messages Direction = received, Message:
ACK sip:22222@9.40.1.30:5060 SIP/2.0
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1-4
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>;tag=38C97-1057
Call-ID: 1-5671@9.40.1.22
CSeq: 1 ACK
Contact: sip:11111@9.40.1.22:9232
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp


--------

*Jul  2 13:16:30.146: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
           Current State = STATE_SENT_SUCCESS
*Jul  2 13:16:30.146: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_SENT_SUCCESS Next State = STATE_ACTIVE Current Substate = STATE_SENT_SUCCESS Next
Substate = STATE_ACTIVE
*Jul  2 13:16:30.146: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_DIALOG_ESTD,
  Current State = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE,   Next State =
S_SIP_MID_DIALOG_IDLE
*Jul  2 13:16:30.147: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_ACTIVE,
    Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.148: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_CALL_ACTIVE,  Current State = CNFSM_CONTAINER_STATE,      Next State
= CNFSM_NO_STATE_CHANGE
*Jul  2 13:32:52.829: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 19, Last Fragment
 = Yes, Messages Direction = received, Message:
BYE sip:22222@9.40.1.30:5060 SIP/2.0
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1--1
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>;tag=38C97-1057
Call-ID: 1-5671@9.40.1.22
```

```
CSeq: 2 BYE
Max-Forwards: 70
Contact: <sip:9.40.1.22:9232;transport=UDP>
Content-Length: 0
--------

*Jul  2 13:32:52.829: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
           Current State = STATE_ACTIVE
*Jul  2 13:32:52.830: sip_apis: API Name = cc_api_call_disconnected Ret_code= 0
*Jul  2 13:32:52.830: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_ACTIVE
 Next State = STATE_DISCONNECTING Current Substate = STATE_ACTIVE Next Substate =
STATE_DISCONNECTING
*Jul  2 13:32:52.830: sip_apis: API Name = voip_rtp_destroy_dp_session Ret_code= 0
*Jul  2 13:32:52.830: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,  Current State = CNFSM_CONTAINER_STATE,      Next
 State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:32:52.831: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:32:52.831: sip_apis: API Name = cc_api_bridge_drop_done Ret_code= 0
*Jul  2 13:32:52.831: sip_apis: API Name = cc_api_update_interface_cac_resource Ret_code=
0
*Jul  2 13:32:52.831: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_DISCONNECT    Current State = STATE_DISCONNECTING
*Jul  2 13:32:52.832: sip_apis: API Name = voip_rtp_delete_dp_session Ret_code= 0
*Jul  2 13:32:52.831: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 20, Last Fragment
 = Yes, Messages Direction = Sent, Message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1--1
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>;tag=38C97-1057
Date: Tue, 02 Jul 2013 13:32:52 GMT
Call-ID: 1-5671@9.40.1.22
Server: Cisco-SIPGateway/IOS-15.3.20130514.122658.
CSeq: 2 BYE
Reason: Q.850;cause=16
Content-Length: 0

--------

*Jul  2 13:32:52.851: sip_apis: API Name = ccsip_voip_rtp_fpi_event_handler Ret_code= 0
*Jul  2 13:32:52.851: sip_apis: API Name = cc_api_call_disconnect_done Ret_code= 0
*Jul  2 13:32:52.851: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_DISCONNECTING Next State = STATE_DEAD Current Substate = STATE_DISCONNECTING Next
Substate = STATE_DEAD
*Jul  2 13:33:24.851: sip_fsm:  FSM TYPE = SIP Timer-STate FSM, Event =
SIP_TIMER_REMOVE_TRANSACTION    Current State = STATE_DEAD
```

The following table describes the significant fields shown in the display.

Table 1: Command Field Name Descriptions

Field Name	Description
Called-Number	The destination number.
Calling-Number	The number that originated the call.
Sip-Call-Id	The SIP call ID.
Total Traces logged	The total number of traces logged for the specified message type.
buffer-id	The buffer ID uniquely identifies the buffer in which the traces are stored.

Field Name	Description
ccCallId	The call-id of the leg whose traces are displayed.
PeerCallId	The remote party call-id

show mrcp client session active

To display information about active Media Resource Control Protocol (MRCP) client sessions, use the **show mrcp client session active**command in privileged EXEC mode.

show mrcp client session active [**detailed**]

Syntax Description

detailed	(Optional) Displays detailed information about each active MRCP session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	The MRCP version, ASR callid, and TTS callid fields were added to the command output and the URL and Stream URL fields were modified to display Media Resource Control Protocol version 2 (MRCP v2) format URLs.

Usage Guidelines

Use this command to display information about all active MRCP sessions for the gateway. Use the **detailed** keyword to display additional information about the sessions.

Examples

The following is sample output from this command:

```
Router# show mrcp client session active
No Of Active MRCP Sessions:1
          Call-ID:0x1A
     Resource Type:Synthesizer        URL:rtsp://server-asr/synthesizer
Method In Progress:SPEAK      State:SPEAKING
     Resource Type:Recognizer         URL:rtsp://server-asr/recognizer
Method In Progress:RECOGNIZE      State:RECOGNIZING
```

The following is sample output when the **detailed** keyword is used:

```
Router# show mrcp client session active detailed
No Of Active MRCP Sessions: 1
           Call-ID: 0x14 same: 0
--------------------------------------------
     Resource Type: Synthesizer            URL: sip:mrcpv2TTSServer@10.5.18.224
Method In Progress: SPEAK                State: S_SYNTH_IDLE
Associated CallID: 0x17
     MRCP version: 2.0
 Control Protocol: TCP Server IP Address: 10.5.18.224    Port: 51000
    Data Protocol: RTP Server IP Address: 10.5.18.224    Port: 10000
Stream URL: sip:mrcpv2TTSServer@10.5.18.224:5060
Packets Transmitted: 0 (0 bytes)
Packets Received: 177 (28320 bytes)
ReceiveDelay: 100     LostPackets: 0
--------------------------------------------
--------------------------------------------
```

```
     Resource Type: Recognizer              URL: sip:mrcpv2ASRServer@10.5.18.224
Method In Progress: RECOGNITION-START-TIMERS             State: S_RECOG_RECOGNIZING
Associated CallID: 0x18
     MRCP version: 2.0
 Control Protocol: TCP Server IP Address: 10.5.18.224     Port: 51001
    Data Protocol: RTP Server IP Address: 10.5.18.224     Port: 10002
Packets Transmitted: 191 (30560 bytes)
Packets Received: 0 (0 bytes)
ReceiveDelay: 100     LostPackets: 0
```

The table below describes the fields shown in this output.

Table 2: show mrcp client session active detailed Field Descriptions

Field	Description
No. Of Active MRCP Sessions	Number of MRCP sessions that are currently active between the gateway and the media server.
Call-ID	Unique identification number for the call, in hexadecimal.
Resource Type	Whether the media server being used is a speech synthesizer (TTS) or a speech recognizer (ASR).
URL	URL of the media server.
Method In Progress	Type of event that was initiated between the gateway and the media server. Values are defined by the MRCP informational RFC. For speech synthesis, values are IDLE, SPEAK, SET-PARAMS, GET-PARAMS, STOP, or BARGE-IN-OCCURRED. For speech recognition, values are DEFINE-GRAMMAR, RECOGNIZE, SET-PARAMS, GET-PARAMS, STOP, GET-RESULT, or RECOGNITION-START-TIMERS.
State	Current state of the method in progress. Values are defined by the MRCP informational RFC. For speech synthesis, values are SYNTH_IDLE, SPEAKING, SYNTH_ASSOCIATING, PAUSED, or SYNTH_ERROR_STATE. For speech recognition, values are RECOG_IDLE, RECOG_ASSOCIATING, RECOGNIZING, RECOGNIZED, or RECOG_ERROR_STATE.
Associated CallID	Unique identification number for the associated MRCP session, in hexadecimal.
MRCP version	MRCP version used by the client.
Control Protocol	Call control protocol being used, which is always TCP.
Data Protocol	Data protocol being used, which is always RTP.
Local IP Address	IP address of the Cisco gateway that is the MRCP client. This field is not displayed for MRCP v2 sessions because the local IP address is not specified in SIP call legs.
Local Port	Identification number of the Cisco gateway port through which the TCP connection is made. This field is not displayed for MRCP v2 sessions because the local port is not specified in SIP call legs.

Field	Description
Server IP Address	IP address of the media server that is the MRCP server.
Server Port	Identification number of the MRCP server port through which the TCP connection is made.
Signalling URL	URL of the MRCP v2 media server.
Stream URL	URL of the MRCP v1 media server.
Packets Transmitted	Total number of packets that have been transmitted from the client to the ASR server.
Packets Received	Total number of packets that have been received by the client from the TTS server.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call.

Related Commands

Command	Description
debug mrcp	Displays debug messages for MRCP operations.
show mrcp client session history	Displays information about past MRCP client sessions that are stored on the gateway.
show mrcp client statistics hostname	Displays statistics about MRCP sessions.

show mrcp client session history

To display information about past Media Resource Control Protocol (MRCP) client sessions that are stored on the gateway, use the **show mrcp client session history**command in privileged EXEC mode.

show mrcp client session history [**detailed**]

Syntax Description

detailed	(Optional) Displays detailed information about each MRCP session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	The MRCP version field was added to the command output and the URL field was modified to display Media Resource Control Protocol version 2 (MRCP v2) format URLs.

Usage Guidelines

The maximum number of inactive MRCP sessions that are stored in history is configured by using the **mrcp client session history records** command. If the **mrcp client session history records** command is not used, the maximum number of history records that are saved is 50.

MRCP history records are stored for the length of time that is specified by the **mrcp client session history duration** command. If the **mrcp client session history duration** command is not configured, MRCP history records are stored for a maximum of 3600 seconds (1 hour).

Examples

The following is sample output from this command:

```
Router# show mrcp client session history
MRCP Session ID:0x9
Associated CallID:0x1A
Control Protocol:TCP     Data Protocol:RTP
Local  IP Address:10.1.2.230     Local  Port 17120
Server IP Address:10.1.2.58     Server Port 4858
Stream URL:rtsp://server-asr:554
Packets Transmitted:423 (101520 bytes)
Packets Received:819 (131040 bytes)
MRCP Session ID:0x8
Associated CallID:0x16
Control Protocol:TCP     Data Protocol:RTP
Local  IP Address:10.1.2.230     Local  Port 16948
Server IP Address:10.1.2.58     Server Port 4850
Stream URL:rtsp://server-asr:554
Packets Transmitted:284 (68160 bytes)
Packets Received:598 (95680 bytes)
MRCP Session ID:0x7
Associated CallID:0x12
Control Protocol:TCP     Data Protocol:RTP
Local  IP Address:10.1.2.230     Local  Port 16686
Server IP Address:10.1.2.58     Server Port 4842
Stream URL:rtsp://server-asr:554
```

```
Packets Transmitted:353 (84720 bytes)
Packets Received:716 (114560 bytes)
MRCP Session ID:0x6
Associated CallID:0xE
Control Protocol:TCP     Data Protocol:RTP
Local  IP Address:10.1.2.230     Local  Port 19398
Server IP Address:10.1.2.58     Server Port 4834
Stream URL:rtsp://server-asr:554
Packets Transmitted:358 (85920 bytes)
Packets Received:720 (115200 bytes)
```

The following is sample output from the show mrcp client session history detailed command:

```
Router# show mrcp client session history detailed
MRCP Session ID: 0x7
Associated CallID: 0x14
     MRCP version: 2.0
     =================
     Control Protocol: TCP    Data Protocol: RTP
     ASR (Callid = 0x18)
Server IP Address: 10.5.18.224     Server Port 10002
Signalling URL: sip:mrcpv2ASRServer@10.5.18.224:5060
Packets Transmitted: 373 (59680 bytes)
Packets Received: 0 (0 bytes)
OntimeRcvPlayout: 3000
GapFillWithSilence: 0
GapFillWithPrediction: 0
GapFillWithInterpolation: 6025
GapFillWithRedundancy: 0
HighWaterPlayoutDelay: 100
LoWaterPlayoutDelay: 95
ReceiveDelay: 100     LostPackets: 0
EarlyPackets: 0     LatePackets: 0
-----------------------------------------
     TTS (Callid = 0x17)
Server IP Address: 10.5.18.224     Server Port 10000
Signalling URL: sip:mrcpv2TTSServer@10.5.18.224:5060
Packets Transmitted: 0 (0 bytes)
Packets Received: 679 (108640 bytes)
OntimeRcvPlayout: 3000
GapFillWithSilence: 0
GapFillWithPrediction: 0
GapFillWithInterpolation: 6025
GapFillWithRedundancy: 0
HighWaterPlayoutDelay: 100
LoWaterPlayoutDelay: 95
ReceiveDelay: 100     LostPackets: 0
EarlyPackets: 0     LatePackets: 0
```

The table below describes the fields shown in this output.

Table 3: show mrcp client session history detailed Field Descriptions

Field	Description
MRCP Session ID	Unique identification number for the MRCP session, in hexadecimal.
Associated CallID	Unique identification number for the associated call, in hexadecimal.
MRCP version	MRCP version used by the client.
Control Protocol	Call control protocol being used, which is always TCP.

Field	Description
Data Protocol	Data protocol being used, which is always RTP.
ASR (Callid =)	For MRCP v2 sessions, the unique identification number for the ASR SIP call leg, in hexadecimal.
TTS (Callid =)	For MRCP v2 sessions, the unique identification number for the TTS SIP call leg, in hexadecimal.
Local IP Address	IP address of the Cisco gateway that is the MRCP client. This field is not displayed for MRCP v2 sessions because the local IP address is not specified in SIP call legs.
Local Port	Identification number of the Cisco gateway port through which the TCP connection is made. This field is not displayed for MRCP v2 sessions because the local port is not specified in SIP call legs.
Server IP Address	IP address of the media server that is the MRCP server.
Server Port	Identification number of the MRCP server port through which the TCP connection is made.
Signalling URL	URL of the MRCP v2 media server.
Stream URL	URL of the MRCP v1 media server.
Packets Transmitted	Total number of packets that have been transmitted from the client to the ASR server.
Packets Received	Total number of packets that have been received by the client from the TTS server.
OntimeRcvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRcvPlayout value to the GapFill values.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GapFillWithPrediction	Duration of a voice signal played out with a signal synthesized from parameters or samples of data preceding in time because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser or frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
HighWaterPlayoutDelay	High-water mark voice playout FIFO delay during this call.

Field	Description
LoWaterPlayoutDelay	Low-water mark voice playout FIFO delay during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call.

Related Commands

Command	Description
debug mrcp	Displays debug messages for MRCP operations.
mrcp client session history duration	Sets the maximum number of seconds for which MRCP history records are stored on the gateway
mrcp client session history records	Sets the maximum number of MRCP history records that the gateway can store.
show mrcp client session active	Displays information about active MRCP client sessions.

show mrcp client statistics hostname

To display statistics about Media Resource Control Protocol (MRCP) sessions for a specific MRCP client host, use the **show mrcp client statistics hostname**command in privileged EXEC mode.

show mrcp client statistics hostname {*hostnameip-address*}

Syntax Description

hostname	Hostname of the MRCP server. Format uses host name only or hostname:port.
ip-address	IP address of the MRCP server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to display statistics about MRCP version 2 (MRCP v2) sessions.

Usage Guidelines

To display output from this command, you must first use the **mrcp client statistics enable**command.

Examples

The following is sample output from this command:

```
Router# show mrcp client statistics hostname asr-host
hostname:asr-host
Method                   :Count   Min   Avg   Max
RECOGNIZE                :3       40    562   1604
DEFINE-GRAMMAR           :3       48    568   1604
RECOGNITION-START-TIMERS :2       140   164   188
SPEAK                    :6       44    568   1596
RECOG-TIME               :3       804   965   1128
SPEAK-TIME               :6       3636  7063  12068
```

The table below describes the fields shown in this output.

Table 4: show mrcp client statistics hostname Field Descriptions

Field	Description
hostname	Host name of the media server.
Method	Type of event that was initiated between the gateway and the media server. Values as defined by the MRCP informational RFC are RECOGNIZE, DEFINE-GRAMMAR, RECOGNITION-START-TIMERS, and SPEAK. RECOG-TIME is the milliseconds that it takes the ASR server to recognize the grammar. SPEAK-TIME is the milliseconds that it takes the TTS server to speak.
Count	Total number of MRCP sessions that used this method.

Field	Description
Min	Length of the shortest session, in milliseconds.
Avg	Average length of a session, in milliseconds, based on all sessions.
Max	Length of the longest session, in milliseconds.

Related Commands

Command	Description
debug mrcp	Displays debug messages for MRCP operations.
mrcp client statistics enable	Enables MRCP client statistics to be displayed.
show mrcp client session active	Displays information about active MRCP client sessions.
show mrcp client session history	Displays information about MRCP client history records that are stored on the gateway.

show mwi relay clients

To display registration information for the list of message-waiting indicator (MWI) relay clients, use the **show mwi relay clients**command in privileged EXEC mode.

show mwi relay clients

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XT	This command was introduced on the Cisco 1750, Cisco 1751, Cisco 2600, Cisco 3600, and Cisco IAD2420.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 3725 and Cisco 3745.
12.2(8)T1	This command was implemented on the Cisco 2600-XM and Cisco 2691.
12.2(11)T	This command was implemented on the Cisco 1760.

Examples

The following is sample output from thiscommand:

```
Router# show mwi relay clients
Client              IPADDR        EXPIRES(sec)   MWI
============   ===============   ============    ====
4085550153       10.8.17.25        89077          ON
6505550143       10.8.17.34        87654         OFF
```

The table below describes significant fields shown in this output.

Table 5: show mwi relay clients Field Descriptions

Field	Description
Client	Client number.
IPADDR	IP address.
EXPIRES	Seconds before expiration.
MWI	MWI status.

Related Commands

Command	Description
mwi relay	Enables the Cisco IOS Telephony Service router to relay MWI information to remote Cisco IP phones.

show nextport

To display statistical information on NextPort digital signal processor (DSP) resources for diagnostic and debugging purposes, use the **show nextport** command in privileged EXEC mode.

show nextport {**dfc** *slot*/*port* | **est** [*slot*/*dfc*/*module* | **enabled**] | **ifd** {**queue** *slot*/*port* [**control** | **data** | **est** | **gdb** | **voice** | *npaddress* [*qid*]] | **statistics**} | **md** *modem* | **mm** [*slot*/*dfc*/*module* | **interrupt**] | **np-address** *slot*/*port* | **session** {*slot*/*port* | **tty** *ttynumber*} | **siglib test** | **ssm** {**info** *slot*/*port* | **test** | **vdev** *slot*/*port*} | **test** | **vpd** {**statistics** *slot*/*port* | **traffic** *slot*/*port*} | **vsmgr protocol violations**}

Syntax Description

dfc *slot* / *port*	Displays dial feature card (DFC) manager statistics for the specified slot and port. Range for the slot and port numbers is 1 to 7. The slash is required in the command syntax.
est	Displays Error/Status/Trace (EST) statistics for all the NextPort modules.
est *slot* / *dfc* / *module*	Displays EST information for the NextPort module in the specified slot, DFC, and module location. The slash is required in the command syntax.
est enabled	Displays a list of the enabled NextPort modules.
ifd queue *slot* / *port*	Displays the contents of one or more NextPort interface driver queues for the specified slot and port. Information includes the contents of the free, ready, and index rings, and the buffer description tables. The slash is required in the command syntax.
control	(Optional) Displays statistics for the interface control driver queue.
data	(Optional) Displays statistics for the interface data driver queue.
est	(Optional) Displays statistics for the interface EST driver queue.
gdb	(Optional) Displays statistics for the interface GDB driver queue.
voice	(Optional) Displays statistics for the interface voice driver queue.
npaddress	(Optional) The module address, expressed as a number (for example, 0x06000100).
qid	(Optional) Specific queue ID number. Range is from 0 to 31.
ifd statistics	Displays interface driver statistics, including any weak assertions generated.
md *modem*	Displays information for the specified NextPort modem instance.
mm	Displays modem manager information for the enabled NextPort modules.
mm *slot* / *dfc* / *module*	Displays modem manager information for the specified slot, DFC, and module location. The slash is required in the command syntax.
mm interrupt	Displays a list of system timer interrupt enabled modules.

np-address *slot* / *port*	Displays the NextPort address for the specified slot and port. The slash is required in the command syntax.
session *slot* / *port*	Displays NextPort session information for the specified slot and port. The slash is required in the command syntax.
session tty *ttynumber*	Displays NextPort session information for the specified tty session. Range is from 0 to 2003.
siglib test	Displays statistics for the SigLib test configuration.
ssm info *slot* / *port*	Displays information about the NextPort session and service manager (SSM) for the specified slot and port. The slash is required in the command syntax.
ssm test	Displays svc_id type, service type, and signaling type for the unit test configuration.
ssm vdev *slot* / *port*	Displays NextPort SSM Vdev information for the specified slot and port. The slash is required in the command syntax.
test	Displays information about the NextPort test parameters configuration.
vpd statistics *slot* / *port*	Displays the TX/RX packet counters for voice packet drivers (VPDs) (including success and failure statistics). The *slot* / *port* argument limits the output to statistics for the specified slot and port. The slash is required in the command syntax.
vpd traffic *slot* / *port*	Displays TX/RX VPD traffic statistics for the specified slot and port. The slash is required in the command syntax.
vsmgr protocol violations	Displays the number of payload violations for the NextPort voice resource manager.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	Router output for the **show nextport mm**command updated.
12.1(1)XD1	The **show nextport ifd queue** command was introduced.
12.3(11)T	This command was modified. Keywords and arguments were added to expand the variations of command output. The command was renamed **show nextport** with the **ifd queue**keyword was added.

Usage Guidelines

The **show nextport** command is intended to be used by Cisco Technical Support personnel to look at the NextPort DSP statistics and to perform detailed debugging. Please consult Cisco Technical Support before using this command.

The **show nextport** command is supported on the Cisco AS5300XM series, Cisco AS5400XM series, and Cisco AS5800XM series platforms.

When you enter the **show nextport vpd statistics**command on the Cisco AS5850, the output shows the TX/RX packet counters that could not be forwarded by distributed Cisco Express Forwarding. These packets are routed back to the enhanced route switch controller (ERSC).

The **show nextport vpd statistics***slot/port* command (on individual feature boards) displays the TX/RX packet counts for the packets that have been forwarded by distributed Cisco Express Forwarding.

The display of packet counts for the packets forwarded on the Cisco AS5850 is the result of the distributed architecture of the platform.

Examples

The following examples show some of the variations of the **show nextport** command.

Note Field descriptions in the examples provided are self-explanatory.

```
Router# show nextport session 1/1
 Session Information Display
  slot/port : 1/1 TTY# : 217 Session ID : 0x006D
  Module Address : Slot 1 DFC 0 Module 0 SPE 0 Channel 1
  Service Type   : DATA FAX MODEM
  Session State  : IDLE
  TDM Information:
   DSP is connected to TDM stream 0, channel 1 on the NextPort module
Router# show nextport vpd statistics
Voice Statistics for slot 1
Status: Active
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 2
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 3
Status: Active
Rx Statistics
 rx_successful= 0
 rx_failed= 0
```

```
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 4
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 5
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 6
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 7
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
```

```
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Router# show nextport ssm vdev 3/1
vdev_common handle @ 0xC0D92E20
 slot 3, port 1, tone , device_status(0): VDEV_STATUS_UNLOCKED
csm_state(0x0100)=CSM_IDLE_STATE, csm_event_proc=0x601EA0C0
invalid_event_count=2, wdt_timeout_count=0
wdt_timestamp_started is not activated
wait_for_dialing:False, wait_for_bchan:False
pri_chnl=TDM_ISDN_STREAM(s0, u0, c0), tdm_chnl=TDM_DSP_STREAM(s3, c1)
dchan_idb_start_index=0, dchan_idb_index=0, call_id=0x0000, bchan_num=-1
csm_event=CSM_EVENT_MODEM_ONHOOK, cause=0x0007
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=0
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, stat_busyout=0
oobp_failure=0, cas_address_signalling_failure=0
call_duration_started=00:00:00, call_duration_ended=00:00:00, total_call_durati0
The calling party phone number =
The called party phone number  =
total_free_rbs_timeslot = 0, total_busy_rbs_timeslot = 0, total_rtr_busy_rbs_ti,
total_sw56_rbs_timeslot = 0, total_sw56_rbs_static_bo_ts = 0,
total_free_isdn_channels = 0, total_auto_busy_isdn_channels = 0,
total_rtr_busy_isdn_channels = 0,
min_free_device_threshold = 0
Router# show nextport mm
IOS bundled NextPort image version: 0.0.0.0
NP Module(3 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(4 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(5 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(6 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(7 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(8 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(9 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(10): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(11): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 7.37.10.90
NP Module(12): slot=4, dfc=0, module=0
               state = MODULE RUNNING
               crash=0, bad=0, restarts=0, num SPEs=6
               max_mpt_redundancy_session = 18
               spe country code = 0
               session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(13): slot=4, dfc=0, module=1
               state = MODULE RUNNING
               crash=0, bad=0, restarts=0, num SPEs=6
               max_mpt_redundancy_session = 18
               spe country code = 0
               session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(14): slot=4, dfc=0, module=2
```

```
                state = MODULE RUNNING
                crash=0, bad=0, restarts=0, num SPEs=6
                max_mpt_redundancy_session = 18
                spe country code = 0
                session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(15): slot=5, dfc=0, module=0
                state = MODULE RUNNING
                crash=0, bad=0, restarts=0, num SPEs=6
                max_mpt_redundancy_session = 18
                spe country code = 0
                session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(16): slot=5, dfc=0, module=1
                state = MODULE RUNNING
                crash=0, bad=0, restarts=0, num SPEs=6
                max_mpt_redundancy_session = 18
                spe country code = 0
                session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(17): slot=5, dfc=0, module=2
                state = MODULE RUNNING
                crash=0, bad=0, restarts=0, num SPEs=6
                max_mpt_redundancy_session = 18
                spe country code = 0
                session handle enable = TRUE
IOS bundled NextPort image version: 0.0.0.0
NP Module(18): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(19): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(20): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(21): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(22): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(23): state = MODULE NOT INSERTED
```

Related Commands

Command	Description
show voice dsp	Displays the current status or selective statistics of DSP voice channels.

show nextport vpd

To display the TX/RX packet counters for voice packet drivers (VPDs) (including success and failure statistics), use the **show nextport vpd**command in privileged EXEC mode.

show nextport vpd {**statistics** [*slot*/*port-number*] | **traffic** [*slot*/*port-number*]}

Syntax Description

statistics	Displays information about the VPD statistics.
slot / *port number*	(Optional) The slot or port number of the interface.
traffic	Displays TX/RX VPD traffic statistics for the specified slot and port.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **show nextport vpd statistics** command displays the TX/RX packet counters that could not be forwarded by distributed Cisco Express Forwarding (dCEF). These packets are routed back to the enhanced route switch controller (ERSC). Executing show nextport vpd statistics slot/port (on individual feature boards) shows the TX/RX packet counts for the packets that have been forwarded by dCEF.

Examples

The following is sample output from the **show nextport vpd traffic**command for slot1 ans port1:

```
Router# show nextport vpd traffic 1/1
Voice Instance for slot 1 port 1
Status: Idle
Session Duration in second: 0
Rx traffic Statistics
  total rx bytes: 0
  total rx packets: 0
  average rx packets per second: 0
Tx traffic Statistics
  total tx bytes: 0
  total tx packets: 0
  average tx packets per second: 0
```

The table below describes the significant fields shown in the display.

Table 6: show nextport vpd Field Descriptions

Field	Description
Status	Current status of the voice traffic.
Session	Duration of the voice sessions in seconds.
Rx traffic Statistics	Number of packets received.

Field	Description
Tx traffic Statistics	Number of packets sent.

The following is sample output from the **show nextport vpd statistics**command. The field descriptions are self-explanatory.

```
Router# show nextport vpd statistics
Voice Instance for slot 1 port 1
Status: Idle
Rx Statistics
  rx_successful= 0
  rx_failed= 0
    queue destroyed = 0
    buffer pool depleted = 0
    invalid packet = 0
    wrong session packet = 0
Tx Statistics
  tx_successful= 0
  tx_acked_by_ifd= 0
  tx_failed= 0
    rejection by IFD = 0
```

show num-exp

To display the number expansions configured, use the **show num-exp**command in privileged EXEC mode.

show num-exp [*dialed-number*]

Syntax Description

dialed -number	(Optional) Dialed number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)T	This command was implemented on the Cisco AS5300.
12.0(4)XL	This command was implemented on the Cisco AS5800.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command to display all the number expansions configured for this router. To display number expansion for only one number, specify that number by using the *dialed-number* argument.

Examples

The following is sample output from this command:

```
Router# show num-exp
Dest Digit Pattern = '0...'     Translation = '+14085270...'
Dest Digit Pattern = '1...'     Translation = '+14085271...'
Dest Digit Pattern = '3..'      Translation = '+140852703..'
Dest Digit Pattern = '4..'      Translation = '+140852804..'
Dest Digit Pattern = '5..'      Translation = '+140852805..'
Dest Digit Pattern = '6....'    Translation = '+1408526....'
Dest Digit Pattern = '7....'    Translation = '+1408527....'
Dest Digit Pattern = '8...'     Translation = '+14085288...'
```

The table below describes significant fields shown in this output.

Table 7: show num-exp Field Descriptions

Field	Description
Dest Digit Pattern	Index number identifying the destination telephone number digit pattern.
Translation	Expanded destination telephone number digit pattern.

Related Commands

Command	Description
show call active voice	Displays the VoIP active call table.
show call history voice	Displays the VoIP call-history table.
show dial -peer voice	Displays configuration information for dial peers.
show voice port	Displays configuration information about a specific voice port.

show piafs status

To display the status of Personal Handyphone System (PHS) Internet Access Forum Standard (PIAFS) calls for each B channel in use on a router, use the **show piafs status** command in privileged EXEC mode.

show piafs status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from this command showing the status of PIAFS calls on B channel 1 on a Cisco 813 router:

```
Router# show piafs status
PIAFS STATUS INFORMATION
-------------------------
Number of active calls = 1
Details of connection 1
************************
Call Direction is: INCOMING
Call speed is: 64K
Current speed is: 64K
Call Elapsed Time: 59 seconds
The B channel assigned for this call is: B1 CHAN
Control Parameters Agreed Upon:
ARQ Control Information Transfer Protocol: Version 1
ARQ Data Transmission Protocol: Version 1
Measured RTF value: 9
PIAFS Frame Length in Bytes: 80
Maximum Frame Number: 63
Data Transmission Protocol of Peer: FIXED SPEED
Data Transmission Protocol of 800 Router: FIXED SPEED
V42 Negotiated: YES
V42 Parameters:
Direction: BOTH
No of code words: 4096
Max string length: 250
First PPP Frame Detected: YES
Piafs main FSM state: PIAFS_DATA
PIAFS Data Frames Tx Statistics:
Total No: of PIAFS Frames Confirmed: 344
Total Bytes of Application Data Transmitted:
Before Compression:  47021
After Compression: 30952
Compression Ratio in Tx direction is 1.51: 1
Total No: of PIAFS Frames Retransmitted: 32
Total Bytes of Application Data Retransmitted: 2336
Total Throughput in Tx Direction:
Including PIAFS Dummy Frames: 8000 Bytes/Second
Excluding PIAFS Dummy Frames: 859 Bytes/Second
```

```
Excluding PIAFS Dummy and Retransmitted Data Frames: 593 Bytes/Second
PIAFS Data Frames Rx Statistics:
Total No: of PIAFS Frames Received: 86
Total No: of Bad PIAFS Frames Received: 0
Total Bytes of Application Data Received:
Before Uncompression: 1459
After Uncompression: 2955
Compression Ratio in Rx direction is 2.02: 1
Total Throughput in Rx Direction:
Including PIAFS Dummy Frames: 8000 Bytes/Second
Excluding PIAFS Dummy Frames: 656 Bytes/Second
Excluding PIAFS Dummy and Retransmitted Data Frames: 126 Bytes/Second
No: of ReSynchronizations so far: 0
```

The table below describes significant fields shown in this output.

Table 8: show piafs status Field Descriptions

Field	Description
First PPP Frame Detected	If the output shows "YES," the first PPP frame from the peer device has been detected by the Cisco 803, Cisco 804, or Cisco 813 router. If the output shows "NO," the router has not received any PPP frames from the peer device.
Piafs main FSM state	Valid states for the finite state machine (FSM) are Initialization, Sync, Control, and Data.

Related Commands

Command	Description
debug piafs events	Displays debugging messages for PIAFS calls.

show platform hardware qfp active feature sbc fork global

To display media forking statistics that are related to all the forking instances for an active Cisco Quantum Flow Processor (QFP) instance of CUBE, use the **show platform hardware qfp active feature sbc fork global** command in privileged EXEC mode.

show platform hardware qfp active feature sbc fork global

Syntax Description

qfp	Cisco Quantum Flow Processor (QFP).
active	Displays the active instance of the processor.
sbc	Session Border Controller. CUBE is a Session Border Controller.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was modified to include statistics that are related to Websocket-based media forking.
Cisco IOS Release 15.2(1)S	This command was introduced.

Usage Guidelines

Use this command to display the global media forking statistics related to all the media forking instances of a CUBE platform. Media forking statistics that are related to WebSocket connections are included in the command as part of Cisco IOS XE Bengaluru 17.6.1a release. The statistics that are displayed for WebSocket-based media forking includes **SBC WebSocket Fork Global Statistics**, **Dropped RTP Packets**, and **Dropped Control Packets**. The section **SBC WebSocket Fork Global Statistics** displays statistics that are related to the transmission (TX) and receipt (RX) of RTP packets. For instance, the drop and replication of RTP packets in a media forking scenario. It also includes statistical details on the forward and drop of packets to control the session parameters in WebSocket-based media forking. The section **Dropped RTP Packets** provides statistical insight into the reasons for RTP packet drop. **Dropped Control Packets** contains statistical insight into the reasons for control packet drop.

Examples

The following sample output displays the media forking statistics, related to a CUBE platform:

```
router#show platform hardware qfp active feature sbc fork global
SBC Media Fork Global Statistics
------------------------------

  Total TX RTP packets replicated            = 0
  Total TX RTP octets replicated             = 0
  Total TX RTP packets dropped               = 0
  Total TX RTP octets dropped                = 0
  Total RX RTP packets replicated            = 0
  Total RX RTP octets replicated             = 0
  Total RX RTP packets dropped               = 0
  Total RX RTP octets dropped                = 0

SBC WebSocket Fork Global Statistics
------------------------------
```

```
Total TX RTP packets replicated          = 23641
Total TX RTP octets replicated           = 5413789
Total TX RTP packets dropped             = 0
Total TX RTP octets dropped              = 0
Total RX RTP packets replicated          = 23641
Total RX RTP octets replicated           = 5413789
Total RX RTP packets dropped             = 0
Total RX RTP octets dropped              = 0
Total control packets forwarded          = 6
Total control octets forwarded           = 1662
Total control packets dropped            = 0
Total control octets dropped             = 0

Dropped RTP Packets
-----------------------------

  Without associated fork session        = 0
  Invalid socket connection              = 0
  Invalid stream ID                      = 0
  Invalid packet data                    = 0
  WebSocket frame build failure          = 0
  Protobuf encoding failure              = 0
  Socket write failure                   = 0
  TLS sb setup failure                   = 0
  TLS encryption failure                 = 0
  Internal error                         = 0

Dropped Control Packets
-----------------------------

  Without associated fork session        = 0
  Invalid socket connection              = 0
  Invalid packet data                    = 0
  WebSocket frame decode failure         = 0
  Invalid WebSocket frame                = 0
  Socket write failure                   = 0
  TLS sb setup failure                   = 0
  TLS encryption failure                 = 0
  Internal error                         = 0
```

Related Commands

Command	Description
show voip stream-service connection history	Displays information about all the closed WebSocket connections in CUBE.
show voip stream-service server <ip:port>	Displays information about the WebSocket connection that is based on the WebSocket server IP and port.
show voip stream-service connection id <id>	Displays information about a WebSocket connection that is based on the WebSocket ID. Also, it displays all the forked call details.

show platform hardware qfp active feature sbc fork session

To display media forking statistics specific to a fork session for an active Cisco Quantum Flow Processor (QFP) instance of CUBE, use the **show platform hardware qfp active feature sbc fork session***id* command in privileged EXEC mode.

show platform hardware qfp active feature sbc fork session *id*

Syntax Description

qfp	Cisco Quantum Flow Processor (QFP).
active	Displays the active instance of the processor.
sbc	Session Border Controller. CUBE is a Session Border Controller.
id	The ID associated with a WebSocket media forking session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was modified to include statistics that are related to Websocket-based media forking.
Cisco IOS Release 15.2(1)S	This command was introduced.

Usage Guidelines

Use this command to display the statistics related to a specific media forking session in a WebSocket connection. The statistical information is displayed for the active instance of the QFP. The statistics that are displayed for WebSocket-based media forking as part of this command includes the following categories:

- **SBC WebSocket Fork Session Information**
  - **Primary call mgm correlator** and **Primary call mpf correlator**—Displays information that is related to the correlators of the original call.
  - **RX stream ID** and **TX stream ID**—Displays information about the WebSocket channels that are used to perform forking.
  - **Primary call anchor side**—Displays information about the side of the anchor on the call that is associated with the forking session.
  - **Payload type**—Displays information about the payload encoding type or the payload type that is contained in the packets. For example, payload type is zero for G711ulaw and eight for G711alaw.
- **SBC WebSocket Connection Information**—The forking session is associated with a WebSocket connection. Displays information about the WebSocket connection that is related to your forking session. This section contains information on whether your WebSocket connection is secure or not. Also, it provides information on the Local IP and port, Remote IP and port, WebSocket ID and WebSocket TCP socket ID.

- **SBC WebSocket Fork Session Statistics**—Displays information about the RTP packet drop and packet replication for both TX and RX streams. Also, it provides information on the packet drop and packet forward count for control packets.

Examples

The following sample output displays the media forking statistics, related to a fork session in a WebSocket connection:

```
router#show platform hardware qfp active feature sbc fork session 1
SBC WebSocket Fork Session Information
---------------------------------------

  Fork session ID                              = 1
  Fork session mgm correlator                  = 2
  Primary call mgm correlator                  = 1
  Primary call mpf correlator                  = 1
  Primary call anchor side                     = SIDE_A
  RX stream ID                                 = 1
  TX stream ID                                 = 2
  Payload type                                 = 0

SBC WebSocket Connection Information
---------------------------------------

  Secure                                       = No
  WebSocket ID                                 = 3
  WebSocket TCP socket ID                      = 0xec5f26c0
  Local port                                   = 38122
  Local IP (if v4)                             = 0a40565b
  Local IP (if v6)                             = 0a40565b:00000000:00000000:00000000
  Remote port                                  = 8083
  Remote IP (if v4)                            = 0a4056d7
  Remote IP (if v6)                            = 0a4056d7:00000000:00000000:00000000

SBC WebSocket Fork Session Statistics
---------------------------------------

  Total TX RTP packets replicated              = 3073
  Total TX RTP octets replicated               = 491680
  Total TX RTP packets dropped                 = 174
  Total TX RTP octets dropped                  = 30972
  Total RX RTP packets replicated              = 3071
  Total RX RTP octets replicated               = 491360
  Total RX RTP packets dropped                 = 176
  Total RX RTP octets dropped                  = 31328
  Total control packets forwarded              = 2
  Total control octets forwarded               = 464
  Total control packets dropped                = 0
  Total control octets dropped                 = 0
```

Related Commands

Command	Description
show voip stream-service connection history	Displays information about all the closed WebSocket connections in CUBE.
show voip stream-service server <ip:port>	Displays information about the WebSocket connection that is based on WebSocket server IP and port address.

Command	Description
show voip stream-service connection id <id>	Displays information about a WebSocket connection that is based on the WebSocket ID. Also, it displays all the forked call details.

show pots csm

To display the current state of calls and the most recent event received by the call-switching module (CSM) on a Cisco 800 series router, use the **show pots csm** command in privileged EXEC mode.

show pots csm *port*

Syntax Description

port	Port number. Range is from 1 to 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series.

Examples

The following is sample output from this command:

```
Router# show pots csm 1
POTS PORT: 1
   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 1 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 2 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
test pots dial	Dials a telephone number for the POTS port on the router by using a dial application on your workstation.
test pots disconnect	Disconnects a telephone call for the POTS port on the router.

show pots status

To display the settings of the telephone port physical characteristics and other information on the telephone interfaces of a Cisco 800 series router, use the **show pots status**command in privileged EXEC mode.

show pots status [**1** | **2**]

Syntax Description

1	(Optional) Displays the settings of telephone port 1.
2	(Optional) Displays the settings of telephone port 2.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Examples

The following is sample output from thiscommand.

```
Router# show pots status
POTS Global Configuration:
   Country: United States
   Dialing Method: Overlap, Tone Source: Remote, CallerId Support: YES
   Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
   Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
   Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
   TX Gain: 6dB, RX Loss: -6dB,
   Filter Mask: 6F
   Adaptive Cntrl Mask: 0
POTS PORT: 1
   Hook Switch Finite State Machine:
      State: On Hook, Event: 0
      Hook Switch Register: 10, Suspend Poll: 0
   CODEC Finite State Machine:
      State: Idle, Event: 0
      Connection: None, Call Type: Two Party, Direction: Rx only
      Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
      Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
      Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
      TX Gain: 6dB, RX Loss: -6dB,
      Filter Mask: 6F
      Adaptive Cntrl Mask: 0
   CODEC Registers:
      SPI Addr: 2, DSLAC Revision: 4
      SLIC Cmd: 0D, TX TS: 00, RX TS: 00
      Op Fn: 6F, Op Fn2: 00, Op Cond: 00
      AISN: 6D, ELT: B5, EPG: 32 52 00 00
      SLIC Pin Direction: 1F
   CODEC Coefficients:
      GX: A0 00
      GR: 3A A1
```

```
        Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
        B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
        X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
        R: 01 11 01 90 01 90 01 90 01 90 01 90
       GZ: 60
      ADAPT B: 91 B2 8F 62 31
   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
      Call 1 - State: idle, Call Id: 0x0
               Active: no
      Call 2 - State: idle, Call Id: 0x0
               Active: no
POTS PORT: 2
   Hook Switch Finite State Machine:
      State: On Hook, Event: 0
      Hook Switch Register: 20, Suspend Poll: 0
   CODEC Finite State Machine:
      State: Idle, Event: 0
      Connection: None, Call Type: Two Party, Direction: Rx only
      Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
      Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
      Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
      TX Gain: 6dB, RX Loss: -6dB,
      Filter Mask: 6F
      Adaptive Cntrl Mask: 0
   CODEC Registers:
      SPI Addr: 3, DSLAC Revision: 4
      SLIC Cmd: 0D, TX TS: 00, RX TS: 00
      Op Fn: 6F, Op Fn2: 00, Op Cond: 00
      AISN: 6D, ELT: B5, EPG: 32 52 00 00
      SLIC Pin Direction: 1F
   CODEC Coefficients:
      GX: A0 00
      GR: 3A A1
       Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
       B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
       X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
       R: 01 11 01 90 01 90 01 90 01 90 01 90
      GZ: 60
     ADAPT B: 91 B2 8F 62 31
   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
      Call 1 - State: idle, Call Id: 0x0
               Active: no
      Call 2 - State: idle, Call Id: 0x0
               Active: no
Time Slot Control: 0
```

The table below describes significant fields shown in this output.

Table 9: show pots status Field Descriptions

Field	Descriptions
POTS Global Configuration	Settings of the telephone port physical characteristic commands. Also displays the following: • TX GAIN--Current transmit gain of telephone ports. • RX LOSS--Current transmit loss of telephone ports. • Filter Mask--Value determines which filters are currently enabled or disabled in the telephone port hardware. • Adaptive Cntrl Mask--Value determines if telephone port adaptive line impedance hardware is enabled or disabled.
Hook Switch Finite State Machine	Device driver that tracks state of telephone port hook switch.
CODEC Finite State Machine	Device driver that controls telephone port codec hardware.
CODEC Registers	Register contents of telephone port codec hardware.
CODEC Coefficients	Codec coefficients selected by telephone port driver. Selected line type determines codec coefficients.
CSM Finite State Machine	State of call-switching module (CSM) software.
Time Slot Control	Register that determines if telephone port voice or data packets are sent to an ISDN B channel.

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive-ring-guard-time	Specifies a delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.

Command	Description
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.

show pots volume

To display the receiver volume level that is configured for each POTS port on a router, use the **show pots volume** command in privileged EXEC mode.

show pots volume

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from this command showing that the receiver volume level is 5 for both POTS port 1 and POTS port 2.

```
Router# show pots volume
POTS PORT 1: Volume 5
POTS PORT 2: Volume 5
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
volume	Configures the receiver volume level for a POTS port on a router.

show presence global

To display configuration information about the presence service, use the **show presence global** command in user EXEC or privileged EXEC mode.

show presence global

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command displays the configuration settings for presence.

Examples

The following example displays output from the **show subscription global** command:

```
Router# show subscription global
Presence Global Configuration Information:
=============================================
Presence feature enable            : TRUE
Presence allow external watchers   : FALSE
Presence max subscription allowed  : 100
Presence number of subscriptions   : 0
Presence allow external subscribe  : FALSE
Presence call list enable          : TRUE
Presence server IP address         : 0.0.0.0
Presence sccp blfsd retry interval : 60
Presence sccp blfsd retry limit    : 10
Presence router mode               : CME mode
```

The table below describes the significant fields shown in the display.

Table 10: show subscription global Field Descriptions

Field	Description
Presence feature enable	Indicates whether presence is enabled on the router with the **presence** command.
Presence allow external watchers	Indicates whether internal presentities can be watched by external watchers, as set by the **watcher all** command
Presence max subscription allowed	Maximum number of presence subscriptions allowed by the **max-subscription** command.

Field	Description
Presence number of subscriptions	Current number of active presence subscriptions.
Presence allow external subscribe	Indicates whether internal watchers are allowed to subscribe to status notifications from external presentities, as set by the **allow subscribe** command.
Presence call list enable	Indicates whether the Busy Lamp Field (BLF) call-list feature is enabled with the **presence call-list** command.
Presence server IP address	Displays the IP address of an external presence server defined with the **server** command.
Presence sccp blfsd retry interval	Retry timeout, in seconds, for BLF speed-dial numbers on SCCP phones set by the **sccp blf-speed-dial retry interval** command.
Presence sccp blfsd retry limit	Maximum number of retries allowed for BLF speed-dial numbers on SCCP phones set by the **sccp blf-speed-dial retry interval** command.
Presence router mode	Indicates whether the configuration mode is set to Cisco Unified CME or Cisco Unified SRST by the **mode** command.

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
debug presence	Displays debugging information about the presence service.
presence enable	Allows the router to accept incoming presence requests.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
show presence subscription	Displays information about active presence subscriptions.
watcher all	Allows external watchers to monitor internal presence entities (directory numbers).

show presence subscription

To display information about active presence subscriptions, use the **show presence subscription** command in user EXEC or privileged EXEC mode.

show presence subscription [**details** | **presentity** *telephone-number* | **subid** *subscription-id* | **summary**]

Syntax Description

details	(Optional) Displays detailed information about presentities, watchers, and presence subscriptions.
presentity *telephone-number*	(Optional) Displays information on the presentity specified by the destination telephone number.
subid *subscription-id*	(Optional) Displays information for the specific subscription ID.
summary	(Optional) Displays summary information about active subscription requests.

Command Default

Information for all active presence subscriptions is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

This command displays details about the currently active presence subscriptions

Examples

The following is sample output from the **show presence subscription details** command:

```
Presence Active Subscription Records Details:
=============================================

Subscription ID         : 1
  Watcher               : 6002@10.4.171.60
  Presentity            : 6005@10.4.171.34
  Expires               : 3600 seconds
  Subscription Duration : 1751 seconds
  line status           : idle
  watcher type          : local
  presentity type       : local
  Watcher phone type    : SIP Phone
  subscription type     : Incoming Indication
  retry limit           : 0
  sibling subID         : 0
  sdb                   : 0
```

```
  dp                     : 6555346C
  watcher dial peer tag : 40001
  number of presentity  : 1

Subscription ID         : 2
  Watcher               : 6002@10.4.171.60

Presence Active Subscription Records:
=============================================

Subscription ID         : 30
  Watcher               : 4085550103@10.4.171.34
  Presentity            : 5001@10.4.171.20
  Expires               : 3600 seconds
  line status           : idle
  watcher type          : local
  presentity type       : remote
  Watcher phone type    : SCCP [BLF Call List]
  subscription type     : Outgoing Request
  retry limit           : 0
  sibling subID         : 23
  sdb                   : 0
  dp                    : 0
  watcher dial peer tag : 0
```

The following is sample output from the **show presence subscription summary** command:

```
Router# show presence subscription summary

Presence Active Subscription Records Summary: 15 subscription
Watcher                  Presentity               SubID  Expires SibID  Status
======================== ======================== ====== ======= ====== ======
6002@10.4.171.60         6005@10.4.171.34          1     3600    0      idle
6005@10.4.171.81         6002@10.4.171.34          6     3600    0      idle
6005@10.4.171.81         6003@10.4.171.34          8     3600    0      idle
6005@10.4.171.81         6002@10.4.171.34          9     3600    0      idle
6005@10.4.171.81         6003@10.4.171.34          10    3600    0      idle
6005@10.4.171.81         6001@10.4.171.34          12    3600    0      idle
6001@10.4.171.61         6003@10.4.171.34          15    3600    0      idle
6001@10.4.171.61         6002@10.4.171.34          17    3600    0      idle
6003@10.4.171.59         6003@10.4.171.34          19    3600    0      idle
6003@10.4.171.59         6002@10.4.171.34          21    3600    0      idle
6003@10.4.171.59         5001@10.4.171.34          23    3600    24     idle
6002@10.4.171.60         6003@10.4.171.34          121   3600    0      idle
6002@10.4.171.60         5002@10.4.171.34          128   3600    129    idle
6005@10.4.171.81         1001@10.4.171.34          130   3600    131    busy
6005@10.4.171.81         7005@10.4.171.34          132   3600    133    idle
```

The following is sample output from the **show presence subscription summary** command showing that device-based BLF monitoring is enabled on two phones.

```
Watcher                    Presentity                SubID  Expires SibID  Status
========================== ========================= ====== ======= ====== ======
D 2036@10.6.2.6            2038@10.6.2.254           33     3600    0      idle

  2036@10.6.2.6            2038@10.6.2.254           35     3600    0      idle

D 2036@10.6.2.6            8883@10.6.2.254           37     3600    0      unknown
```

The following is sample output from the **show presence subscription subid**command:

```
Router# show presence subscription subid 133

Presence Active Subscription Records:
=============================================

Subscription ID          : 133
  Watcher                : 6005@10.4.171.34
  Presentity             : 7005@10.4.171.20
  Expires                : 3600 seconds
  line status            : idle
  watcher type           : local
  presentity type        : remote
  Watcher phone type     : SIP Phone
  subscription type      : Outgoing Request
  retry limit            : 0
  sibling subID          : 132
  sdb                    : 0
  dp                     : 0
  watcher dial peer tag : 0
```

The table below describes the significant fields shown in the display.

Table 11: show presence subscription Field Descriptions

Field	Description
Watcher	IP address of the watcher.
Presentity	IP address of the presentity.
Expires	Number of seconds until the subscription expires. Default is 3600.
line status	Status of the line: • Idle--Line is not being used. • In-use--User is on the line, whether or not this line can accept a new call. • Unknown--Phone is unregistered or this line is not allowed to be watched.
watcher type	Whether the watcher is local or remote.
presentity type	Whether the presentity is local or remote.
Watcher phone type	Type of phone, either SCCP or SIP.
subscription type	The type of presence subscription, either incoming or outgoing.
retry limit	Maximum number of times the router attempts to subscribe for the line status of an external SCCP phone when either the presentity does not exist or the router receives a terminated NOTIFY from the external presence server. Set with the **sccp blf-speed-dial retry-interval** command.
sibling subID	Sibling subscription ID if presentity is remote. If value is 0, presentity is local.
sdb	Voice port of the presentity.

Field	Description
dp	Dial peer of the presentity.
watcher dial peer tag	Dial peer tag of the watcher device.

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
blf-speed-dial	Enables BLF monitoring for a speed-dial number on a phone registered to Cisco Unified CME.
debug ephone blf	Displays debugging information for BLF presence features.
debug presence	Displays debugging information about the presence service.
presence	Enables presence service and enters presence configuration mode.
presence enable	Allows the router to accept incoming presence requests.
show presence global	Displays configuration information about the presence service.

show proxy h323 calls

To display a list of active calls on the proxy, use the **show proxy h323 calls** command in privilegedEXEC mode.

show proxy h323 calls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Examples

The following is sample output from thiscommand:

```
Router# show proxy h323 calls
Call unique key = 1
  Conference ID = [277B87C0A283D111B63E00609704D8EA]
  Calling endpoint call signalling address = 55.0.0.41
  Calling endpoint aliases:
   H323_ID: ptel11@zone1.com
  Call state = Media Streaming
  Time call was initiated = 731146290 ms
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show proxy h323 detail-call	Displays the details of a particular call on a proxy.
show proxy h323 status	Displays the overall status of a proxy.

show proxy h323 detail-call

To display the details of a particular call on a proxy, use the **show proxy h323 detail-call** command in privileged EXEC mode.

show proxy h323 detail-call *call-key*

Syntax Description

call -key	Call to be displayed, derived from the **show proxy h323 calls** command output.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Usage Guidelines

You can use this command with or without proxy statistics enabled.

Examples

The following is sample output from this command without proxy statistics enabled:

```
Router# show proxy h323 detail-call 1
ConferenceID = [277B87C0A283D111B63E00609704D8EA]
Calling endpoint aliases:
      H323_ID: ptel11@zone1.com
Called endpoint aliases:
      H323_ID: ptel21@zone2.com
Peer proxy call signalling address = 172.17.0.41
Time call was initiated = 731146290 ms
Inbound CRV = 144
Outbound CRV = 70
Call state = Media Streaming
H245 logical channels for call leg pte111@zone1.com<->px1@zone.com
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146317 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146316 ms
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146318 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
```

```
        Time created = 731146317 ms
H245 logical channels for call leg pte111@zone1.com<->172.17.50.21:
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146317 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146316 ms
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146318 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146317 ms
```

The following is sample output from this command with proxy statistics enabled:

```
Router# show proxy h323 detail-call 1
ConferenceID = [677EB106BD0D111976200002424F832]
Calling endpoint call signalling address = 172.21.127.49
    Calling endpoint aliases:
      H323_ID: intel2
      E164_ID: 2134
Called endpoint aliases:
      H323_ID: mcs@sanjose.cisco.com
Peer proxy call signalling address = 172.68.183.199
Peer proxy aliases:
      H323_ID: proxy.sanjose.cisco.com
Time call was initiated = 730949651 ms
Inbound CRV = 2505
Outbound CRV = 67
Call state = H245 open logical channels
H245 logical channels for call leg intel2 <-> cisco7-pxy:
    Channel number = 259
      RTP stream from intel2 to cisco7-pxy
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949676 ms
    Channel number = 257
      RTP stream from intel2 to cisco7-pxy
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949658 ms
    Channel number = 2
      RTP stream from cisco7-pxy to intel2
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949664 ms
        RTP Statistics:
          Packet Received Count = 3390
          Packet Dropped Count = 0
          Packet Out of Sequence Count = 0
          Number of initial packets used for Arrival-Spacing bin setup = 200
```

```
min_arrival_spacing = 0(ms)  max_arrival_spacing = 856(ms)
Average Arrival Rate = 86(ms)
Arrival-Spacing(ms)   Packet-Count
   0                     2116
   26                    487
   52                    26
   78                    0
   104                   0
   130                   1
   156                   0
   182                   1
   208                   0
   234                   4
   260                   99
   286                   315
   312                   154
   338                   8
   364                   0
   390                   2
   416                   10
   442                   73
   468                   51
   494                   43
==============================
Min Jitter = 34(ms)  Max Jitter = 408(ms)
Average Jitter Rate = 117
Jitter Rate(ms)   Packet-Count
   0                     0
   41                    514
   82                    2117
Number of initial packets used for Arrival-Spacing bin setup = 200
min_arrival_spacing = 32(ms)  max_arrival_spacing = 96(ms)
Average Arrival Rate = 60(ms)
Arrival-Spacing(ms)   Packet-Count
   32                    35
   34                    0
   36                    177
   38                    0
   40                    56
   42                     0
   44                    10
   46                    0
   48                    27
   50                    0
   52                    541
   54                    0
   56                    2642
   58                    1
   60                    1069
   62                    0
   64                    77 0
   68                    6
   70                    257
==============================
Min Jitter = 0(ms)  Max Jitter = 28(ms)
Average Jitter Rate = 5
Jitter Rate(ms)   Packet-Count
   0                     1069
   3                     2720
   6                     0
   9                     804
   12                    27
   15                    10
   18                    0
```

```
            21                    56
            24                    177
            27                    35
H245 logical channels for call leg cisco7-pxy <->
proxy.sanjose.cisco.com:
    Channel number = 259
      RTP stream from cisco7-pxy to proxy.sanjose.cisco.com
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949676 ms
        RTP Statistics:
          Packet Received Count = 3398
          Packet Dropped Count = 1
          Packet Out of Sequence Count = 0
          Number of initial packets used for Arrival-Spacing bin setup = 200
          min_arrival_spacing = 0(ms)  max_arrival_spacing = 872(ms)
          Average Arrival Rate = 85(ms)
          Arrival-Spacing(ms)   Packet-Count
            0                     2636
            28                    0
            56                    0
            84                    0
            112                   0
            140                   1
            168                   0
            196                   0
            224                   0
            252                   0
            280                   2
            308                   425
            336                   154
            364                   5
            392                   0
            420                   0
            448                   0
            476                   114
            504                   41
            532                   20
          ==============================
          Min Jitter = 55(ms)  Max Jitter = 447(ms)
          Average Jitter Rate = 127
          Jitter Rate(ms)   Packet-Count
            0                     0
            45                    1
            90                    2636
            135                   0
            180                   2
            225                   425
            270                   159
            315                   0
            360                   0
            405                   175
    Channel number = 257
      RTP stream from cisco7-pxy to proxy.sanjose.cisco.com
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949658 ms
        RTP Statistics:
          Packet Received Count = 2537
          Packet Dropped Count = 3
          Packet Out of Sequence Count = 0
          Number of initial packets used for Arrival-Spacing bin setup = 200
```

```
          min_arrival_spacing = 0(ms)  max_arrival_spacing = 32716(ms)
          Average Arrival Rate = 112(ms)
          Arrival-Spacing(ms)   Packet-Count
             0                     2191
             72                    253
             144                   31
             216                   7
             288                   3
             360                   4
             432                   4
             504                   2
             576                   1
             648                   3
             720                   2
             792                   1
             864                   2
             936                   1
             1008                  1
             1080                  1
             1152                  1
             1224                  1
             1296                  0
             1368                  28
          ==============================
          Min Jitter = 32(ms)  Max Jitter = 1256(ms)
          Average Jitter Rate = 121
          Jitter Rate(ms)   Packet-Count
             0                     284
             126                   2201
             252                   4
             378                   6
             504                   4
             630                   3
             756                   2
             882                   2
             1008                  2
             1134                  29
    Channel number = 2
      RTP stream from proxy.sanjose.cisco.com to cisco7-pxy
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949664 ms
    Channel number = 1
      RTP stream from proxy.sanjose.cisco.com to cisco7-pxy
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949661 ms
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
h323 qos	Enables QoS on the proxy.
show proxy h323 calls	Displays a list of active calls on the proxy.
show proxy h323 status	Displays the overall status of a proxy.

show proxy h323 status

To display the overall status of a proxy, use the **show proxy h323 status**command in privileged EXEC mode.

show proxy h323 status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Examples

The following is sample output from this command:

```
Router# show proxy h323 status
  H.323 Proxy Status
        ==================
    H.323 Proxy Mode: Enabled
    Proxy interface = Serial1: UP
    Application Specific Routing: Disabled
    RAS Initialization: Complete
    Proxy aliases configured:
      H323_ID: px2
    Proxy aliases assigned by Gatekeeper:
      H323_ID: px2
    Gatekeeper multicast discovery: Disabled
    Gatekeeper:
        Gatekeeper ID: gk.zone2.com
        IP address: 70.0.0.31
    Gatekeeper registration succeeded
    T.120 Mode: BYPASS
    RTP Statistics: OFF
    Number of calls in progress: 1
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show proxy h323 calls	Displays a list of active calls on the proxy.
show proxy h323 detail-call	Displays the details of a particular call on a proxy.

show raw

To display leaking raw buffers that have been captured, use the **show raw** command in privileged EXEC mode.

show raw {**all** | **cas** | **ccapi** | **h323** | **ivr** | **reclaimed** | **tsp** | **vtsp**}

Syntax Description

all	Displays the record of all sections.
cas	Displays the record of channel-associated signaling (CAS).
ccapi	Displays the application programming interface (API) that is used to coordinate interaction between application and call legs (telephony or IP).
h323	Displays the record of the H.323 subsystem.
ivr	Displays the record of interactive voice response (IVR).
reclaimed	Displays the raw buffers reclaimed by the audit module.
tsp	Displays the telephony service provider (TSP) subsystem.
vtsp	Displays the voice telephony service provider (VTSP) subsystem.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XU3	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The number of raw leaks that are displayed by the **show raw reclaimed** command should be zero, indicating that there are no memory leaks.

Examples

The following is a sample output from this command showing that there are no leaking raw buffers:

```
Router# show raw reclaimed
```

RAW LEAK REPORT:

ORPHAN : 0 raw buffers reclaimed

TSP : 0 raw buffers reclaimed

VTSP : 0 raw buffers reclaimed

H323 : 0 raw buffers reclaimed

SIP : 0 raw buffers reclaimed

CCAPI : 0 raw buffers reclaimed

VOATM : 0 raw buffers reclaimed

XGCP : 0 raw buffers reclaimed

CAS : 0 raw buffers reclaimed

IVR : 0 raw buffers reclaimed

SSAPP : 0 raw buffers reclaimed

Last Audit Session is at 20:28:13 UTC Fri Mar 27 2002

The table below describes significant fields shown in this output.

Table 12: show raw reclaimed Field Descriptions

Field	Description
ORPHAN	R aw buffers when a valid owner is not found.
TSP	Raw buffers on the telephony service provider (TSP) subsystem.
VTSP	Raw buffers on the voice telephony service provider (VTSP) subsystem.
H323	Raw buffers on the H.323 subsystem.
SIP	Raw buffers on the Session Initiation Protocol session.
CCAPI	Raw buffers on the API system used to coordinate interaction between application and call legs (telephony or IP).
VOATM	Raw buffers on the Voice over ATM network.
XGCP	Raw buffers on external media gateway control protocols. Includes Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP).
CAS	Raw buffers on the channel-associated signaling (CAS).
IVR	Raw buffers on the interactive voice response (IVR) system.
SSAPP	Raw buffers on the session application.

Related Commands

Command	Description
show rawmsg	Shows raw messages owned by the required component.

show rawmsg

To display the raw messages owned by the required component, use the **show rawmsg** command in privileged EXEC mode.

show rawmsg {**all** | **cas** | **ccapi** | **h323** | **ivr** | **reclaimed** | **tsp** | **vtsp**}

Syntax Description

all	Displays the raw messages owned by all the components.
cas	Displays the Channel Associated Signaling (CAS) subsystem.
ccapi	Displays the Application programming interface (API) used to coordinate interaction between application and call legs (telephony or IP).
h323	Displays the H.323 subsystem.
ivr	Displays the Interactive Voice Response (IVR) subsystem.
reclaimed	Displays the raw reclaimed by the audit module.
tsp	Displays the Telephony Service Provider (TSP) subsystem.
vtsp	Displays the Voice Telephony Service Provider (VTSP) subsystem.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **cas**, **ivr**, and **reclaimed** keywords were added.

Usage Guidelines

The number displayed for the **show rawmsg all** command should be zero to indicate that there are no memory leaks.

Examples

The following is a sample output from the **show rawmsg tsp** command that displays memory leaks from the Telephony Service Provider. The field names are self-explanatory.

```
Router# show rawmsg tsp
 Raw Msg Summary:
       Raw Msg in used: 0
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.

Command	Description
isdn switch type	Configures the Cisco AS5300 PRI interface to support Q.SIG signaling.
pri-group nec-fusion	Configures the NEC PBX to support FCCS.
show cdapi	Displays the CDAPI.

show rlm group statistics

To display the network latency of a Redundant Link Manager (RLM) group, use the **show rlm group statistics**command in privileged EXEC mode.

show rlm group [*group-number*] **statistics**

Syntax Description

group -number	(Optional) RLM group number. The range is from 0 to 255. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(7)	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

You can specify the *group-number* argument to view the network latency of a specific RLM group. If you do not specify the *group-number* argument, then the **show rlm group statistics** command displays the network latency of all the configured RLM groups.

Examples

The following is sample output from the **show rlm group statistics** command:

```
Router# show rlm group statistics
RLM Group Statistics
 Link_up:
     last time occurred at 02:45:48.724, total transition=1
     avg=00:00:00.000, max=00:00:00.000, min=00:00:00.000, latest=00:00:00.000
 Link_down:
     last time occurred at 02:42:33.724, total transition=1
     avg=00:03:15.000, max=00:03:15.000, min=00:00:00.000, latest=00:03:15.000
 Link_recovered:
     last time occurred at 00:00:00.000, success=0(0%), failure=0
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
 Link_switched:
     last time occurred at 00:00:00.000, success=0(0%), failure=0
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
 Server_changed:
     last time occurred at 00:00:00.000 for totally 0 times
 Server Link Group[r1-server]:
  Open the link [10.1.1.1(Loopback1), 10.1.4.1]:
     last time occurred at 02:43:03.724, success=1(100%), failure=0
     avg=162.000s, max=162.000s, min=0.000s, latest=162.000s
  Echo over link [10.1.1.1(Loopback1), 10.1.4.1]:
     last time occurred at 02:47:15.724, success=91(62%), failure=54
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Open the link [10.1.1.2(Loopback2), 10.1.4.2]:
     last time occurred at 02:43:03.724, success=1(100%), failure=0
     avg=162.000s, max=162.000s, min=0.000s, latest=162.000s
  Echo over link [10.1.1.2(Loopback2), 10.1.4.2]:
     last time occurred at 02:47:19.724, success=95(63%), failure=54
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
 Server Link Group[r2-server]:
```

```
  Open the link [10.1.1.1(Loopback1), 10.1.5.1]:
     last time occurred at 02:46:06.724, success=0(0%), failure=1
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Echo over link [10.1.1.1(Loopback1), 10.1.5.1]:
     last time occurred at 02:47:18.724, success=0(0%), failure=85
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
Open the link [10.1.1.2(Loopback2), 10.1.5.2]:
     last time occurred at 02:46:06.724, success=0(0%), failure=1
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Echo over link [10.1.1.2(Loopback2), 10.1.5.2]:
     last time occurred at 02:47:18.724, success=0(0%), failure=85
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
```

The table below describes the significant fields shown in the display.

Table 13: show rlm group statistics Field Descriptions

Field	Description
Link_up	Statistics collected when the RLM group is in the link up state.
total transition	Total number of transitions into a particular RLM group state.
avg	Total average time (in seconds) that the interval lasts.
max	Total maximum time (in seconds) that the interval lasts.
min	Total minimum time (in seconds) that the interval lasts.
latest	The most recent interval.
Link_down	Statistics collected when the RLM group is in the link down state.
Link_recovered	Statistics collected when the RLM group is in the link recovery state.
Link_switched	Statistics collected when the RLM group is in the link switching state.
Server_changed	Statistics collected for when and how many times an RLM server failover happens.
Server Link Group[r1-server]	Statistics collected for the signaling links defined under a particular server link group, for example, r1-server.
Open the link	Statistics collected when a particular signaling link connection is open (broken).
Echo over link	Statistics collected when a particular signaling link connection is established.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Configures an interface type and enters interface configuration mode.
link (RLM)	Specifies the link preference.

Command	Description
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP address of the server.
show rlm group status	Displays the status of an RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under an RLM group.
timer	Overwrites the default setting of timeout values.

show rlm group status

To display the status of a Redundant Link Manager (RLM) group, use the **show rlm group status** command in privileged EXEC mode.

show rlm group [*group-number*] **status**

Syntax Description

group -number	(Optional) RLM group number. The range is from 0 to 255. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(7)	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

You can specify the *group-number* argument to view the status of a specific RLM group. If you do not specify the *group-number* argument, then the **show rlm group status** command displays the status of all the configured RLM groups.

Examples

The following is sample output from the **show rlm group status** command:

```
Router# show rlm group status
RLM Group 1 Status
 User/Port: RLM_MGR/3000
 Link State: Up         Last Link Status Reported: Up
 Next tx TID: 1         Last rx TID: 0
 Server Link Group[r1-server]:
  link [10.1.1.1(Loopback1), 10.1.4.1] = socket[active]
  link [10.1.1.2(Loopback2), 10.1.4.2] = socket[standby]
 Server Link Group[r2-server]:
  link [10.1.1.1(Loopback1), 10.1.5.1] = socket[opening]
  link [10.1.1.2(Loopback2), 10.1.5.2] = socket[opening]
```

The table below describes the significant fields shown in the display.

Table 14: show rlm group status Field Descriptions

Field	Description
User/Port	List of registered RLM users and the port numbers associated with them.
RLM_MGR	RLM management module.
Link State	Current RLM group's link state for connecting to the remote end.
Last Link Status Reported	Most recent link status change is reported to RLM users.
Next tx TID	Next transaction ID for transmission.

Field	Description
Last rx TID	Most recent transaction ID has been received.
Server Link Group[r1-server]	Status of all signaling links configured under a particular RLM server link group, for example, r1-server.
socket	Status of the individual signaling link.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Configures an interface type and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP address of the server.
show rlm group statistics	Displays the network latency of an RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under an RLM group.
timer	Overwrites the default setting of timeout values.

show rlm group timer

To display the current timer values of a Redundant Link Manager (RLM) group, use the **show rlm group timer** command in privileged EXEC mode.

show rlm group [*group-number*] **timer**

Syntax Description

group -number	(Optional) RLM group number. The range is from 0 to 255. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(7)	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

You can specify the *group-number* argument to view the timer values of a specific RLM group. If you do not specify the *group-number* argument, then the **show rlm group timer**command displays the timer values of all the configured RLM groups.

Examples

The following is sample output from the **show rlm group timer** command:

```
Router# show rlm group timer
RLM Group 1 Timer Values
 open_wait  = 3s               force-down  = 30s
 recovery   = 12s              switch-link = 5s
 minimum-up = 60s              retransmit  = 1s
 keepalive  = 1s
```

The table below describes the significant fields shown in the display.

Table 15: show rlm group timer Field Descriptions

Field	Description
open_wait	Wait for the connection request to be acknowledged.
recovery	Time (in seconds) to allow the link to recover to backup link before declaring the link is down.
minimum-up	Minimum time (in seconds) to force RLM to stay in the link down state for the remote end to detect that the link state is down.
keepalive	A keepalive packet is sent out from the network access server to the Card Security Code (CSC) periodically.
force-down	Minimum time (in seconds) to force RLM to stay in the link down state for the remote end to detect that the link state is down.

Field	Description
switch-link	The maximum transition period allows RLM to switch from a lower preference link to a higher preference link. If the switching link does not complete successfully before this timer expires, RLM goes into the recovery state.
retransmit	Because RLM is operating under User Datagram Protocol (UDP), it needs to resend the control packet if the packet is not acknowledged within this retransmit interval (in seconds).

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Configures an interface type and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP address of the server.
show rlm group statistics	Displays the network latency of an RLM group.
show rlm group status	Displays the status of an RLM group.
shutdown (RLM)	Shuts down all of the links under an RLM group.
timer	Overwrites the default setting of timeout values.

show rpms-proc counters

To display statistics for the number of leg 3 authentication, authorization, and accounting (AAA) preauthentication requests, successes, and rejects, use the **show rpms-proc counters** command in privileged EXEC mode.

show rpms-proc counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Leg 3 refers to a call segment from the IP network to a terminating (outgoing) gateway that takes traffic from an IP network to a PSTN network.

Examples

The following sample output displays leg 3 statistics for AAA preauthentication requests, successes, and rejects:

```
Router# show rpms-proc counters
H323 Calls
Preauth Requests Sent      : 43433
Preauth Requests Accepted  : 43433
Preauth Requests Rejected  : 0
Preauth Requests TimedOut  : 0
Disconnects during Preauth : 0
SIP Calls
Preauth Requests Sent      : 43080
Preauth Requests Accepted  : 43080
Preauth Requests Rejected  : 0
Preauth Requests TimedOut  : 0
Disconnects during Preauth : 0
```

The table below describes significant fields shown in this output.

Table 16: show rpms-proc counters Field Descriptions

Field	Description
Preauth Requests Sent	Number of preauthentication requests sent.
Preauth Requests Accepted	Number of preauthentication requests accepted.
Preauth Requests Rejected	Number of preauthentication requests rejected.
Preauth Requests Timed Out	Number of preauthentication requests rejected because they timed out.
Disconnects during Preauth	Number of calls that were disconnected during the preauthentication process.

Related Commands

Command	Description
clear rpms -proc counters	Clears statistics counters for AAA preauthentication requests, successes, and rejects.

show running-config dial-peer

To display only dial-peer configuration information from running configuration, use the **show running-config dial-peer** command in privileged EXEC (#) mode.

show running-config dial-peer {**sort** [**descending**] | **voice** *tag*}

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.5(2)T, Cisco IOS XE Release 3.15S	This command was introduced.

Usage Guidelines

The **show running-config dial-peer** command displays the dial-peers in the running-configuration based on the timestamp in which they were configured.

Example

In the below examples, 5, 4020, and 5000 indicate dial-peer tags. The following command displays the dial-peers in ascending order of timestamp in which they were configured:

```
Device# show running-config dial-peer

dial-peer voice 4020 pots
 destination-pattern 4020
 port 0/2/0
!
dial-peer voice 5000 voip
 destination-pattern 5...
 session protocol sipv2
 session target ipv4:1.4.65.5
!
dial-peer voice 5 pots
incoming called-number 1...
port 1/0/0:23
```

The following command displays the dial-peers in ascending order of dial-peer tag:

```
Device# show running-config dial-peer sort

dial-peer voice 5 pots
incoming called-number 1...
port 1/0/0:23
!
dial-peer voice 4020 pots
 destination-pattern 4020
 port 0/2/0
!
dial-peer voice 5000 voip
 destination-pattern 5...
 session protocol sipv2
 session target ipv4:1.4.65.5
```

The following command displays the dial-peers in descending order of dial-peer tag:

```
Device# show running-config dial-peer sort descending

dial-peer voice 5000 voip
 destination-pattern 5...
 session protocol sipv2
 session target ipv4:1.4.65.5
!
dial-peer voice 4020 pots
 destination-pattern 4020
 port 0/2/0
!
dial-peer voice 5 pots
incoming called-number 1...
port 1/0/0:23
```

The following command displays the dial-peer information specific to a dial-peer tag:

```
Device# show running-config dial-peer voice 4020

dial-peer voice 4020 pots
 destination-pattern 4020
 port 0/2/0
```

show rtpspi

To display Real-time Transport Protocol (RTP) serial peripheral interface (SPI) active call details and call statistics, use the **show rtpspi**command in privileged EXEC mode.

show rtpspi {**call** | **statistics**}

Syntax Description

call	Displays RTP SPI active call details.
statistics	Displays RTP SPI call statistics information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T.

Examples

The following is sample output from the **show rtpspi statistics**command:

```
Router# show rtpspi statistics
RTP Statistics info:
No. CallId     Xmit-pkts Xmit-bytes Rcvd-pkts  Rcvd-bytes Lost pkts  Jitter Latenc
1   48         0x3BA     0x25440    0x17       0xD99      0x0        0x0     0x0
2   50         0x3BA     0x4A88     0x70       0x8AD      0x0        0x0     0x0
```

The table below describes the significant fields shown in the display.

Table 17: show rtpspi statistics Field Descriptions

Field	Description
CallId	The call ID number.
Xmit-pkts	Number of packets transmitted.
Xmit-bytes	Number of bytes transmitted.
Rcvd-pkts	Number of packets received.
Rcvd-bytes	Number of bytes received.
Lost pkts	Number of lost packets.
Jitter	Reports the jitter encountered.
Latenc	Reports the level of latency on the call.

Related Commands

Command	Description
debug rtpspi all	Debugs all RTP SPI errors, sessions, and in/out functions.

show rtsp client session

To display cumulative information about Real Time Streaming Protocol (RTSP) session records, use the **show rtsp client session** command in privileged EXEC mode.

show rtsp client session {**history** | **active**} [**detailed**]

Syntax Description

history	Displays cumulative information about the session, packet statistics, and general call information such as call ID, session ID, individual RTSP stream URLs, packet statistics, and play duration.
active	Displays session and stream information for the stream that is currently active.
detailed	(Optional) Displays session and stream information in detail for all streams that are associated with the session. This keyword is not available on Cisco 7200 series routers.

Command Default

Active (current) stream information is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800 and Cisco AS5850 is not included in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Usage Guidelines

Use this command to display cumulative information about the session, packet statistics, and general call information such as call ID and session ID.

Note Session refers to a session between the application and the RTSP client. Each call leg that is configured to use RTSP streaming has a session.

A call leg could play several prompts in a session; the "Play Time" refers to the play time associated with a stream or, in other words, a prompt; the cumulative play time is the sum total of all streams (or prompts) played out in a session.

The command output is a stream block that contains information about the stream (URL, packet statistics, current state of the stream, play duration, call ID, session ID, individual RTSP stream URLs, and packet statistics).

Examples

The following is sample output from the **show rtsp client session active** command :

```
Router# show rtsp client session active
RTSP Session ID:0x8     Current Status:RTSP_STATUS_PLAYING
Associated CallID:0xF
Active Request:RTSP_API_REQ_PLAY
Control Protocol:TCP     Data Protocol:RTP
Total Packets Transmitted:0 (0 bytes)
Total Packets Received:708 (226560 bytes)
Cumulative Elapsed Play   Time:00:00:28.296
Cumulative Elapsed Record Time:00:00:00.000
        Session ID:0x8     State:ACTIVE
        Local  IP Address:10.13.79.45     Local  Port 16660
        Server IP Address:10.13.79.6     Server Port 11046
        Stream URL:rtsp://rtsp-cisco.cisco.com:554/chinna.au/streamid=0
        Packets Transmitted:0 (0 bytes)
        Packets Received:708 (226560 bytes)
        Elapsed Play   Time:00:00:28.296
        Elapsed  Record Time:00:00:00.000
        ReceiveDelay:85     LostPackets:0
```

The following is sample output from the **show rtsp client session history detailed** command:

```
Router# show rtsp client session history detailed
RTSP Session ID:0x8
Associated CallID:0xF
Control Protocol:TCP     Data Protocol:RTP
Total Packets Transmitted:0 (0 bytes)
Total Packets Received:2398 (767360 bytes)
Cumulative Elapsed Play   Time:00:01:35.916
Cumulative Elapsed Record Time:00:00:00.000
        Session ID:0x8     State:INACTIVE
        Local  IP Address:10.13.79.45     Local  Port 16660
        Server IP Address:10.13.79.6     Server Port 11046
        Stream URL:rtsp://rtsp-cisco.cisco.com:554/chinna.au/streamid=0
        Packets Transmitted:0 (0 bytes)
        Packets Received:2398 (767360 bytes)
        Play   Time:00:01:35.916
        Record Time:00:00:00.000
        OntimeRcvPlayout:93650
        GapFillWithSilence:0
        GapFillWithPrediction:70
        GapFillWithInterpolation:0
        GapFillWithRedundancy:0
        HighWaterPlayoutDelay:85
        LoWaterPlayoutDelay:64
        ReceiveDelay:85     LostPackets:0
        EarlyPackets:2     LatePackets:12
```

The table below describes significant fields shown in this output.

Table 18: show rtsp client session Field Descriptions

Field	Description
RTSP Session ID:0x8	Unique ID for the RTSP session.

Field	Description
Current Status:RTSP_STATUS_PLAYING	Current status: • RTSP_STATUS_SESSION_IDLE • RTSP_STATUS_SERVER_CONNECTED • RTSP_STATUS_PLAY_PAUSED • RTSP_STATUS_PLAY_COMPLETE
Associated CallID:0xF	ID of associated call.
Control Protocol:TCP	Transport protocol.
Data Protocol:RTP	Data protocol.
Total Packets Transmitted:0 (0 bytes)	Bytes sent out to the RTSP server.
Total Packets Received:708 (226560 bytes)	Bytes received from the server for playing.

Related Commands

Command	Description
rtsp client session history duration	Specifies the length of time for which the RTSP is kept during the session.
rtsp client session history records	Specifies the number of RTSP client session history records during the session.

show rudpv0 failures

To display SS7 Reliable User Datagram Protocol (RUDP) failure statistics, use the **show rudpv0 failures** command in privileged EXEC mode.

show rudpv0 failures

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following is sample output from this command showing displaying RUDP failures.

```
Router# show rudpv0 failures
**** RUDP Failure Stats ****
CreateBufHdrsFailure       0
CreateConnRecsFailure      0
CreateEventsFailure        0
NotReadyFailures           0
OptionNotSupportedFailures 0
OptionRequiredFailures     0
GetConnRecFailures         0
InvalidConnFailures        0
EventUnavailFailures       0
EmptyBufferSendFailures    0
BufferTooLargeFailures     0
ConnNotOpenFailures        0
SendWindowFullFailures     0
GetBufHdrSendFailures      0
GetDataBufFailures         0
GetBufHdrFailures          0
SendEackFailures           0
SendAckFailures            0
SendSynFailures            0
SendRstFailures            0
SendNullFailures           0
TimerNullFailures          0
FailedRetransmits          0
IncomingPktsDropped        0
UnknownRudpEvents          0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clear rudpv0 statistics	Resets the counters for the statistics generated by the **show rudpv0 failures** commandto 0.

Command	Description
show rudpv0 statistics	Displays RUDP information about number of packets sent, received, and so forth.

show rudpv0 statistics

To display SS7 Reliable User Datagram Protocol (RUDP) internal statistics, use the **show rudpv0 statistics** command in privileged EXEC command.

show rudpv0 statistics

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Because statistics counters are continually updated, the cumulative total may not be exactly equal to individual connection counters. After a connection is reset, previous statistics are lost, so the current connection statistics reflect only instances of the RUDP connection since the last reset.

Cumulative statistics reflect counts since the router was rebooted or since the **clear rudpv0 statistics** command was used.

Examples

The following is sample output from this command displaying RUDP statistics and states for two connections. The fields are self-explanatory.

```
Router# show rudpv0 statistics
*** RUDP Internal Stats ****
Connection ID: 811641AC,   Current State: OPEN
RcvdInSeq                  1
RcvdOutOfSeq               0
SoftResets                 0
SoftResetsRcvd             0
TotalPacketsSent           4828
TotalPacketsReceived       4826
TotalDataBytesSent         0
TotalDataBytesReceived     4
TotalDataPacketsSent       0
TotalDataPacketsReceived   1
TotalPacketsRetrans        0
TotalPacketsDiscarded      0
Connection ID: 81163FD4,   Current State: OPEN
RcvdInSeq                  2265
RcvdOutOfSeq               0
SoftResets                 0
SoftResetsRcvd             0
TotalPacketsSent           7863
TotalPacketsReceived       6755
TotalDataBytesSent         173690
TotalDataBytesReceived     56121
TotalDataPacketsSent       2695
TotalDataPacketsReceived   2265
```

```
TotalPacketsRetrans        0
TotalPacketsDiscarded      0
Cumulative RudpV0 Statistics
RcvdInSeq                  2266
RcvdOutOfSeq               0
SoftResets                 0
SoftResetsRcvd             0
TotalPacketsSent           12691
TotalPacketsReceived       11581
TotalDataBytesSent         173690
TotalDataBytesReceived     56125
TotalDataPacketsSent       2695
TotalDataPacketsReceived   2266
TotalPacketsRetrans        0
TotalPacketsDiscarded      0
```

Related Commands

Command	Description
clear rudpv0 statistics	Resets the counters for the statistics generated by the **show rudpv0 statistics** command to 0.
show rudpv0 failures	Displays RUDP information about failed connections and the reasons for them.

show rudpv1

To display Reliable User Datagram Protocol (RUDP) information, use the **show rudpv1** command in privileged EXEC mode.

show rudpv1 {**failures** | **parameters** | **statistics**}

Syntax Description

failures	RUDP failure statistics.
parameters	RUDP connection parameters.
statistics	RUDP internal statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco IAD2420 series.

Usage Guidelines

Because statistics counters are continually updated, the cumulative total may not be exactly equal to individual connection counters. After a connection is reset, previous statistics are lost, so the current connection statistics reflect only instances of the RUDP connection since the last reset.

Cumulative statistics reflect counts since the router was rebooted or since the **clear rudpv1 statistics** command was used.

Examples

The following is sample output from this command:

```
Router# show rudpv1 failures
**** RUDPV1 Failure Stats ****
CreateBufHdrsFailure       0
CreateConnRecsFailure      0
CreateEventQueueFailure    0
OsSpecificInitFailure      0
NotReadyFailures           0
OptionNotSupportedFailures 0
InvalidOptionFailures      0
OptionRequiredFailures     0
GetConnRecFailures         0
InvalidConnFailures        0
EventUnavailFailures       0
GetConnRecFailures         0
```

```
FindConnRecFailures        0
EmptyBufferSendFailures    0
BufferTooLargeFailures     0
ConnNotOpenFailures        0
SendWindowFullFailures     0
GetBufHdrSendFailures      0
SendInProgressFailures     0
GetDataBufFailures         0
GetBufHdrFailures          0
SendFailures               0
SendEackFailures           0
SendAckFailures            0
SendSynFailures            0
SendRstFailures            0
SendTcsFailures            0
SendNullFailures           0
TimerFailures              0
ApplQueueFailures          0
FailedRetransmits          0
IncomingPktsDropped        0
CksumErrors                0
UnknownRudpv1Events        0
InvalidVersion             0
InvalidNegotiation         0
```

The following is sample output from the **show rudpv1 parameters** command:

```
Router# show rudpv1 parameters
*** RUDPV1 Connection Parameters ***
Next Connection Id:61F72B6C,  Remote conn id 126000
  Conn State              OPEN
  Conn Type               ACTIVE
  Accept Negot params?    Yes
  Receive Window          32
  Send Window             32
  Receive Seg Size        384
  Send Seg Size           384
                      Requested     Negotiated
  Max Auto Reset          5             5
  Max Cum Ack             3             3
  Max Retrans             2             2
  Max OutOfSeq            3             3
  Cum Ack Timeout       100           100
  Retrans Timeout       300           300
  Null Seg Timeout      1000          1000
  Trans State Timeout   2000          2000
  Cksum type              Hdr           Hdr
Next Connection Id:61F72DAC,  Remote conn id 126218
  Conn State              OPEN
  Conn Type               ACTIVE
  Accept Negot params?    Yes
  Receive Window          32
  Send Window             32
  Receive Seg Size        384
  Send Seg Size           384
                      Requested     Negotiated
  Max Auto Reset          5             5
  Max Cum Ack             3             3
  Max Retrans             2             2
  Max OutOfSeq            3             3
  Cum Ack Timeout       100           100
  Retrans Timeout       300           300
  Null Seg Timeout      1000          1000
```

```
  Trans State Timeout   2000          2000
  Cksum type             Hdr           Hdr
```

The following is sample output from **the show rudpv1 statistics** command:

```
Router# show rudpv1 statistics
*** RUDPV1 Internal Stats ****
Connection ID:61F72B6C,   Current State:OPEN
RcvdInSeq                  647
RcvdOutOfSeq               95
AutoResets                 0
AutoResetsRcvd             0
TotalPacketsSent           1011
TotalPacketsReceived       958
TotalDataBytesSent         17808
TotalDataBytesReceived     17808
TotalDataPacketsSent       742
TotalDataPacketsReceived   742
TotalPacketsRetrans        117
TotalPacketsDiscarded      38
Connection ID:61F72DAC,   Current State:OPEN
RcvdInSeq                  0
RcvdOutOfSeq               0
AutoResets                 0
AutoResetsRcvd             0
TotalPacketsSent           75
TotalPacketsReceived       75
TotalDataBytesSent         0
TotalDataBytesReceived     0
TotalDataPacketsSent       0
TotalDataPacketsReceived   0
TotalPacketsRetrans        0
TotalPacketsDiscarded      0
Cumulative RudpV1 Statistics
NumCurConnections          2
RcvdInSeq                  652
RcvdOutOfSeq               95
AutoResets                 0
AutoResetsRcvd             0
TotalPacketsSent           1102
TotalPacketsReceived       1047
TotalDataBytesSent         18048
TotalDataBytesReceived     18048
TotalDataPacketsSent       752
TotalDataPacketsReceived   752
TotalPacketsRetrans        122
TotalPacketsDiscarded      38
```

Related Commands

Command	Description
clear rudpv1 statistics	Clears the RUDP statistics counters.
debug rudpv1	Displays debugging information for RUDP.

show sccp

To display Skinny Client Control Protocol (SCCP) information such as administrative and operational status, use the **show sccp** command in user EXEC or privileged EXEC mode.

show sccp [**all** | **ccm group** [*number*] | **connections** [**details** | **internal** | **rsvp** | **summary**] | **server** | **statistics** | **call-identifications** | **call-references**]

Syntax Description

all	(Optional) Specifies all Skinny Client Control Protocol (SCCP) global information.
ccm	(Optional) Displays SCCP Cisco Unified Communications Manager (CUCM) group related information.
group	(Optional) Displays CUCM groups.
number	(Optional) CUCM group number that needs to be displayed.
connections	(Optional) Specifies information about the connections controlled by the SCCP transcoding and conferencing applications.
details	(Optional) Displays SCCP connections in detail.
internal	(Optional) Displays information about SCCP internal connections.
rsvp	(Optional) Displays Resource Reservation Protocol (RSVP) information about SCCP connections.
summary	(Optional) Displays information about SCCP connections.
server	(Optional) Displays SCCP server information.
statistics	(Optional) Specifies statistical information for SCCP transcoding and conferencing applications.
call-identifications	(Optional) Displays the following identification numbers that is associated with each leg of a call: • Session • Call Reference • Connection • Call • Bridge • Profile
call-references	(Optional) Displays codec, port, ID numbers for each leg of a call.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(6)T	This command was modified. The **rsvp**keyword was added.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.
12.3(8)T	This command was modified. The following keywords and arguments were added: **ccm**, **connections**, **details**, **group**, **internal,** *number,* **summary**.
12.4(11)XW1	This command was modified. The stype field was added to the show output to show whether a connections is encrypted.
12.4(15)XY	This command was modified. The **statistics** and **server**keywords were added.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information and it was integrated into Cisco IOS Release 12.2(13)T.
15.1(4)M	This command was modified. The **call-identifications** and **call-references** keywords were added.

Usage Guidelines

The router on which you use the **show sccp** command must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital signal processor (DSP) resources.

Use the **show sccp ccm** group command to show detailed information about all groups assigned to the Cisco Unified CallManager. The optional group-number argument can be added to select details about a specific group.

Configure the **show sccp server statistics** command on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller where no SCCP phone is registered, to show the statistical counts on the SCCP server. The counts display queuing errors and message drops on the transcoder alone when it is on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller.

When the **show sccp server statistics** command is used on the Cisco Unified Manager Express (CME), it is recommended for use together with the clear sccp server statistics command.

Examples

In the following sample output, the gateway IP address can be an IPv4 or IPv6 address when it operates on an IPv4/IPv6 dual stack.

```
Router# show sccp
SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/0
        IPv6 Address: 2001:DB8:C18:1::3
        IPv4 Address: 10.4.34.100
        Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 172.19.242.27, Port Number: 2000
```

```
                Priority: N/A, Version: 5.0.1, Identifier: 4
                Trustpoint: N/A
Call Manager: 2001:DB8:C18:1::100, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 1
                Trustpoint: N/A
```

The table below describes the significant fields shown in the display.

Table 19: show sccp Field Descriptions

Field	Description
SCCP Admin State	Current state of the SCCP session.
Gateway Local Interface	Local interface that SCCP applications use to register with Cisco Unified Communications Manager.
IP precedence	Sets the IP precedence value for SCCP.
User Masked Codec list	Codec to mask.
Call Manager	Cisco Unified CallManager server information.

The following is sample output from this command for IPv4 only. The field descriptions are self-explanatory.

```
Router# show sccp
SCCP Admin State: UP
Gateway IP Address: 10.10.10.11, Port Number: 0
Switchover Method: IMMEDIATE, Switchback Method: GUARD_TIMER
Switchback Guard Timer: 1200 sec, IP Precedence: 5
Max Supported MTP sessions: 100
Transcoding Oper State: ACTIVE - Cause Code: NONE
Active CallManager: 10.10.10.35, Port Number: 2000
TCP Link Status: CONNECTED
Conferencing Oper State: DOWN - Cause Code: DSPFARM_DOWN
Active CallManager: NONE
TCP Link Status: NOT_CONNECTED
CallManager: 10.10.10.37, Port Number: 2000
Priority: 3, Version: 3.1
CallManager: 10.10.10.35, Port Number: 2000
Priority: 2, Version: 3.0
```

The following sample shows statistical information for SCCP transcoding and conferencing applications.

```
Router# show sccp statistics
SCCP Transcoding Application Statistics:
TCP packets rx 548, tx 559
Unsupported pkts rx 3, Unrecognized pkts rx 0
Register tx 3, successful 3, rejected 0, failed 0
KeepAlive tx 543, successful 540, failed 2
OpenReceiveChannel rx 2, successful 2, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 2, successful 2, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 1, Switchback 1
SCCP Conferencing Application Statistics:
TCP packets rx 0, tx 0
```

```
Unsupported pkts rx 0, Unrecognized pkts rx 0
Register tx 0, successful 0, rejected 0, failed 0
KeepAlive tx 0, successful 0, failed 0
OpenReceiveChannel rx 0, successful 0, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 0, successful 0, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 0, Switchback 0
```

In the following example, the secure value of the stype field indicates that the conection is encrypted. The field descriptions are self-explanatory.

```
Router# show sccp connections
sess_id    conn_id    stype        mode codec   ripaddr       rport sport
16777222   16777409   secure-xcode sendrecv g729b   10.3.56.120   16772 19534
16777222   16777393   secure-xcode sendrecv g711u   10.3.56.50    17030 18464
Total number of active session(s) 1, and connection(s) 2
```

The following example shows the remote IP addresses of active RTP sessions, each of which shows either an IPv4 or an IPv6 address.

```
Router# show sccp connections
sess_id  conn_id  stype  mode    codec sport rport ripaddr
16777219 16777245 conf  sendrecv g711u 16516 27814 10.3.43.46
16777219 16777242 conf  sendrecv g711u 17712 18028 10.3.43.2
16777219 16777232 conf  sendrecv g711u 16890 19440 10.3.43.2
16777219 16777228 conf  sendrecv g711u 19452 17464 10.3.43.2
16777220 16777229 xcode sendrecv g711u 17464 19452 10.3.43.2
16777220 16777227 xcode sendrecv g729b 19466 19434 2001:0DB8:C18:1:212:79FF:FED7:B254
16777221 16777233 mtp   sendrecv g711u 19440 16890 10.3.43.2
16777221 16777231 mtp   sendrecv g711u 17698 17426 2001:0DB8:C18:1:212:79FF:FED7:B254
16777223 16777243 mtp   sendrecv g711u 18028 17712 10.3.43.2
16777223 16777241 mtp   sendrecv g711u 16588 19446 2001:0DB8:C18:1:212:79FF:FED7:B254
```

The following is sample output for the two Cisco CallManager Groups assigned to the Cisco Unified CallManager: group 5 named "boston office" and group 988 named "atlanta office".

```
Router# show sccp ccm group
CCM Group Identifier: 5
 Description: boston office
 Binded Interface: NONE, IP Address: NONE
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 3, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 1200 sec
 Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
 Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
 Signaling DSCP value: default, Audio DSCP value: default
CCM Group Identifier: 988
 Description: atlanta office
 Binded Interface: NONE, IP Address: NONE
 Associated CCM Id: 1, Priority in this CCM Group: 1
 Associated Profile: 6, Registration Name: MTP123456789988
 Associated Profile: 10, Registration Name: CFB123456789966
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 5, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 10 sec
 Switchover Method: IMMEDIATE, Switchback Method: IMMEDIATE
 Switchback Interval: 15 sec, Switchback Timeout: 0 sec
 Signaling DSCP value: default, Audio DSCP value: default
```

The table below describes the significant fields shown in the display.

Table 20: show sccp ccm group Field Descriptions

Field	Description
CCM Group Identifier	Current state of the SCCP session.
Description	Local interface that SCCP applications use to register with Cisco Unified Communications Manager.
Binded Interface	Sets the IP precedence value for SCCP.
Registration Retries	Codec to mask.
Registration Timeout	Cisco Unified CallManager server information.
Keepalive Retries	Displays the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager.
Keepalive Timeout	Displays the number of times that a DSP farm attempts to connect to a Cisco Unified CallManager.
CCM Connect Retries	Displays the amount of time, in seconds, that a given DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
CCM Connect Interval	Method that the SCCP client uses when the communication link between the active Cisco Unified CallManager and the SCCP client fails.
Switchover Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Interval	Amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails.
Switchback Timeout	Amount of time, in seconds, that the secondary Cisco Unified CallManager waits before switching back to the primary Cisco Unified CallManager.
Associated CCM Id	Number assigned to the Cisco Unified CallManager.
Registration Name	User-specified device name in Cisco Unified CallManager.
Associated Profile	Number of the DSP farm profile associated with the Cisco Unified CallManager group.

The following sample output displays the summary information for all SCCP call references:

```
Router# show sccp call-reference
session_id: 16805277   session_type: vcf  , profile_id: 101,
    call-reference: 25666614  , Name: , Number: 3004
        Audio conn_id: 16777929  , str_passthr: 0
              rtp-call-id: 21        , bridge-id: 15        , msp-call-id: 12
              mode: sendrecv, sport: 25146, rport 16648, ripaddr: 10.22.82.205
```

```
              codec: g711u  , pkt-period: 20
    call-reference: 25666611  , Name: , Number: 6628
        Audio conn_id: 16777926  , str_passthr: 0
              rtp-call-id: 19        , bridge-id: 13        , msp-call-id: 12
              mode: sendrecv, sport: 28168, rport 2398 , ripaddr: 128.107.147.125
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777927  , conn_id_tx: 16777928  , str_passthr: 0
              rtp-call-id: 20        , bridge-id: 14        , msp-call-id: 12
              mode: sendrecv, sport: 22604, rport 2400 , ripaddr: 128.107.147.125
              bit rate: 1100kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 2.2, max mbps: 81 (x500 MB/s), max fs: 7
(x256 MBs)
    call-reference: 25666608  , Name: , Number: 62783365
        Audio conn_id: 16777923  , str_passthr: 0
              rtp-call-id: 16        , bridge-id: 11        , msp-call-id: 12
              mode: sendrecv, sport: 21490, rport 20590, ripaddr: 10.22.83.142
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777924  , conn_id_tx: 16777925  , str_passthr: 0
              rtp-call-id: 17        , bridge-id: 12        , msp-call-id: 12
              mode: sendrecv, sport: 23868, rport 29010, ripaddr: 10.22.83.142
              bit rate: 960kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 3.0, max mbps: 0 (x500 MB/s), max fs: 0
(x256 MBs)
    call-reference: 25666602  , Name: , Number: 62783363
        Audio conn_id: 16777916  , str_passthr: 0
              rtp-call-id: 11        , bridge-id: 7         , msp-call-id: 12
              mode: sendrecv, sport: 26940, rport 20672, ripaddr: 10.22.82.48
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777917  , conn_id_tx: 16777919  , str_passthr: 0
              rtp-call-id: 13        , bridge-id: 8         , msp-call-id: 12
              mode: sendrecv, sport: 16462, rport 20680, ripaddr: 10.22.82.48
              bit rate: 960kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 2.0, max mbps: 72 (x500 MB/s), max fs: 5
(x256 MBs)
Total number of active session(s) 1
   Total of number of active session(s) 1
      with total of number of call-reference(s) 4
         with total of number of audio connection(s) 4
         with total of number of video connection(s) 3
```

The following sample output displays summary information for all SCCP call identifications:

```
Router# show sccp call-identifications
sess_id   callref   conn_id   conn_id_tx spid  rtp_callid msp_callid bridge_id  codec  stype
 prof_id
16805277  25666614  16777929  0          0     21         12         15         g711u  vcf
   101
16805277  25666611  16777926  0          0     19         12         13         g711u  vcf
   101
16805277  25666611  16777927  16777928   0     20         12         14         h264   vcf
   101
16805277  25666608  16777923  0          0     16         12         11         g711u  vcf
   101
16805277  25666608  16777924  16777925   0     17         12         12         h264   vcf
   101
16805277  25666602  16777916  0          0     11         12         7          g711u  vcf
   101
16805277  25666602  16777917  16777919   0     13         12         8          h264   vcf
   101
Total number of active session(s) 1
```

The following sample displays the output from show sccp:

```
Router# show sccp
SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/1
        IPv4 Address: 172.19.156.7
        Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 1.4.211.39, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 1
                Trustpoint: N/A
Call Manager: 128.107.151.39, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 100
                Trustpoint: N/A
V_Conferencing Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 128.107.151.39, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 101
Reported Max Streams: 4, Reported Max OOS Streams: 0
Layout: default 1x1
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
Supported Codec: g729r8, Maximum Packetization Period: 60
Supported Codec: g729br8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30
Supported Codec: h264: QCIF, Frame Rate: 15fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: QCIF, Frame Rate: 30fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: CIF, Frame Rate: 15fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: CIF, Frame Rate: 30fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: 4CIF, Frame Rate: 30fps, Bit Rate: 1000-1000 Kbps
TLS : ENABLED
```

Related Commands

Command	Description
dsp service dspfarm	Configures DSP farm services for a specified voice card.
dspfarm (DSP farm)	Enables DSP-farm service.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show dspfarm	Displays summary information about DSP resources.

show sccp ccm group

To display the groups that are configured on a specific Cisco Unified CallManager, use the **show sccp ccm group**command in privileged EXEC mode.

show sccp ccm group [*group-number*]

Syntax Description

group-number	(Optional) Number that identifies the Cisco CallManager group. Range is 1 to 65535. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **show sccp ccm group** command to show detailed information about all groups assigned to the Cisco Unified CallManager. The optional *group-number* argument can be added to select details about a specific group.

Examples

The following is sample output for the two Cisco CallManager Groups assigned to the Cisco Unified CallManager: group 5 named "boston office" and group 988 named "atlanta office".

```
Router# show sccp ccm group
CCM Group Identifier: 5
 Description: boston office
 Binded Interface: NONE, IP Address: NONE
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 3, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 1200 sec
 Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
 Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
 Signaling DSCP value: default, Audio DSCP value: default
CCM Group Identifier: 988
 Description: atlanta office
 Binded Interface: NONE, IP Address: NONE
 Associated CCM Id: 1, Priority in this CCM Group: 1
 Associated Profile: 6, Registration Name: MTP123456789988
 Associated Profile: 10, Registration Name: CFB123456789966
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 5, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 10 sec
 Switchover Method: IMMEDIATE, Switchback Method: IMMEDIATE
 Switchback Interval: 15 sec, Switchback Timeout: 0 sec
 Signaling DSCP value: default, Audio DSCP value: default
```

The table below describes significant fields shown in this output.

Table 21: show sccp ccm group Field Descriptions

Field	Description
CCM Group Identifier	Displays the Cisco CallManager group number.
Description	Displays the optional description of the group assigned to the group number.
Binded Interface	Displays the IP address of the selected interface is used for all calls within a given profile.
Registration Retries	Number of times that SCCP tries to register with a Cisco Unified CallManger
Registration Timeout	Length of time, in seconds, between registration messages sent from SCCP to the Cisco Unified CallManager.
Keepalive Retries	Displays the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager.
Keepalive Timeout	Displays the length of time, in seconds, between keepalive retries.
CCM Connect Retries	Displays the number of times that a DSP farm attempts to connect to a Cisco Unified CallManager.
CCM Connect Interval	Displays the amount of time, in seconds, that a given DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
Switchover Method	Method that the SCCP client uses when the communication link between the active Cisco Unified CallManager and the SCCP client fails.
Switchback Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Interval	Amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails.
Switchback Timeout	Amount of time, in seconds, that the secondary Cisco Unified CallManager waits before switching back to the primary Cisco Unified CallManager.
Associated CCM Id	Number assigned to the Cisco Unified CallManager.
Registration Name	User-specified device name in Cisco Unified CallManager.
Associated Profile	Number of the DSP farm profile associated with the Cisco Unified CallManager group.

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco Unified CallManager server to the list of available servers.

show sccp connections details

To display Skinny Client Control Protocol (SCCP) connection details such as call-leg details, use the **show sccp connections details** command in privileged EXEC mode.

show sccp connections details

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections details
bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)
sess_id    conn_id    call-id    codec   pkt-period type      bridge-info(bid, cid)
mmbridge-info(bid, cid)
16800395   -          15         N/A     N/A        transmsp  All RTPSPI Callegs      N/A

16800395   18425889   14         g711u   20         rtpspi    (10,15)                 N/A

16800395   18425905   13         g711u   20         rtpspi    (9,15)                  N/A

Total number of active session(s) 1, connection(s) 2, and callegs 3
```

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.
show sccp connections internal	Displays the internal SCCP details.
show sccp connections summary	Displays a summary of the number of SCCP sessions and connections.

show sccp connections internal

To display the internal Skinny Client Control Protocol (SCCP) details such as time-stamp values, use the **show sccp connections internal**command in privileged EXEC mode.

show sccp connections internal

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections internal
Total number of active session(s) 0, and connection(s) 0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.
show sccp connections details	Displays the SCCP connection details.
show sccp connections summary	Displays a summary of the number of SCCP sessions and connections.

show sccp connections rsvp

To display information about active Skinny Client Control Protocol (SCCP) connections that are using RSVP, use the **show sccp connections rsvp** command in privileged EXEC mode.

show sccp connections rsvp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from this command:

```
Router# show sccp connections rsvp
sess_id    conn_id    rsvp_id    dir  local ip       :port  remote ip      :port
16777578   16778093   -210       SEND 192.168.21.1   :18486 192.168.20.1   :16454
16777578   16778093   -211       RECV 192.168.21.1   :18486 192.168.20.1   :16454

 Total active sessions 1, connections 2, rsvp sessions 2
```

The table below describes the fields shown in the display.

Table 22: show sccp connections rsvp Field Descriptions

Field	Description
sess_id	Identification number of the SCCP session.
conn_id	Identification number of the SCCP connection.
rsvp_id	Identification number of the RSVP connection.
dir	Direction of the SCCP connection.
local ip	IP address of the local endpoint.
remote ip	IP address of the remote endpoint.
port	Port number of the local or remote endpoint.
Total active sessions	Total number of active SCCP sessions.
connections	Number of active connections that are a part of the SCCP sessions.
rsvp session	Number of active connections that use RSVP.

Related Commands

Command	Description
debug sccp all	Displays debugging information for SCCP.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
rsvp	Enables RSVP support on a transcoding or MTP device.
sccp	Enables SCCP on the interface.
sccp local	Selects the local interface that SCCP applications use to register with Cisco Unified CallManager.
show sccp connections summary	Displays a summary of the number of SCCP sessions and connections.

show sccp connections summary

To display a summary of the number of sessions and connections based on the service type under the Skinny Client Control Protocol (SCCP) application, use the **show sccp connections summary** command in privileged EXEC mode.

show sccp connections summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections summary
SCCP Application Service(s) Statistics Summary:
Total Conferencing Sessions: 0, Connections: 0
Total Transcoding Sessions: 0, Connections: 0
Total MTP Sessions: 0, Connections: 0
Total SCCP Sessions: 0, Connections: 0
```

The table below describes significant fields shown in this output.

Table 23: show sccp connections summary Field Descriptions

Field	Description
Connections	Displays the total number of current connections associated with a given application.
Total Conferencing Sessions	Displays the number of current conferencing sessions.
Total MTP Sessions	Displays the number of current Media Termination Point (MTP) sessions.
Total SCCP Sessions	Displays the number of current SCCP sessions.
Total Transcoding Sessions	Displays the number of current transcoding sessions.

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.

Command	Description
show sccp connections details	Displays the SCCP connection details.
show sccp connections internal	Displays the internal SCCP details.

show sccp server statistics

To display the statistical counts on the Skinny Client Control Protocol (SCCP) server, use the **show sccp server statistics** command in privileged EXEC mode.

show sccp server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.

Usage Guidelines

Configure the **show sccp server statistics** command on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller where no SCCP phone is registered, to show the statistical counts on the SCCP server. The counts display queuing errors and message drops on the transcoder alone when it is on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller.

When the **show sccp server statistics** command is used on the Cisco Unified Manager Express (CME), it is recommended for use together with the **clear sccp server statistics**command.

Examples

The following example shows the SCCP statistical counts on the server:

```
Router# show sccp server statistics
Failure type              Error count
------------------------  -----------
Send queue enqueue        2
Socket send               3
Msg discarded upon error  5
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clear sccp server statistics	Clears the counts displayed the **under show sccp server statistics** command.

show sdspfarm

To display the status of the configured digital signal processor (DSP) farms and transcoding streams, use the **show sdspfarm**command in privileged EXEC mode.

show sdspfarm {**units** [**name** *unit-name* | **register** | **summary** | **tag** *number* | **unregister**] | **sessions** [**active** | **callID** *number* | **states** | **statistics** | **streamID** *number* | **summary**] | **message statistics**} [**video**]

Syntax Description

units	Displays the configured and registered DSP farms.
name *unit-name*	(Optional) Displays the name of the unit.
register	(Optional) Displays information about the registered units.
summary	(Optional) Displays summary information about the units.
tag *number*	(Optional) Displays the tag number of the unit.
unregister	(Optional) Displays information about the unregistered units.
sessions	Displays the transcoding streams.
active	(Optional) Displays all active sessions.
callID	(Optional) Displays activities for a specific caller ID.
number	(Optional) The caller ID number displayed by the **show voip rtp connection** command.
states	(Optional) Displays the current state of the transcoding stream.
statistics	(Optional) Displays session statistics.
streamID *number*	(Optional) Displays the transcoding stream sequence number.
summary	(Optional) Displays summary information.
message	Displays message information.
statistics	Displays statistics information about the messages.
video	(Optional) Displays information on video streams.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(22)T	The following combinations of keywords and arguments were added: **name**, *unit-name*, **register**, **summary**, **tag** *number*, **unregister**, **states**, **streamID** *number*, **message statistics**.

Release	Modification
15.1(4)M	The **video** keyword was added.

Examples

The following example displays the configured and registered DSP farms:

```
Router# show sdspfarm units
mtp-1 Device:MTP123456782012 TCP socket:[-1]  UNREGISTERED
actual_stream:0 max_stream 0 IP:0.0.0.0  0  Unknown 0 keepalive 0
mtp-2 Device:MTP000a8aeaca80 TCP socket:[5]  REGISTERED
actual_stream:40 max_stream 40 IP:10.5.49.160  11001  MTP YOKO keepalive 12074
Supported codec:G711Ulaw
                 G711Alaw
                 G729
                 G729a
                 G729b
                 G729ab
 max-mtps:2, max-streams:240, alloc-streams:40, act-streams:0
```

The following is sample output from the **show sdspfarm sessions active**command:

```
Router# show sdspfarm sessions active
Stream-ID:3 mtp:2 192.0.2.0 20174  Local:2000 START
 usage:MoH  (DN=3  , CH=1) FE=TRUE
 codec:G729  duration:20 vad:0 peer Stream-ID:4
Stream-ID:4 mtp:2 192.0.2.0 17072  Local:2000 START
 usage:MoH  (DN=3  , CH=1) FE=FALSE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:3
```

The following is sample output from the **show sdspfarm sessions callID**command:

```
Router# show sdspfarm sessions callID 51
Stream-ID:6, srcCall-ID:51, codec:G729AnnexA , dur:20ms, vad:0, dstCall-ID:52, confID:5,
mtp:2^
Peer Stream-ID:5, srcCall-ID:52, codec:G711Ulaw64k , dur:20ms, vad:0, dstCall-ID:51, confID:5,
 mtp:2^
Router-2015# show sdspfarm sessions callid 52
Stream-ID:5, srcCall-ID:52, codec:G711Ulaw64k , dur:20ms, vad:0, dstCall-ID:51, confID:5,
mtp:2
Peer Stream-ID:6, srcCall-ID:51, codec:G729AnnexA , dur:20ms, vad:0, dstCall-ID:52, confID:5,
 mtp:2
```

The following is sample output from the **show sdspfarm sessions statistics**command:

```
Router# show sdspfarm sessions statistics
Stream-ID:1 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:1014 in-pak:0 discard:0
Stream-ID:2 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:3 mtp:2 10.5.49.160  20174  Local:2000START  MoH  (DN=3  , CH=1) FE=TRUE
 codec:G729  duration:20 vad:0 peer Stream-ID:4
 recv-pak:0 xmit-pak:0 out-pak:4780 in-pak:0 discard:0
Stream-ID:4 mtp:2 10.5.49.160  17072  Local:2000START  MoH  (DN=3  , CH=1) FE=FALSE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:3
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:5 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
```

```
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:6 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:7 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:8 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:9 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:10 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:11 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:12 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:13 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:14 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:15 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:16 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:17 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:18 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:19 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:20 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:21 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:22 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:23 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:24 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:25 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:26 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
```

```
Stream-ID:27 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:28 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:29 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:30 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:31 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:32 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:33 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:34 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:35 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:36 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:37 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:38 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:39 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:40 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
```

The following is sample output from the **show sdspfarm sessions summary**command:

```
Router# show sdspfarm sessions summary
max-mtps:2, max-streams:240, alloc-streams:40, act-streams:2
  ID   MTP  State      CallID confID Usage                         Codec/Duration
==== ===== ====== =========== ====== ============================= ==============
1    2     IDLE   -1          0                                  G711Ulaw64k /20ms
2    2     IDLE   -1          0                                  G711Ulaw64k /20ms
3    2     START  -1          3      MoH  (DN=3   , CH=1) FE=TRUE  G729 /20ms
4    2     START  -1          3      MoH  (DN=3   , CH=1) FE=FALSE G711Ulaw64k /20ms
5    2     IDLE   -1          0                                  G711Ulaw64k /20ms
6    2     IDLE   -1          0                                  G711Ulaw64k /20ms
7    2     IDLE   -1          0                                  G711Ulaw64k /20ms
8    2     IDLE   -1          0                                  G711Ulaw64k /20ms
9    2     IDLE   -1          0                                  G711Ulaw64k /20ms
10   2     IDLE   -1          0                                  G711Ulaw64k /20ms
11   2     IDLE   -1          0                                  G711Ulaw64k /20ms
12   2     IDLE   -1          0                                  G711Ulaw64k /20ms
13   2     IDLE   -1          0                                  G711Ulaw64k /20ms
14   2     IDLE   -1          0                                  G711Ulaw64k /20ms
15   2     IDLE   -1          0                                  G711Ulaw64k /20ms
```

```
16   2     IDLE   -1          0                                    G711Ulaw64k /20ms
17   2     IDLE   -1          0                                    G711Ulaw64k /20ms
18   2     IDLE   -1          0                                    G711Ulaw64k /20ms
19   2     IDLE   -1          0                                    G711Ulaw64k /20ms
20   2     IDLE   -1          0                                    G711Ulaw64k /20ms
21   2     IDLE   -1          0                                    G711Ulaw64k /20ms
22   2     IDLE   -1          0                                    G711Ulaw64k /20ms
23   2     IDLE   -1          0                                    G711Ulaw64k /20ms
24   2     IDLE   -1          0                                    G711Ulaw64k /20ms
25   2     IDLE   -1          0                                    G711Ulaw64k /20ms
26   2     IDLE   -1          0                                    G711Ulaw64k /20ms
27   2     IDLE   -1          0                                    G711Ulaw64k /20ms
28   2     IDLE   -1          0                                    G711Ulaw64k /20ms
29   2     IDLE   -1          0                                    G711Ulaw64k /20ms
30   2     IDLE   -1          0                                    G711Ulaw64k /20ms
31   2     IDLE   -1          0                                    G711Ulaw64k /20ms
32   2     IDLE   -1          0                                    G711Ulaw64k /20ms
33   2     IDLE   -1          0                                    G711Ulaw64k /20ms
34   2     IDLE   -1          0                                    G711Ulaw64k /20ms
35   2     IDLE   -1          0                                    G711Ulaw64k /20ms
36   2     IDLE   -1          0                                    G711Ulaw64k /20ms
37   2     IDLE   -1          0                                    G711Ulaw64k /20ms
38   2     IDLE   -1          0                                    G711Ulaw64k /20ms
39   2     IDLE   -1          0                                    G711Ulaw64k /20ms
40   2     IDLE   -1          0                                    G711Ulaw64k /20ms
```

The table below describes the fields shown in the **show sdspfarm** command display.

Table 24: show sdspfarm Field Descriptions

Field	Description
act-streams	Active streams that are involved in calls.
alloc-streams	Number of transcoding streams that are actually allocated to all DSP farms that are registered to Cisco CME.
callID	Caller ID that the active stream is in.
Codec	Codec in use.
confID	ConfID that is used to communicate with DSP farms.
discard	Number of packets that are discarded.
dstCall-ID	Caller ID of the destination IP call leg.
Duration or dur	Packet rates, in milliseconds.
ID	Transcoding stream sequence number in Cisco CME.
in-pak	Number of incoming packets from the source call leg.
Local	Local port for voice packets.
max-mtps	Maximum number of Message Transfer Parts (MTPs) that are allowed to register in Cisco CME.
max-streams	Maximum number of transcoding streams that are allowed in Cisco CME.

Field	Description
mtp or MTP	MTP sequence number where the transcoding stream is located.
out-pak	Number of outgoing packets sending to source call leg.
peer Stream-ID	Stream sequence number of the other stream paired in the same transcoding session. (Two transcoding streams make up a transcoding session).
recv-pak	Number of voice packets received from the DSP farm.
srcCall-ID	Source caller ID of the source IP call leg.
State	Current state of the transcoding stream; could be IDLE, SEIZE, START, STOP, or END.
Stream-ID	Transcoding stream sequence number in Cisco CME.
TCP socket	Socket number for DSP farm (similar to TCP socket for **show ephone** output).
usage	Current usage of the stream; for example, Ip-Ip (IP to IP transcoding), Moh (for MOH transcoding) and Conf (conference).
vad	Voice-activity detection (VAD) flag for the transcoding stream. It should always be 0 (False).
xmit-pak	Number of packets that are sent to the DSP farm.

Related Commands

Command	Description
sdspfarm tag	Permits a DSP farm to be to registered to Cisco CME and be associated with an SCCP client interface's MAC address.
sdspfarm transcode sessions	Specifies the maximum number of transcoding sessions allowed per Cisco CME router.
sdspfarm units	Specifies the maximum number of DSP farms that are allowed to be registered to Cisco CME.

show settlement

To display the configuration for all settlement servers and see specific provider and transactions, use the **show settlement** command in privileged EXEC mode.

show settlement [**provider-number** [**transactions**]]

Syntax Description

provider -number	(Optional) Displays the attributes of a specific provider.
transactions	(Optional) Displays the transaction status of a specific provider.

Command Default

Information about all servers is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following is sample output from this command displaying information about all settlement servers that are configured:

```
Router# show settlement
Settlement Provider 0
Type = osp
Address url = https://1.14.115.100:6556/
Encryption = all                (default)
Max Concurrent Connections = 20 (default)
Connection Timeout = 3600 (s)   (default)
Response Timeout = 1 (s)        (default)
Retry Delay = 2 (s)             (default)
Retry Limit = 1                 (default)
Session Timeout = 86400 (s)     (default)
Customer Id = 1000
Device Id = 1000
Roaming = Disabled              (default)
Signed Token = on
Number of Connections = 0
Number of Transactions = 7
```

The following is sample output from this command displaying transaction and state information about a specific settlement server:

```
Router# show settlement 0 transactions
Transaction ID=8796304133625270342
        state=OSPC_GET_DEST_SUCCESS, index=0
        callingNumber=5710868, calledNumber=15125551212
```

The table below describes significant fields shown in this output. Provider attributes that are not configured are not shown.

Table 25: show settlement Field Descriptions

Field	Description
type	Settlement provider type.
address url	URL address of the provider.
encryption	SSL encryption method.
max-connections	Maximum number of concurrent connections to provider.
connection-timeout	Connection timeout with provider (in seconds).
response-timeout	Response timeout with provider (in seconds).
retry-delay	Delay time between retries (in seconds).
retry-limit	Number of retries.
session-timeout	SSL session timeout (in seconds).
customer-id	Customer ID, assigned by provider.
device-id	Device ID, assigned by provider.
roaming	Roaming enabled.
signed-token	Indicates if the settlement token is signed by the server.

Related Commands

Command	Description
connection -timeout	Configures the time that a connection is maintained after a communication exchange is completed.
customer -id	Identifies a carrier or ISP with a settlement provider.
device -id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max -connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response -timeout	Configures the maximum time to wait for a response from a server.
retry -delay	Sets the time between attempts to connect with the settlement provider.
session -timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
type	Configures an SAA-RTR operation type.

show sgcp connection

To display all active Simple Gateway Control Protocol (SGCP) connections on a router, use the **show sgcp connection**command in EXEC mode.

show sgcp connection [**interface** *number*]

Syntax Description

interface	(Optional) Displays output for a particular DS1 interface.
number	(Optional) Interface (controller) number.

Command Default

All active SGCP connections on the host are displayed.

Command Modes

EXEC (>)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.

Examples

The following is sample output from thiscommand displaying active connections on a router:

```
Router# show sgcp connection
Endpoint        Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (E)vent[SIFL] (R)esult[EA]
1. ds1-0/1@r3810-5      C=1,1,2  I=0x1  P=16492,16476  M=3  S=4  E=3,0,0,3  R=0, 0
```

The following is sample output from thiscommand displaying the state of SGCP on a router:

```
Router# show sgcp connection
SGCP Admin State DOWN, Oper State DOWN
SGCP call-agent:
209.165.200.225
 , SGCP graceful-shutdown enabled? FALSE
SGCP request timeout 40, SGCP request retries 10
```

The table below describes significant fields shown in this output.

Table 26: show sgcp connection Field Descriptions

Field	Description
SGCP Admin State	Administrative and operational state of the SGCP daemon.
SGCP call-agent	Address of the call agent specified with the **sgcp** command.
SGCP graceful-shutdown enabled	The state of the **sgcp graceful-shutdown** command.

Field	Description
SGCP request timeout	The setting for the **sgcp request timeout** command.
SGCP request retries	The setting for the **sgcp request retries** command.

Related Commands

Command	Description
show sgcp endpoint	Displays SGCP endpoint information.
show sgcp statistics	Displays global statistics for the SGCP packet count, success, and failure counts.

show sgcp endpoint

To display Simple Gateway Control Protocol (SGCP) endpoints that are eligible for SGCP management, use the **show sgcp endpoint** command in EXEC mode.

show sgcp endpoint [**interface** *ds1* [*ds0*]]

Syntax Description

interface *ds1*	(Optional) DS1 interface for which to display SGCP endpoint information. Range is from 1 to 1000.
ds0	(Optional) DS0 interface for which to display SGCP endpoint information. Range is from 0 to 30.

Command Modes

EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.

Usage Guidelines

Use this command to display SGCP endpoint information for the whole router or for a specific DS1 interface and, optionally, a specific DS0. If you enter a nonexistent combination of a DS1 and DS0, the following error message appears: "No matching connection found."

Examples

The following is sample output from this command displaying SGCP endpoint information being set for a matching connection between DS1 interface 1 and DS0 interface 10:

```
Router# show sgcp endpoint interface 1 10
```

Related Commands

Command	Description
show sgcp connection	Displays all the active connections on the host router.
show sgcp statistics	Displays global statistics for the SGCP packet count, success, and failure counts.

show sgcp statistics

To display global statistics for the Simple Gateway Control Protocol (SGCP) packet count, success and failure counts, and other information, use the **show sgcp statistics** command in EXEC mode.

show sgcp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC (#)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.0(5)T	This command was implemented on the Cisco AS5300 only in a private release that was not generally available.

Usage Guidelines

You can filter the displayed output, as shown in the examples.

Examples

The following is sample output from this command displaying SGCP packet statistics:

```
Router# show sgcp statistics
UDP pkts rx 5, tx 13
Unrecognized rx pkts 0, SGCP message parsing errors 0
Duplicate SGCP ack tx 0
Failed to send SGCP messages 0
CreateConn rx 1, successful 1, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 3, successful 3, failed 0
Notify tx 3, successful 3, failed 0
ACK tx 4, NACK tx 0
ACK rx 1, NACK rx 0
IP address based Call Agents statistics:
IP address 1.4.63.100, Total msg rx 5,
                   successful 5, failed 2
```

The following is sample output from this command showing how to filter output for specific information:

```
Router# show sgcp statistics | begin Failed
Failed to send SGCP messages 0
CreateConn rx 0, successful 0, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 0, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 0, NACK tx 0
ACK rx 0, NACK rx 0
```

```
Router# show sgcp statistics | exclude ACK
UDP pkts rx 0, tx 0
Unrecognized rx pkts 0, SGCP message parsing errors 0
Duplicate SGCP ack tx 0
Failed to send SGCP messages 0
CreateConn rx 0, successful 0, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 0, failed 0
Notify tx 0, successful 0, failed 0
Router# show sgcp statistics | include ACK
ACK tx 0, NACK tx 0
ACK rx 0, NACK rx 0
```

Related Commands

Command	Description
show sgcp connection	Displays all the active connections on the host Cisco AS5300 universal access server.
show sgcp endpoint	Displays SGCP endpoint information.

show shared-line

To display information about the Session Initiation Protocol (SIP) shared lines, use the **show shared-line** command in user EXEC or privileged EXEC mode.

show shared-line {**call** | **details** | **subscription** | **summary**}

Syntax Description

call	Displays information about all active calls on shared lines.
details	Displays detailed information about each shared line.
subscription	Displays information for specific subscriptions to shared lines.
summary	Displays summary information about active subscriptions to shared lines.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following is sample output from the **show shared-line call** command:

```
Router# show shared-line call
Shared-Line active call info:
Shared-Line: '20141',  active calls: 3
Local User       Local Address             Remote User       Remote Address    CallID
==========       =====================     ===========       ===================== ====
20141            20141@10.6.0.2             20143             20143@10.10.0.1   3168

20141            20141@10.6.0.1             Barge             20143@10.10.0.1   3209

20141            20141@10.6.0.2             20141             20141@10.10.0.1   3210
```

The following is sample output from the **show shared-line details** command:

```
Router# show shared-line details
Shared-Line info details:

Shared-Line: '20141',  subscribed users: 2,  max calls limit: 10
Index        Users                 sub_id        peer_tag        Status
=====        =====                 ======        ========        ======
  1          20141@10.6.0.1           5             40001           ACTIVE
  2          20141@10.6.0.2           6             40002           ACTIVE
Free call queue size: 7,   Active call queue size: 3

Message queue size: 20,   Event queue size: 64
```

The following is sample output from the **show shared-line subscription** command:

```
Router# show shared-line subscription
Shared-Line Subscription Info:

Subscriptions to: '20141',   total subscriptions: 2
SubID        Subscriber                   Expires         Sub-Status
=====        ==========                   =======         ==========
  5          20141@10.6.0.1                  3600          NOTIFY_ACKED
  6          20141@10.6.0.2                  3600          NOTIFY_ACKED
```

The following is sample output from the **show shared-line summary** command:

```
Router# show shared-line summary
Shared-Line info summary:
Shared-Line: '20141',  subscribed users: 2,  max calls limit: 10
```

The table below describes the significant fields shown in the displays.

Table 27: show shared-line Field Descriptions

Field	Description
Expires	Number of seconds until the subscription expires.
Local Address	IP address of the local phone involved in the shared line call.
Local User	Extension number of the shared line.
Remote Address	IP address of the remote phone involved in the shared line call.
Remote User	Extension of the remote phone involved in the shared line call.
SubID	Subscription ID.
Subscriber	Extension number of the shared line and the IP address of the phone subscriber.
Sub-Status	Status of the subscription.
Users	IP addresses of the phones using the shared line.

Related Commands

Command	Description
debug shared-line	Displays debugging information about SIP shared lines.

show sip dhcp

To display the Session Initiation Protocol (SIP) parameters retrieved via the Dynamic Host Configuration Protocol (DHCP), use the **show sip dhcp** command in privileged EXEC mode.

show sip dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.

Usage Guidelines

If SIP parameters are configured to be retrieved via DHCP, use the show sip dhcp command to display the SIP parameters retrieved.

Examples

The following is sample output from the show sip dhcp command:

```
Router# show sip dhcp
SIP UAC DHCP Info
SIP-DHCP interface:  GigabitEthernet0/0
SIP server address:  ipv4:9.13.2.36
Pilot number:        777777
Domain name:         dns:cisco.com
Secondary number:    222222
Secondary number:    333333
Secondary number:    444444
Secondary number:    555555
Secondary number:    666666
```

Table 1 describes the significant fields shown in the display.

Table 28: show sip dhcp Field Descriptions

Field	Description
SIP-DHCP interface	Indicates the type and number of the interface assigned to be used for SIP provisioning via DHCP.
SIP server address	Displays the address of the SIP server configured on the DHCP server and retrieved via DHCP.
Pilot number	Displays the pilot or contract number retrieved via DHCP and registered with the SIP server. Registration is done only for the pilot number.

Field	Description
Domain name	Indicates the domain name of the SIP server. The Cisco Unified Border Element will try to resolve this domain name by Domain Name System (DNS) into a routable layer 3 IP address for sending Register and Invite messages.
Secondary number	Indicates the first five secondary or additional numbers retrieved from the DHCP server. Secondary numbers are not registered with the SIP server.

Related Commands

Command	Description
debug ccsip dhcp	Displays information on SIP and DHCP interaction for debugging DHCP provisioning of SIP parameters.