show sip service through show trunk hdlc

show sip service

To display the status of SIP call service on a SIP gateway, use the **show sip service**commandin voice configuration mode.

show sip service

Syntax Description

This command has no arguments or keywords

Command Default

No default behaviors or values

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example displays output when SIP call service is enabled:

```
Router# show sip service
SIP Service is up
```

The following example displays output when SIP call service is shut down with the **shutdown** command:

```
Router# show sip service
SIP service is shut globally
under 'voice service voip'
```

The following example displays output when SIP call service is shut down with the **call service stop** command:

```
Router# show sip service
SIP service is shut
under 'voice service voip', 'sip' submode
```

The following example displays output when SIP call service is shut down with the **shutdown forced** command:

```
Router# show sip service
SIP service is forced shut globally
under 'voice service voip'
```

The following example displays output when SIP call service is shut down with the **call service stop forced** command:

```
Router# show sip service
SIP service is forced shut
under 'voice service voip', 'sip' submode
```

Field descriptions should be self-explanatory.

show sip-ua calls

To display active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (SIP) calls, use the **show sip-ua calls** command in privileged EXEC mode.

show sip-ua calls [**brief**]

Syntax Description

brief	Displays a summary of calls.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(22)T	Command output was updated to show IPv6 information and to display Resource Reservation Protocol (RSVP) quality of service (QoS) preconditions information.
Cisco IOS 15.6(2)T	Command output was updated to show Local UUID and Remote UUID information.
Cisco IOS XE Everest 16.5.1b	Command output was updated to show AEAD_AES_256_GCM and AEAD_AES_128_GCM cipher suites under Local Crypto Suite and Remote Crypto Suite.
Cisco IOS XE Release 16.11.1	Command output was updated to show Local Crypto Key and Remote Crypto Key.
Cisco IOS XE Bengaluru 17.6.1a	This command was enhanced to include information on fields related to WebSocket calls.

Usage Guidelines

The **show sip-ua calls** command displays active UAC and UAS information for SIP calls on a Cisco IOS device. The output includes information about IPv6, RSVP, and media forking for each call on the device and for all media streams associated with the calls. There can be any number of media streams associated with a call, of which typically only one is active. However, a call can include up to three active media streams if the call is media-forked. Use this command when debugging multiple media streams to determine if an active call on the device is forked.

From Cisco IOS XE Bengaluru 17.6.1a, this command was enhanced to include the following fields relevant to WebSocket calls:

- fork session id
- near-end channel ID (CVP side)
- far-end channel ID (CUBE side)

Note Fields corresponding to QoS negotiation in the output produced by the **show sip-ua calls** command should be ignored when the CUBE is not configured with RSVP.

```
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
```

Note If you are using Cisco IOS XE Denali 16.3.6, 16.3.7, or 16.3.8, we recommend that you upgrade to Cisco IOS XE Everest 16.06.05, 16.06.06, or Cisco IOS XE Fuji 16.09.03 to see the correct details in the *Media Dest IP Addr:Port* and *RmtMediaIP* fields.

The following is sample output from the **show sip-ua calls** command for a call forked with WebSocket connection:

```
router# show sip-ua calls
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID : 382AC8C3-CF1611EA-80229C76-5A10D8B5@10.64.86.201
State of the call : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number : 808808
Called Number : 5555
Called URI : sip:5555@10.64.86.70:8071
Bit Flags : 0xC04018 0x90000100 0x80
CC Call ID : 24
Local UUID : 87f5a958859a5067ba927188cfe38eac
Remote UUID : 224a1be49f0059e69ab10a29d7956345
Source IP Address (Sig ): 10.64.86.201
Destn SIP Req Addr:Port : [10.64.86.70]:8071
Destn SIP Resp Addr:Port: [10.64.86.70]:8071
Destination Name : 10.64.86.70
Number of Media Streams : 1
Number of Active Streams: 1
RTP Fork Object : 0x0
Media Mode : flow-through
Media Stream 1
State of the stream : STREAM_ACTIVE
Stream Call ID : 24
Stream Type : voice-only (0)
Stream Media Addr Type : 1
Negotiated Codec : g711alaw (160 bytes)
Codec Payload Type : 8
Negotiated Dtmf-relay : inband-voice
Dtmf-relay Payload Type : 0
QoS ID : -1
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
Local QoS Status : None
Media Source IP Addr:Port: [10.64.86.201]:8006
Media Dest IP Addr:Port : [10.64.86.70]:6021
Mid-Call Re-Assocation Count: 0
SRTP-RTP Re-Assocation DSP Query Count: 0
Fork session id: 2
```

```
Near-end channel id: 3
Far-end channel id: 4


Options-Ping ENABLED:NO ACTIVE:NO
Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
Call 1
SIP Call ID : 1-14135@10.64.86.70
State of the call : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number : 808808
Called Number : 5555
Called URI : sip:5555@CUBE.com
Bit Flags : 0xC0401C 0x10000100 0x4
CC Call ID : 23
Local UUID : 224a1be49f0059e69ab10a29d7956345
Remote UUID : 87f5a958859a5067ba927188cfe38eac
Source IP Address (Sig ): 10.64.86.201
Destn SIP Req Addr:Port : [10.64.86.70]:5064
Destn SIP Resp Addr:Port: [10.64.86.70]:5064
Destination Name : 10.64.86.70
Number of Media Streams : 1
Number of Active Streams: 1
RTP Fork Object : 0x0
Media Mode : flow-through
Media Stream 1
State of the stream : STREAM_ACTIVE
Stream Call ID : 23
Stream Type : voice-only (0)
Stream Media Addr Type : 1
Negotiated Codec : g711alaw (160 bytes)
Codec Payload Type : 8
Negotiated Dtmf-relay : inband-voice
Dtmf-relay Payload Type : 0
QoS ID : -1
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
Local QoS Status : None
Media Source IP Addr:Port: [10.64.86.201]:8004
Media Dest IP Addr:Port : [10.64.86.70]:6024
Mid-Call Re-Assocation Count: 0
SRTP-RTP Re-Assocation DSP Query Count: 0


Options-Ping ENABLED:NO ACTIVE:NO
Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command for a forked call with four associated media streams, three of which are currently active:

```
Device# show sip-ua calls
SIP UAC CALL INFO
Call 1
SIP Call ID : 515205D4-20B711D6-8015FF77-1973C402@172.18.195.49
State of the call : STATE_ACTIVE (6)
Substate of the call : SUBSTATE_NONE (0)
Calling Number : 5550200
Called Number : 5551101
Bit Flags : 0x12120030 0x220000
Source IP Address (Sig ): 172.18.195.49
```

```
Destn SIP Req Addr:Port : 172.18.207.18:5063
Destn SIP Resp Addr:Port: 172.18.207.18:5063
Destination Name : 172.18.207.18
Number of Media Streams : 4
Number of Active Streams: 3
RTP Fork Object : 0x637C7B60
Media Stream 1
State of the stream : STREAM_ACTIVE
Stream Call ID : 28
Stream Type : voice-only (0)
Negotiated Codec : g711ulaw (160 bytes)
Codec Payload Type : 0
Negotiated Dtmf-relay : inband-voice
Dtmf-relay Payload Type : 0
Media Source IP Addr:Port: 172.18.195.49:19444
Media Dest IP Addr:Port : 172.18.193.190:16890
Media Stream 2
State of the stream : STREAM_ACTIVE
Stream Call ID : 33
Stream Type : voice+dtmf (1)
Negotiated Codec : g711ulaw (160 bytes)
Codec Payload Type : 0
Negotiated Dtmf-relay : rtp-nte
Dtmf-relay Payload Type : 101
Media Source IP Addr:Port: 172.18.195.49:18928
Media Dest IP Addr:Port : 172.18.195.73:18246
Media Stream 3
State of the stream : STREAM_ACTIVE
Stream Call ID : 34
Stream Type : dtmf-only (2)
Negotiated Codec : No Codec (0 bytes)
Codec Payload Type : -1 (None)
Negotiated Dtmf-relay : rtp-nte
Dtmf-relay Payload Type : 101
Media Source IP Addr:Port: 172.18.195.49:18428
Media Dest IP Addr:Port : 172.16.123.99:34463
Media Stream 4
State of the stream : STREAM_DEAD
Stream Call ID : -1
Stream Type : dtmf-only (2)
Negotiated Codec : No Codec (0 bytes)
Codec Payload Type : -1 (None)
Negotiated Dtmf-relay : rtp-nte
Dtmf-relay Payload Type : 101
Media Source IP Addr:Port: 172.18.195.49:0
Media Dest IP Addr:Port : 172.16.123.99:0
Number of UAC calls: 1
SIP UAS CALL INFO
```

The following is sample output from the **show sip-ua calls** command showing IPv6 information:

```
Device# show sip-ua calls
SIP UAC CALL INFO
Call 1
SIP Call ID                : 8368ED08-1C2A11DD-80078908-BA2972D0@2001::21B:D4FF:FED7:B000
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 2000
   Called Number           : 1000
   Bit Flags               : 0xC04018 0x100 0x0
   CC Call ID              : 2
   Source IP Address (Sig ): 2001::21B:D4FF:FED7:B000
   Destn SIP Req Addr:Port : [2001::21B:D5FF:FE1D:6C00]:5060
   Destn SIP Resp Addr:Port: [2001::21B:D5FF:FE1D:6C00]:5060
```

```
   Destination Name        : 2001::21B:D5FF:FE1D:6C00
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 2
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1709707780
     Negotiated Codec         :  (20 bytes)
     Codec Payload Type       : 18
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     Media Source IP Addr:Port: [2001::21B:D4FF:FED7:B000]:16504
     Media Dest IP Addr:Port  : [2001::21B:D5FF:FE1D:6C00]:19548
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1
SIP UAS CALL INFO
   Number of SIP User Agent Server(UAS) calls: 0
```

The following is sample output from the **show sip-ua calls** command when mandatory QoS is configured at both endpoints and RSVP has succeeded:

```
Device# show sip-ua calls
SIP UAC CALL INFO
  Number of SIP User Agent Client(UAC) calls: 0
SIP UAS CALL INFO
Call 1
SIP Call ID              : F31FEA20-CFF411DC-8068DDB4-22C622B8@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:64440
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:18542
  Media Dest IP Addr:Port  : 172.18.19.73:16912
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Mandatory
  Negotiated QoS Strength  : Mandatory
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success
Options-Ping    ENABLED:NO     ACTIVE:NO
```

```
 Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when optional QoS is configured at both endpoints and RSVP has succeeded:

```
Device# show sip-ua calls
SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID                : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call         : STATE_ACTIVE (7)
 Substate of the call      : SUBSTATE_NONE (0)
 Calling Number            : 6001
 Called Number             : 1001
 Bit Flags                 : 0x8C4401E 0x100 0x4
 CC Call ID                : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name          : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object           : 0x0
 Media Mode                : flow-through
 Media Stream 1
  State of the stream        : STREAM_ACTIVE
  Stream Call ID             : 30
  Stream Type                : voice-only (0)
  Negotiated Codec           : g711ulaw (160 bytes)
  Codec Payload Type         : 0
  Negotiated Dtmf-relay      : inband-voice
  Dtmf-relay Payload Type   : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port   : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                     : -2
  Local QoS Strength         : Optional
  Negotiated QoS Strength   : Optional
  Negotiated QoS Direction : SendRecv
  Local QoS Status           : Success
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when optional QoS is configured at both endpoints and RSVP has failed:

```
Device# show sip-ua calls
SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID                : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call         : STATE_ACTIVE (7)
 Substate of the call      : SUBSTATE_NONE (0)
```

```
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Optional
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Fail
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when the command is used on the originating gateway (OGW) while optional QoS is configured on the OGW, mandatory QoS is configured on the terminating gateway (TGW), and RSVP has succeeded:

```
Device# show sip-ua calls
SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID                : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
```

```
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Mandatory
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from **show sip-ua calls** command showing Local UUID and Remote UUID:

```
Device# show sip-ua calls
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID                : B0965CA5-B83311E5-800DFB70-CD24AE29@10.64.86.130
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : sipp
   Called Number           : 56789
   Called URI              : sip:56789@10.64.86.70:8678
   Bit Flags               : 0xC04018 0x90000100 0x0
   CC Call ID              : 3
   Local UUID              : db248b6cbdc547bbc6c6fdfb6916eeb
   Remote UUID             : 4fd24d9121935531a7f8d750ad16e19
   Source IP Address (Sig ): 10.64.86.130
   Destn SIP Req Addr:Port : [10.64.86.70]:8678
   Destn SIP Resp Addr:Port: [10.64.86.70]:8678
   Destination Name        : 10.64.86.70
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 3
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [10.64.86.130]:16388
     Media Dest IP Addr:Port  : [9.45.33.11]:16384


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
```

```
Call 1
SIP Call ID                : 1-22408@10.64.86.70
   State of the call       : STATE_SENT_SUCCESS (15)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : sipp
   Called Number           : 56789
   Called URI              : sip:56789@10.64.86.130:5060
   Bit Flags               : 0xC0401E 0x10000100 0x200444
   CC Call ID              : 2
   Local UUID              : 4fd24d9121935531a7f8d750ad16e19
   Remote UUID             : db248b6cbdc547bbc6c6fdfb6916eeb
   Source IP Address (Sig ): 10.64.86.130
   Destn SIP Req Addr:Port : [10.64.86.70]:5061
   Destn SIP Resp Addr:Port: [10.64.86.70]:5061
   Destination Name        : 10.64.86.70
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 2
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
```

The following is sample output from the **show sip-ua calls** command showing AEAD_AES_256_GCM and AEAD_AES_128_GCM cipher-suites under Local Crypto Suite and Remote Crypto Suite:

```
Device# show sip-ua calls
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID                : A574C2A9-849711E6-8008B4F0-6A529C6A@8.39.16.17
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 909909
   Called Number           : 909909
   Called URI              : sip:909909@8.0.0.200:1256
   Bit Flags               : 0xC04018 0x90000100 0x0
   CC Call ID              : 2
   Local UUID              : dfe71ed9bfba5a34abd76546cfa07b81
   Remote UUID             : 06c8a6ae52fb57888aeebb588693ba2c
   Source IP Address (Sig ): 8.39.16.17
   Destn SIP Req Addr:Port : [8.0.0.200]:1256
   Destn SIP Resp Addr:Port: [8.0.0.200]:1256
   Destination Name        : 8.0.0.200
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 2
     Stream Type              : voice+dtmf (1)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : rtp-nte
     Dtmf-relay Payload Type  : 101
```

```
      QoS ID                    : -1
      Local QoS Strength        : BestEffort
      Negotiated QoS Strength   : BestEffort
      Negotiated QoS Direction : None
      Local QoS Status          : None
      Media Source IP Addr:Port: [8.39.16.17]:16386
      Media Dest IP Addr:Port   : [8.0.0.200]:39768
      Local Crypto Suite        :  AEAD_AES_128_GCM(
                                   AEAD_AES_256_GCM
                                   AEAD_AES_128_GCM
                                   AES_CM_128_HMAC_SHA1_80
                                   AES_CM_128_HMAC_SHA1_32 )
      Remote Crypto Suite       :  AEAD_AES_128_GCM
      Local Crypto Key          : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z1234tVb2
      Remote Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z9876tVb2
    Mid-Call Re-Assocation Count: 0
    SRTP-RTP Re-Assocation DSP Query Count: 0


 Options-Ping    ENABLED:NO    ACTIVE:NO
    Number of SIP User Agent Client(UAC) calls: 1

 SIP UAS CALL INFO
 Call 1
 SIP Call ID                : 1-25632@8.0.0.200
    State of the call       : STATE_ACTIVE (7)
    Substate of the call    : SUBSTATE_NONE (0)
    Calling Number          : 909909
    Called Number           : 909909
    Called URI              : sip:909909@8.39.16.17:5060
    Bit Flags               : 0x8C4401C 0x10000100 0x0
    CC Call ID              : 1
    Local UUID              : 06c8a6ae52fb57888aeebb588693ba2c
    Remote UUID             : dfe71ed9bfba5a34abd76546cfa07b81
    Source IP Address (Sig ): 8.39.16.17
    Destn SIP Req Addr:Port : [8.0.0.200]:7256
    Destn SIP Resp Addr:Port: [8.0.0.200]:7256
    Destination Name        : 8.0.0.200
    Number of Media Streams : 1
    Number of Active Streams: 1
    RTP Fork Object         : 0x0
    Media Mode              : flow-through
    Media Stream 1
      State of the stream       : STREAM_ACTIVE
      Stream Call ID            : 1
      Stream Type               : voice+dtmf (0)
      Stream Media Addr Type    : 1
      Negotiated Codec          : g711ulaw (160 bytes)
      Codec Payload Type        : 0
      Negotiated Dtmf-relay     : rtp-nte
      Dtmf-relay Payload Type   : 101
      QoS ID                    : -1
      Local QoS Strength        : BestEffort
      Negotiated QoS Strength   : BestEffort
      Negotiated QoS Direction : None
      Local QoS Status          : None
      Media Source IP Addr:Port: [8.39.16.17]:16384
      Media Dest IP Addr:Port   : [8.0.0.200]:39768
      Local Crypto Suite        :  AES_CM_128_HMAC_SHA1_80
      Remote Crypto Suite       :  AES_CM_128_HMAC_SHA1_80(
                                   AEAD_AES_256_GCM
                                   AEAD_AES_128_GCM
                                   AES_CM_128_HMAC_SHA1_80
                                   AES_CM_128_HMAC_SHA1_32 )
```

```
      Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z1234tVb2
      Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z9876tVb2
   Mid-Call Re-Assocation Count: 0
   SRTP-RTP Re-Assocation DSP Query Count: 0


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command showing Local Crypto Key and Remote Crypto Key:

```
Device# show sip-ua calls

Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID                : C9A3AA00-B49A11E8-8018A74B-CD0B0450@10.0.0.1
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 1234
   Called Number           : 9876
   Called URI              : sip:9876@10.0.0.2:9800
   Bit Flags               : 0xC04018 0x90000100 0x80
   CC Call ID              : 13
   Local UUID              : 7d14e2d622ec504f9aaa4ba029ddd136
   Remote UUID             : 2522eaa82f505c868037da95438fc49b
   Source IP Address (Sig ): 10.0.0.1
   Destn SIP Req Addr:Port : [10.0.0.2]:9800
   Destn SIP Resp Addr:Port: [10.0.0.2]:9800
   Destination Name        : 10.0.0.1
   Number of Media Streams : 2
   Number of Active Streams: 2
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 13
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [10.0.0.1]:8022
     Media Dest IP Addr:Port  : [10.0.0.2]:6008
     Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80 (
                                 AEAD_AES_256_GCM
                                 AEAD_AES_128_GCM
                                 AES_CM_128_HMAC_SHA1_80
                                 AES_CM_128_HMAC_SHA1_32 )
     Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80
     Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z1234tVb2
     Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z9876tVb2
   Media Stream 2
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 14
     Stream Type              : video (7)
```

```
      Stream Media Addr Type   : 1
      Negotiated Codec         : h264 (0 bytes)
      Codec Payload Type       : 97
      Negotiated Dtmf-relay    : inband-voice
      Dtmf-relay Payload Type  : 0
      QoS ID                   : -1
      Local QoS Strength       : BestEffort
      Negotiated QoS Strength  : BestEffort
      Negotiated QoS Direction : None
      Local QoS Status         : None
      Media Source IP Addr:Port: [10.0.0.1]:8020
      Media Dest IP Addr:Port  : [10.0.0.2]:9802
      Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80 (
                                  AEAD_AES_256_GCM
                                  AEAD_AES_128_GCM
                                  AES_CM_128_HMAC_SHA1_80
                                  AES_CM_128_HMAC_SHA1_32 )
      Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80
      Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z2345tVb2
      Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z8765tVb2
   Mid-Call Re-Assocation Count: 0
   SRTP-RTP Re-Assocation DSP Query Count: 0


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
Call 1
SIP Call ID                : 1-12049@10.0.0.2
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 1234
   Called Number           : 9876
   Called URI              : sip:9876@10.0.0.1:5060
   Bit Flags               : 0xC0401C 0x10000100 0x4
   CC Call ID              : 11
   Local UUID              : 2522eaa82f505c868037da95438fc49b
   Remote UUID             : 7d14e2d622ec504f9aaa4ba029ddd136
   Source IP Address (Sig ): 10.0.0.1
   Destn SIP Req Addr:Port : [10.0.0.2]:5060
   Destn SIP Resp Addr:Port: [10.0.0.2]:5060
   Destination Name        : 10.0.0.2
   Number of Media Streams : 2
   Number of Active Streams: 2
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
      State of the stream      : STREAM_ACTIVE
      Stream Call ID           : 11
      Stream Type              : voice-only (0)
      Stream Media Addr Type   : 1
      Negotiated Codec         : g711ulaw (160 bytes)
      Codec Payload Type       : 0
      Negotiated Dtmf-relay    : inband-voice
      Dtmf-relay Payload Type  : 0
      QoS ID                   : -1
      Local QoS Strength       : BestEffort
      Negotiated QoS Strength  : BestEffort
      Negotiated QoS Direction : None
      Local QoS Status         : None
      Media Source IP Addr:Port: [10.0.0.1]:8016
      Media Dest IP Addr:Port  : [10.0.0.2]:6009
      Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80
```

```
      Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80
      Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z9876tVb2
      Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z1234tVb2
    Media Stream 2
      State of the stream      : STREAM_ACTIVE
      Stream Call ID           : 12
      Stream Type              : video (7)
      Stream Media Addr Type   : 1
      Negotiated Codec         : h264 (0 bytes)
      Codec Payload Type       : 97
      Negotiated Dtmf-relay    : inband-voice
      Dtmf-relay Payload Type  : 0
      QoS ID                   : -1
      Local QoS Strength       : BestEffort
      Negotiated QoS Strength  : BestEffort
      Negotiated QoS Direction : None
      Local QoS Status         : None
      Media Source IP Addr:Port: [10.0.0.1]:8018
      Media Dest IP Addr:Port  : [10.0.0.2]:5062
      Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80
      Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80
      Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z8765tVb2
      Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z2345tVb2
    Mid-Call Re-Assocation Count: 0
    SRTP-RTP Re-Assocation DSP Query Count: 0


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls brief** command:

```
Device# show sip-ua calls brief

Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
No.  CallId    Calling#       Called#        RmtSignalIP
RmtMediaIP
     dstCallId SIPState       SIPSubState
===============================================================================================
1    2         5680           5678           10.1.76.151
10.1.99.101
     1         STATE_ACTIVE   SUBSTATE_NONE
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
No.  CallId    Calling#       Called#        RmtSignalIP
RmtMediaIP
     dstCallId SIPState       SIPSubState
===============================================================================================
1    1         5680           95678          10.1.76.151
10.1.99.199
     2         STATE_ACTIVE   SUBSTATE_NONE
   Number of SIP User Agent Server(UAS) calls: 1
```

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

Table 1: show sip-ua calls Field Descriptions

Field	Description
SIP UAC CALL INFO	Field header that indicates that the following information pertains to the SIP UAC.

Field	Description
Call 1	Field header.
SIP Call ID	UAC call identification number.
State of the call	Indicates the state of the call. This field is used for debugging purposes. The state is variable and may be different from one Cisco IOS release to another.
Substate of the call	Indicates the substate of the call. This field is used for debugging purposes. The state is variable and may be different from one Cisco IOS release to another.
Calling Number	Indicates the calling number.
Called Number	Indicates the called number.
Bit Flags	Indicates the bit flags used for debugging.
Source IP Address (Sig)	Indicates the signaling source IPv4 or IPv6 address.
Destn SIP Req Addr: Port:	Indicates the signaling destination Request IPv4 or IPv6 address and port number.
Destn SIP Resp Addr: Port:	Indicates the signaling destination Response IPv4 or IPv6 address and port number.
Destination Name	Indicates the signaling destination hostname, IPv4 address, or IPv6 address.
Number of Media Streams	Indicates the total number of media streams for this UAC call.
Number of Active Streams:	Indicates the total number of active media streams.
RTP Fork Object	Pointer address of the internal RTP Fork data structure.
Media Stream	Statistics about each active media stream are reported. The Media Stream header indicates the number of the media stream, and its statistics immediately follow this header.
State of the stream	State of the media stream indicated by the Media Stream header. Can be STREAM_ACTIVE, STREAM_ADDING, STREAM_CHANGING, STREAM_DEAD, STREAM_DELETING, STREAM_IDLE, or Invalid Stream State.
Stream Call ID	Identification of the stream call indicated by the Media Stream header.
Stream Type	Type of stream indicated by the Media Stream header. It can be dtmf-only, dtmf-relay, voice-only, or voice+dtmf-relay.
Negotiated Codec	Codec selected for the media stream. It can be g711ulaw, <G.729>, <G.726>, or No Codec.
Codec Payload Type	Payload type of the Negotiated Codec.
Negotiated Dtmf-relay	DTMF relay selected for the media stream indicated by the Media Stream header. It can be inband-voice or rtp-nte.

Field	Description
Dtmf-relay Payload Type	Payload type of the negotiated DTMF relay.
Media Source IP Addr: Port	The source IPv4 or IPv6 address and port number of the media stream indicated by the Media Stream header.
Media Dest IP Addr: Port	The destination IPv4 or IPv6 address and port number of the media stream indicated by the Media Stream header.
Local QoS Strength	The QoS strength (mandatory or optional) configured for this device.
Negotiated QoS Strength	The QoS strength (mandatory or optional) that has been negotiated.
Negotiated QoS Direction	Displays the direction in which RSVP was negotiated. For example, sendrecv indicates that RSVP was negotiated in both directions.
Local QoS Status	Displays the success or failure of RSVP reservation.
Number of UAC calls	Final SIP UAC CALL INFO field. Indicates the number of UAC calls.
SIP UAS CALL INFO	Field header that indicates that the following information pertains to the SIP UAS.
Number of UAS calls	Final SIP UAS CALL INFO field. Indicates the number of UAS calls.
Local UUID	Unique identifier generated from the originating user agent.
Remote UUID	Unique identifier generated from the terminating user agent.
Local Crypto Suite	Crypto suite negotiated by CUBE. All the crypto suites configured in CUBE are listed in parenthesis.
Remote Crypto Suite	Crypto suites received.

Related Commands

Command	Description
debug ccsip all	Enables all SIP-related debugging.
debug ccsip events	Enables tracing of events that are specific to SIP SPI.
debug ccsip info	Enables tracing of general SIP SPI information.
debug ccsip media	Enables tracing of SIP call media streams.
debug ccsip messages	Enables tracing of SIP Service Provider Interface (SPI) messages.

show sip-ua connections

To display Session Initiation Protocol (SIP) user-agent (UA) transport connection tables, use the **show sip-ua connections** command in privileged EXEC mode.

show sip-ua connections {**tcp** [**tls**] | **udp**} {**brief** | **detail**}

Syntax Description

tcp	Displays all TCP connection information.
tls	(Optional) Displays all Transport Layer Security (TLS) over TCP connection information.
udp	Displays all User Datagram Protocol (UDP) connection information.
brief	Displays a summary of connections.
detail	Displays detailed connection information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1a	The command output was updated to print the tenant-tag information associated with each connection and listen socket for UDP, TCP, and TLS transport types.
Cisco IOS XE 16.10.1	The command output for **show sip-ua connections tcp tls detail** was updated to display the Cipher and the Curve-Size.
Cisco IOS XE 17.14.1a	The command output for **show sip-ua connections tcp tls detail** is updated to display TLS v1.3 cipher configurations.

Usage Guidelines

The **show sip-ua connections** command should be executed only after a call is made. Use this command to learn the connection details.

Cisco IOS XE 17.14.1a and Later Releases

Note The RSA and ECDSA key types are displayed only for TLS version 1.3 configurations.

The following is a sample output from the **show sip-ua connections tcp tls brief** command displaying "RSA" key type along with TLS v1.3 ciphers:

```
Device# show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tls send msg queue size of 1, recorded for 10.64.100.152:5061
TLS client handshake failures : 0
```

```
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition
 * Connections with SIP OAuth ports

Remote-Agent:10.64.100.150, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address
TLS-Version                Cipher              Curve Tenant
  =========== ======= =========== =========== ======================================
=========== ================================== ===== ======
        22943       7 Established           0 10.64.100.151:5061
TLSv1.3         TLS_AES_256_GCM_SHA384:RSA P-521     0

Remote-Agent:10.64.100.152, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address
TLS-Version                Cipher              Curve Tenant
  =========== ======= =========== =========== ======================================
=========== ================================== ===== ======
         5061       8 Established           0 10.64.100.151:47687
TLSv1.3         TLS_AES_256_GCM_SHA384:RSA P-521     0


-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id             Local-Address                      Tenant
 ==========    ===========================             ========
  0             [0.0.0.0]:5061:                             0
  6             [10.64.100.151]:5061:                       0
```

The following is a sample output from the **show sip-ua connections tcp tls detail** command displaying "ECDSA" key type along with TLS v1.3 ciphers:

```
Device# show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tls send msg queue size of 1, recorded for 10.1.10.50:5061
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition
 * Connections with SIP OAuth ports

Remote-Agent:10.1.10.50, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address
TLS-Version               Cipher               Curve Tenant
  =========== ======= =========== =========== ======================================
=========== ================================== ===== ======
```

```
         5061       9 Established           0 10.1.20.155:37081
TLSv1.3  ECDHE-RSA-AES256-GCM-SHA384:ECDSA P-521     0
        41635       8 Established           0 10.1.20.155:5061
TLSv1.3       TLS_AES_256_GCM_SHA384:ECDSA P-256     0

  Remote-Port Conn-Id Conn-State  WriteQ-Size           Local-Address
TLS-Version Cipher                        Curve Tenant
  =========== ======= =========== =========== ======================================
=========== ============================== ===== ======
        53516     102 Established           0 10.64.100.150:5061
TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-521     0



-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id             Local-Address                        Tenant
 ==========    ===========================              ========
  0             [0.0.0.0]:5061:                              0
  1             [::]:5061:                                   0
  6             [10.1.20.155]:5061:                          0
  7             [2001:10:1:20::135]:5061:                    0
```

Cisco IOS XE Cupertino 17.8.1a and Later Releases

The following is a sample output from the **show sip-ua connections tcp tls brief** command showing a brief summary including the associated tenant-tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
router# show sip-ua connections tcp tls brief
Total active connections : 2
No. of send failures : 0
No. of remote closures : 47
No. of conn. failures : 43
No. of inactive conn. ageouts : 0
Max. tls send msg queue size of 1, recorded for 10.105.34.88:5061
TLS client handshake failures : 0
TLS server handshake failures : 4

-------------- SIP Transport Layer Listen Sockets ---------------
Conn-Id  Local-Address   Tenant
=========== ============================ ============
 3             [10.64.86.181]:3000:        1
19             [8.43.21.58]:4000:          2
90             [10.64.86.181]:5061:        0
```

The following is a sample output from the **show sip-ua connections tcp tls detail** command showing a connection details, including the associated tenant tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
Router#sh sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 3
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tls send msg queue size of 1, recorded for 10.105.34.88:8090
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
```

```
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:10.105.34.88, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version (contd.)
  =========== ======= =========== =========== ============= ===========
        38928       9 Established           0 10.64.100.145     TLSv1.2
         8090      10 Established           0 10.64.100.145     TLSv1.2


  Cipher                        Curve       Tenant
  ============================  =========== ======
   ECDHE-RSA-AES256-GCM-SHA384        P-256     10
                    AES256-SHA                  10

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id             Local-Address                      Tenant
 ==========    ===========================             ========
  2             [8.43.21.8]:5061:                            0
  3             [10.64.100.145]:5090:                       10
  4             [10.64.100.145]:8123:                       50
  5             [10.64.100.145]:5061:                        0
```

The following is a sample output from the **show sip-ua connections tcp brief** command showing a summary including that prints the associated tenant-tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
CSR#sh sip-ua connections tcp brief
Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 2
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 1, recorded for 10.105.34.88:8091

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id             Local-Address                      Tenant
 ==========    ===========================             ========
  2             [8.43.21.8]:5060:                            0
  3             [10.64.100.145]:5430:                        1
  4             [10.64.100.145]:5160:                        3
  5             [10.64.100.145]:5267:                        6
```

The following is a sample output from the **show sip-ua connections tcp detail** command showing a connection details, including the associated tenant tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
Router#show sip-ua connections tcp tls detail
Total active connections      : 4
No. of send failures          : 0
No. of remote closures        : 8
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
```

```
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition
 * Connections with SIP OAuth ports

Remote-Agent:10.5.10.200, Connections-Count:0

Remote-Agent:10.5.10.201, Connections-Count:0

Remote-Agent:10.5.10.202, Connections-Count:0

Remote-Agent:10.5.10.212, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher
             Curve
  =========== ======= =========== =========== ============= ===========
============================== =====
        52248      27 Established           0             -      TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:10.5.10.213, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher
             Curve
  =========== ======= =========== =========== ============= ===========
============================== =====
        50901     28* Established           0             -      TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:10.5.10.209, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher
             Curve
  =========== ======= =========== =========== ============= ===========
============================== =====
        51402     29* Established           0             -      TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:10.5.10.204, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher
             Curve
  =========== ======= =========== =========== ============= ===========
============================== =====
        50757     30* Established           0             -      TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:10.5.10.218, Connections-Count:0


-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id               Local-Address
 ===========    =============================
   0             [0.0.0.0]:5061:
   2             [0.0.0.0]:5090:
gw1-2a#
=================================

gw1-2a#show sip status registrar
Line          destination                              expires(sec)  contact
transport     call-id
              peer
==========================================================================================
2999904       10.5.10.204                             76            10.5.10.204

TLS*           00451d86-f1520107-5b4fd894-7ab6c4ce@10.5.10.204
              40004
```

```
2999901       10.5.10.212                              74            10.5.10.212

TLS            00af1f9c-12dc037b-14a5f99d-09f10ac4@10.5.10.212
              40001

2999902       10.5.10.213                              75            10.5.10.213

TLS*           00af1f9c-48370020-2bf6ccd4-2423aff8@10.5.10.213
              40002

2999905       10.5.10.209                              76            10.5.10.209

TLS*           5006ab80-69ca0049-1ce700d8-12edb829@10.5.10.209
              40003
```

The following is a sample output from the **show sip-ua connections udp brief** command showing a summary including that prints the associated tenant-tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
CSR#sh sip-ua connections udp brief
Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id             Local-Address                      Tenant
 ==========    ===========================             ========
  2             [8.43.21.8]:5060:                           0
  3             [10.64.100.145]:5260:                      10
  4             [10.64.100.145]:5330:                      50
  5             [10.64.100.145]:5060:                       0
```

The following is a sample output from the **show sip-ua connections udp detail** command showing a connection details, including the associated tenant tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
CSR#sh sip-ua connections udp detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:10.105.34.88, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address Tenant
  =========== ======= =========== =========== ============= ======
         5061       6 Established           0 10.64.100.145   200
         8091       7 Established           0 10.64.100.145   200


-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id             Local-Address                      Tenant
 ==========    ===========================             ========
```

```
2             [8.43.21.8]:5060:                            0
3             [10.64.100.145]:5361:                       10
4             [10.64.100.145]:5326:                       50
5             [10.64.100.145]:5060:                      200
```

Examples

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

Table 2: show sip-ua connections Field Descriptions

Field	Description
Total active connections	Indicates all the connections that the gateway holds for various targets. Statistics are broken down within individual fields.
No. of send failures.	Indicates the number of TCP or UDP messages dropped by the transport layer. Messages are dropped if there were network issues, and the connection was frequently ended.
No. of remote closures	Indicates the number of times a remote gateway ended the connection. A higher value indicates a problem with the network or that the remote gateway does not support reusing the connections (thus it is not RFC 3261-compliant). The remote closure number can also contribute to the number of send failures.
No. of conn. failures	Indicates the number of times that the transport layer was unsuccessful in establishing the connection to the remote agent. The field can also indicate that the address or port that is configured under the dial peer might be incorrect or that the remote gateway does not support that mode of transport.
No. of inactive conn. ageouts	Indicates the number of times that the connections were ended or timed out because of signaling inactivity. During call traffic, this number should be zero. If it is not zero, we recommend that the inactivity timer be tuned to optimize performance by using the **timers** command.
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0	Indicates the number of messages waiting in the queue to be sent out on the TCP connection when the congestion was at its peak. A higher queue number indicates that more messages are waiting to be sent on the network. The growth of this queue size cannot be controlled directly by the administrator.
Tuples with no matching socket entry	Any tuples for the connection entry that are marked with "**" at the end of the line indicate an upper transport layer error condition; specifically, that the upper transport layer is out of sync with the lower connection layer. Cisco IOS Software should automatically overcome this condition. If the error persists, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection**command and report the problem to your support team.
Tuples with mismatched address/port entry	Any tuples for the connection entry that are marked with "++" at the end of the line indicate an upper transport layer error condition, where the socket is probably readable, but is not being used. If the error persists, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection**command and report the problem to your support team.
Remote-Agent Connections-Count	Connections to the same target address. This field indicates how many connections are established to the same host.

Field	Description
Remote-Port Conn-Id Conn-State WriteQ-Size	Connections to the same target address. This field indicates how many connections are established to the same host. The WriteQ-Size field is relevant only to TCP connections and is a good indicator of network congestion and if there is a need to tune the TCP parameters.
Cipher	Displays the negotiated Cipher.
Curve	Curve Size of the ECDSA Cipher.

Related Commands

Command	Description
clear sip-ua tcp tls connection id	Clears a SIP TCP TLS connection.
clear sip-ua tcp connection	Clears a SIP TCP connection.
clear sip-ua udp connection	Clears a SIP UDP connection.
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP user agent status.
show sip-ua timers	Displays the current settings for the SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.
timers	Configures the SIP signaling timers.

show sip-ua map

To display the mapping table of public switched telephone network (PSTN) cause codes and their corresponding Session Initiation Protocol (SIP) error status codes or the mapping table of SIP-to-PSTN codes, use the **show sip-ua map** command in privileged EXEC mode.

show sip-ua map {**pstn-sip** | **sip-pstn** | **sip-request-pstn**}

Syntax Description

pstn-sip	Displays the PSTN cause-code-to-SIP-status-code mapping table.
sip-pstn	Displays the SIP-status-code-to-PSTN-cause-code mapping table.
sip-request-pstn	Display the SIP-requests-PSTN-cause mapping table.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.4(22)T	This command was modified. The **sip-request-pstn**keyword was added.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Examples

The following is sample output from the **show sip-ua map pstn-sip**command:

```
Router# show sip-ua map pstn-sip
PSTN-Cause   Configured       Default
             SIP-Status      SIP-Status
1               404             404
2               404             404
3               404             404
4               500             500
5               500             500
6               500             500
7               500             500
8               500             500
9               500             500
.
.
.
100             500             500
101             500             500
102             408             408
103             500             500
110             500             500
```

```
111             400             400
126             500             500
127             500             500
```

The following is sample output from the **show sip-ua map sip-pstn**command:

```
Router# show sip-ua map sip-pstn
SIP-Status   Configured        Default
             PSTN-Cause      PSTN-Cause
400             127             127
401             57              57
402             21              21
403             57              57
404             1               1
405             127             127
406             127             127
407             21              21
408             102             102
409             41              41
410             1               1
.
.
.
600             17              17
603             21              21
604             1               1
606             58              58

The following is sample output from the show sip
-ua map request
-pstn
command:
Router# show sip-request-pstn
SIP-Status   Configured        Default
             PSTN-Cause      PSTN-Cause
CANCEL          16              16
```

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

Table 3: show sip-ua map Field Descriptions

Field	Description
PSTN-Cause	Reasons for PSTN call failure or completion. PSTN cause code range is from 1 to 127.
Configured SIP-Status	Configured SIP status code or event. SIP Status code range is from 400 to 699.
Default SIP-Status	Default mapping between and PSTN and SIP networks.
SIP-Status	Configured SIP status code or event. SIP status code range is from 400 to 699.
Configured PSTN-Cause	Reasons for PSTN call failure or completion. PSTN cause code range is from 1 to 127.
Default PSTN-Cause	Default mapping between and SIP and PSTN networks.

Related Commands

Command	Description
set pstn-cause	Sets an incoming PSTN release cause code to a SIP error status code.
set sip-status	Sets an incoming SIP error status code to a PSTN release cause code.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua min-se

To show the current value of the minimum session expiration (Min-SE) header for calls that use the Session Initiation Protocol (SIP) session timer, use the **show sip-ua min-se** command in privileged EXEC mode.

show sip-ua min-se

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.
12.4(9)T	The Min-SE header default time was changed from 3200 to 90 seconds.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use thiscommand to verify the value of the Min-SE header.

Examples

The following is sample output from thiscommand:

```
Router# show sip-ua min-se
SIP UA MIN-SE Value (seconds)
Min-SE: 90
```

The table below describes the fields shown in this output.

Table 4: show sip-ua min-se Field Descriptions

Field	Description
SIP UA MIN-SE Value (seconds)	Field header indicating that the following information shows the current value of the Min-SE header, in seconds.
Min-SE	Current value of the Min-SE header, in seconds.

Related Commands

Command	Description
min-se (SIP)	Changes the Min-SE header value for all calls that use the SIP session timer.

show sip-ua mwi

To display Session Initiation Protocol (SIP) message-waiting indication (MWI) settings on the voice-mail server, use the **show sip-ua mwi command in**privileged EXEC mode.

show sip-ua mwi

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 the **show sip-ua mwi**command:

```
Router#
show sip-ua mwi
MWI type: 2
MWI server: dns:unity-vm.gb.com
MWI expires: 60
MWI port: 5060
MWI transport type: UDP
MWI unsolicited
MWI server IP address:
C801011E
0
0
0
0
0
0
0
MWI ipaddr cnt 1:
MWI ipaddr idx 0:
MWI server: 192.168.1.30, port 5060, transport 1
MWI server dns lookup retry cnt: 0
endpoint 8000  mwi status ON
endpoint 8000  mwi status ON
endpoint 8001  mwi status OFF
```

The table below provides a listing of the fields in the sample output.

Table 5: show sip-ua mwi Field Descriptions

Field	Description
MWI type	Indicates the type of MWI service. 1 indicates MWI application service, which is used when a router provides MWI relay service. 2 indicates SIP-based MWI.

Field	Description
MWI server	Indicates the host device housing the domain name server (DNS) that resolves the name of the voice-mail server.
MWI expires	Indicates the expiration time, in seconds.
MWI port	Indicates the port used by SIP signaling.
MWI transport type	Indicates the desired transport protocol. Values are tcp or udp. UDP is the default.
MWI unsolicited	Indicates whether unsolicited MWI is configured.
MWI server IP address	Indicates the IP address of the voice-mail MWI server in hex format. If you configured the **mwi-server** command for DNS format, DNS lookup may result in multiple IP addresses. All IP addresses are listed.
MWI ipaddr cnt	Indicates the number of IP addresses associated with the voice-mail MWI server.
MWI ipaddr idx	Indicates which MWI server IP address is currently being used. The index starts from 0.
MWI server	Indicates the IP address of the MWI server; the port; and transport protocol (1 indicates UDP; 2 indicates TCP).
MWI server dns lookup retry cnt	Indicates the number of retries for DNS lookup.
endpoint / mwi status	Indicates the endpoint or voice port and whether MWI notification is active. That is, if a message is waiting, the status is on. Once the message is deleted, the status is off.

Related Commands

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

show sip-ua register status

To display the status of E.164 numbers that a Session Initiation Protocol (SIP) gateway has registered with an external primary SIP registrar, use the **show sip-ua register status**command in privileged EXEC mode.

show sip-ua register status [**secondary**]

Syntax Description

secondary	(Optional) Displays the status of E.164 numbers that a SIP gateway has registered with an external secondary SIP registrar.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

SIP gateways can register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar. The command **show sip-ua register status**is only for outbound registration, so if there are no SCCP phones or FXS dialpeers to register, there is no output when the command is run.

Examples

The following is sample output from this command:

```
Router# show sip-ua register status
Line peer expires(sec) registered
4001 20001 596         no
4002 20002 596         no
5100 1     596         no
9998 2     596         no
```

The table below describes significant fields shown in this output.

Table 6: show sip-ua register status Field Descriptions

Field	Description
Line	The phone number to register.
peer	The registration destination number.
expires (sec)	The amount of time, in seconds, until registration expires.
registered	Registration status.

Related Commands

Command	Description
registrar	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.

show sip-ua retry

To display retry statistics for the Session Initiation Protocol (SIP) user agent (UA), use the show sip-ua retrycommand in privileged EXEC mode.

show sip-ua retry

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB	Command output was enhanced to display the following: Reliable provisional responses (PRACK/reliable 1*xx*), Conditions met (COMET) responses, and Notify responses.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua**command found previously in this reference.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and the Cisco AS5400 in this release.
12.2(15)T	This command is supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.

Usage Guidelines

Use this command to verify SIP configurations.

Examples

The following is sample output from this command.

```
Router# show sip-ua retry
SIP UA Retry Values
invite retry count = 6 response retry count = 1
bye retry count = 1 cancel retry count = 1
prack retry count = 10 comet retry count = 10
reliable 1xx count = 6 notify retry count = 10
```

The table below describes significant fields shown in this output, in alphabetical order.

Table 7: show sip-ua retry Field Descriptions

Field	Description
bye retry count	Number of times that a Bye request is retransmitted.

Field	Description
cancel retry count	Number of times that a Cancel request is retransmitted.
comet retry count	Number of times that a COMET request is retransmitted.
invite retry count	Number of times that an Invite request is retransmitted.
notify retry count	Number of times that a Notify message is retransmitted.
prack retry count	Number of times that a PRACK request is retransmitted.
refer retry count	Number of times that a Refer request is retransmitted.
reliable 1*xx* count	Number of times that a Reliable 1*xx* request is retransmitted.
response retry count	Number of times that a Response request is retransmitted.
SIP UA Retry Values	Field header for SIP UA retry values.

Related Commands

Command	Description
retry comet	Configures the number of times that a COMET request is retransmitted.
retry prack	Configures the number of times the PRACK request is retransmitted.
retry rel1xx	Configures the number of times the reliable 1*xx* response is retransmitted.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP UA status.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua service

To display Session Initiation Protocol (SIP) user-agent (UA) service information, use the **show sip-ua service** command in privileged EXEC mode.

show sip-ua service

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Examples

The following example displays output when SIP UA call service is enabled:

```
Router# show sip-ua service

SIP Service is up
```

The following example displays output when SIP call service is shut down with the **shutdown** command:

```
Router# show sip-ua service
SIP service is shut globally
under 'voice service voip'
```

The following example displays output when SIP call service is shut down with the **call service stop** command:

```
Router# show sip-ua service
SIP service is shut
under 'voice service voip', 'sip' submode
```

The following example displays output when SIP call service is stopped forcefully with the **call service stop forced** command:

```
Router# show sip-ua service
SIP service is forced shut
under 'voice service voip', 'sip' submode
```

The following example displays output when SIP call service is forcefully shutdown globally with the **shutdown forced** command:

```
Router# show sip-ua service
SIP service is forced shut globally
under 'voice service voip’
```

The fields in the displays are self-explanatory.

Related Commands

Command	Description
call service stop	Shuts down VoIP call service on a gateway.
voice service	Enters voice-service configuration mode and specifies a voice-encapsulation type.

show sip-ua srtp

To display Session Initiation Protocol (SIP) user-agent (UA) Secure Real-time Transport Protocol (SRTP) information, use the **show sip-ua srtp** command in privileged EXEC mode.

show sip-ua srtp

Syntax Description

This command has no keywords or arguments.

Command Default

SIP UA SRTP information is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS 15.4(1)T	This command was introduced.
Cisco IOS XE Everest 16.5.1b	Command output was updated to show AEAD_AES_256_GCM and AEAD_AES_128_GCM cipher suites.

Example

The following example displays sample output for SIP UA SRTP information prior to Cisco IOS XE Everest Release 16.5.1b:

```
Device> enable
Device# show sip-ua srtp
SIP UA SRTP
Crypto-suite Negotiation
  AES_CM_128_HMAC_SHA1_80: 3
  AES_CM_128_HMAC_SHA1_32: 2
```

The following example displays the sample output for SIP UA SRTP information including AEAD_AES_256_GCM and AEAD_AES_128_GCM cipher suites supported from Cisco IOS XE Everest Release 16.5.1b:

```
Device> enable
Device# show sip-ua srtp
SIP UA SRTP
Crypto-suite Negotiation
  AES_CM_128_HMAC_SHA1_80: 3
  AES_CM_128_HMAC_SHA1_32: 2
  AEAD_AES_256_GCM: 1
  AEAD_AES_128_GCM: 2
```

Related Commands

Command	Description
voice class srtp-crypto	From Cisco IOS XE Everest 16.5.1b onwards, this command is used to configure a Secure Real-time Transport Protocol (SRTP) connection on Cisco Unified Border Element (CUBE) in the global level using the preferred crypto suite.

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

show sip-ua statistics

To display response, traffic, and retry Session Initiation Protocol (SIP) statistics, use the **show sip-ua statistics**command in privileged EXEC mode.

show sip-ua statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	Command output was enhanced as follows: BadRequest counter (400 class) now counts malformed Via entries, reliable provisional responses (PRACK/rel1*xx*), conditions met (COMET), and NOTIFY responses.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua**command.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Command output was enhanced as follows: • OkInfo counter (200) class counts the number of successful responses to INFO requests. • Info counter counts the number of INFO messages received and sent. • BadEvent counter (489 response) counts responses to Subscribe messages with event types that are not understood by the server. • OkSubscribe counter (200 class) counts the number of 200 OK SIP messages received and sent in response to Subscribe messages. • Subscribe requests indicate total requests received and sent. • SDP application statistics added to monitor SDP. This command was supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.

Release	Modification
12.2(13)T	This command was supported in Cisco IOS Release 12.2(13)T. The following cause codes were obsoleted from the command output: • Redirection code: *SeeOther* • Client Error: *LengthRequired* A new SIP statistics counter was added: • Miscellaneous Counters: *RedirectResponseMappedToClientError* Command output was enhanced to display the following: • Time stamp that indicates the last time that SIP statistics counters were cleared.
12.2(15)T	This command is supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.
12.2(15)ZJ	Command output was enhanced to display the following: • Register counter and statistics.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Command output was enhanced to display SUBSCRIBE retry statistics.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.4(2)T	Command output was enhanced to display the SIP error counters: • Number of times a particular error has occurred. • The error string for immediate context • Timestamp of first occurrence • Timestamp of last occurrence
Cisco IOS Release XE 3.12S	Command output was enhanced to display the SIP error counters: • Number of times a particular error has occurred. • The error string for immediate context • Timestamp of first occurrence • Timestamp of last occurrence

Usage Guidelines

Use the **show sip-ua statistics**command to verify SIP configurations and to see SIP global counters. You can also use this command to see the number of times a particular error has occurred. This command is typically helpful when enabling CCSIP error debugs is not desirable. Along with other data, the error counters will provide better code-flow context, so that the issue can be reproduced and targeted RCA can be performed.

Examples

The following is sample output from this command:

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
    Informational:
      Trying 0/0, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/0
     Success:
      OkInvite 0/0, OkBye 0/0,
      OkCancel 0/0, OkOptions 0/0,
      OkPrack 0/0, OkPreconditionMet 0/0,
      OkSubscribe 0/0, OkNOTIFY 0/0,
      OkInfo 0/0, 202Accepted 0/0
      OkRegister 12/49
     Redirection (Inbound only except for MovedTemp(Inbound/Outbound)) :
      MultipleChoice 0, MovedPermanently 0,
      MovedTemporarily 0/0, UseProxy 0,
      AlternateService 0
      Client Error:
      BadRequest 0/0, Unauthorized 0/0,
      PaymentRequired 0/0, Forbidden 0/0,
      NotFound 0/0, MethodNotAllowed 0/0,
      NotAcceptable 0/0, ProxyAuthReqd 0/0,
      ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
      ReqEntityTooLarge 0/0, ReqURITooLarge 0/0,
      UnsupportedMediaType 0/0, BadExtension 0/0,
      TempNotAvailable 0/0, CallLegNonExistent 0/0,
      LoopDetected 0/0, TooManyHops 0/0,
      AddrIncomplete 0/0, Ambiguous 0/0,
      BusyHere 0/0, RequestCancel 0/0,
      NotAcceptableMedia 0/0, BadEvent 0/0,
      SETooSmall 0/0
     Server Error:
      InternalError 0/0, NotImplemented 0/0,
      BadGateway 0/0, ServiceUnavail 0/0,
      GatewayTimeout 0/0, BadSipVer 0/0,
      PreCondFailure 0/0
     Global Failure:
      BusyEverywhere 0/0, Decline 0/0,
      NotExistAnywhere 0/0, NotAcceptable 0/0
      Miscellaneous counters:
      RedirectRspMappedToClientErr 0
SIP Total Traffic Statistics (Inbound/Outbound)
      Invite 0/0, Ack 0/0, Bye 0/0,
      Cancel 0/0, Options 0/0,
      Prack 0/0, Comet 0/0,
      Subscribe 0/0, NOTIFY 0/0,
      Refer 0/0, Info 0/0
      Register 49/16
Retry Statistics
      Invite 0, Bye 0, Cancel 0, Response 0,
      Prack 0, Comet 0, Reliable1xx 0, Notify 0
      Register 4, Subscribe 0
SDP application statistics:
Parses: 0, Builds 0
Invalid token order: 0, Invalid param: 0
Not SDP desc: 0, No resource: 0
Last time SIP Statistics were cleared: <never>
```

Command output, listed in **Table 1 ,** includes a reason phrase and a count describing the SIP messages received and sent. When x/x is included in the reason phrase field, the first number is an inbound count, and the second number is an outbound count. The description field headings are based on the

SIP response code xxx, which the SIP protocol uses in determining behavior. SIP response codes are classified into one of the following six categories:

- 1xx: Informational, indicates call progress.
- 2xx: Success, indicates successful receipt or completion of a request.
- 3xx: Redirection, indicates that a redirect server has returned possible locations.
- 4xx: Client error, indicates that a request cannot be fulfilled as it was submitted.
- 5xx: Server error, indicates that a request has failed because of an error by the server. The request may be retried at another server.
- 6xx: Global failure, indicates that a request has failed and should not be tried again at any server.

The table below describes significant fields shown in this output, in alphabetical order.

Table 8: show sip-ua statistics Field Descriptions

Field	Description
Note For each field, the standard RFC 2543 SIP response number and message are shown.	
Ack 0/0	A confirmed final response received or sent.
Accepted 0/0	202 A successful response to a Refer request received or sent.
AddrIncomplete 0/0	484 Address supplied is incomplete.
AlternateService 0	380 Unsuccessful call; however, an alternate service is available.
Ambiguous 0/0	485 Address supplied is ambiguous.
BadEvent 0/0	489 Bad Event response indicates a Subscribe request having an event type that the server could not understand.
BadExtension 0/0	420 Server could not understand the protocol extension in the Require header.
BadGateway 0/0	502 Network is out of order.
BadRequest	400 Bad Request (includes the malformed Via header).
BadSipVer 0/0	505 Requested SIP version is not supported.
BusyEverywhere 0/0	600 Called party is busy.
BusyHere 0/0	486 Called party is busy.
Bye 0	Number of times that a Bye request is retransmitted to the other user agent.

Field	Description
Bye 0/0	Terminated the session.
CallLegNonExistent 0/0	481 Server is ignoring the request. Either is was a Bye request and there was no matching leg ID, or it was a Cancel request and there was no matching transaction.
Cancel 0	Number of times that a Cancel request is retransmitted to the other user agent.
Cancel 0/0	Terminated the pending request.
Comet 0	Number of times that a COMET request is retransmitted to the other user agent.
Comet 0/0	Conditions have been met.
Conflict 0/0	409 Temporary failure.
Decline 0/0	603 Call rejected.
Forbidden 0/0	403 The SIP server has the request, but cannot provide service.
Forwarded 0/0	181 Call has been forwarded.
GatewayTimeout 0/0	504 The server or gateway did not receive a timely response from another server (such as a location server).
Gone 0/0	410 Resource is no longer available at the server, and no forwarding address is known.
Info 0/0	Number of information messages the gateway has received (inbound) and how many have been transmitted (outbound).
InternalError 0/0	500 The server or gateway encountered an unexpected error that prevented it from processing the request.
Invite 0	Number of times that an INVITE request is retransmitted to the other user agent.
Invite 0/0	Initiates a call.
LoopDetected 0/0	482 A loop--server received a request that included itself in the path.
MethodNotAllowed 0/0	405 Method specified in the request is not allowed.
MovedPermanently 0	301 User is no longer available at this location.
MovedTemporarily 0	302 User is temporarily unavailable.
MultipleChoice 0	300 Address resolves to more than one location.

Field	Description
NotAcceptable 0/0	406/606 Call was contacted, but some aspect of the session description was unacceptable.
NotAcceptableMedia 0/0	406 Call was contacted, but some aspect of the session description was unacceptable.
NotExistAnywhere 0/0	604 Server has authoritative information that the called party does not exist in the network.
NotFound 0/0	404 Called party does not exist in the specified domain.
NOTIFY 0	Number of times that a Notify is retransmitted to the other user agent.
NOTIFY 0/0	Number of Notify messages received or sent.
NotImplemented 0/0	501 Service or option not implemented in the server or gateway.
OkBye 0/0	200 Successful response to a Bye request.
OkCancel 0/0	200 Successful response to a Cancel request.
OkInfo	200 Successful response to an INFO request.
OkInvite 0/0	200 Successful response to an INVITE request.
OkNOTIFY 0/0	200 Successful response to a Notify request.
OkOptions 0/0	200 Successful response to an Options request.
OkPrack 0/0	200 Successful response to a PRACK request.
OkPreconditionMet 0/0	200 Successful response to a PreconditionMet request.
OkRegister 0/0	200 Successful response to a Register request.
OkSubscribe 0/0	200 Successful response to a SUBSCRIBE request.
Options 0/0	Query the receiving or sending server as to its capabilities.
PaymentRequired 0/0	402 Payment is required to complete the call.
Prack 0	Number of times that a PRACK request is retransmitted to the other user agent.
Prack 0/0	Provisional response received or sent.
PreCondFailure 0/0	580 The session could not be established because of failure to meet required preconditions.
ProxyAuthReqd 0/0	407 Rejected for proxy authentication.
Queued 0/0	182 Until the called party is available, the message is queued.

Field	Description
RedirectResponseMappedToClientError 0	Indicates the count of incoming 3*xx* responses that were mapped to 4*xx* responses. It is incremented when the **no redirection** command is active. For the default case, the 3*xx* messages are processed per RFC 2543, and this counter is not incremented. This counter counts only inbound messages and only the 3*xx* responses that are known (300, 301, 302, 305, and 380). The counter is cleared when the **clear sip-ua statistics** command is issued.
Refer 0	Number of times the Refer request is retransmitted to the other user agent.
Refer 0/0	Number of Refer requests received or sent.
Register 0/0	Number of Register requests received or sent.
Register 0	Number of times that a Register request is retransmitted to the other user agent.
Reliable1xx 0	Indicates the number of times the Reliable 1*xx* response is retransmitted to the other user agent.
ReqEntityTooLarge 0/0	413 Server refuses to process request because the request is larger than is acceptable.
ReqTimeout 0/0	408 Server could not produce a response before the Expires time-out.
RequestCancel 0/0	Request has been canceled.
ReqURITooLarge 0/0	414 Server refuses to process, because the URI (URL) request is larger than is acceptable.
Response 0	Indicates number of Response retries.
Retry Statistics	One of the three categories of response statistics.
Ringing 0/0	180 Called party has been located and is being notified of the call.
SeeOther 0	303 Transfer to another address.
ServiceUnavail 0/0	503 Service option is not available because of an overload or maintenance problem.
SessionProgress 0/0	183 Indicates in-band alerting.
SIP Response Statistics (Inbound/Outbound)	One of the three categories of response statistics.
SIP Total Traffic Statistics (Inbound/Outbound)	One of the three categories of response statistics.

Field	Description
Subscribe 0	Indicates the number of Retry Subscribe messages sent.
Subscribe 0/0	Number of Subscribe requests received or sent.
TempNotAvailable 0/0	480 Called party did not respond.
TooManyHops 0/0	483 A server received a request that required more hops than is allowed by the Max-Forward header.
Trying 0/0	100 Action is being taken with no resolution.
Unauthorized 0/0	401 The request requires user authentication.
UnsupportedMediaType 0/0	415 Server refuses to process a request because the service option is not available on the destination endpoint.
UseProxy 0	305 Caller must use a proxy to contact called party.

Examples

The following is sample output from this command that displays the SIP global counters—the error string for immediate context, timestamp for first occurrence of error, and timestamp for last occurrence of error:

```
Device# show sip-ua statistics | sec SIP Global Counters

<File Id, Line: Count  First     Most Recent
    Message>
  0x41, 664   :     2      Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
    main stream, No DNS involved
  0x41, 760   :     2      Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
    resolve_sig_ip_address_to_bind failed
  0x41, 7293  :     10     Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
    Unexpected VoIPCodec Type :%s
  0x41, 10147 :     2      Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
    Offered ptime:%d, Negotiated ptime:%d Negotiated codec bytes: %d for codec %s
  0x41, 10941 :     2      Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
    No voice codec and no dtmf-relay match
  0x41, 13012 :     2      Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
    Media negotiation failed for m-line %d
```

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua status	Displays SIP UA status.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua status

To display status for the Session Initiation Protocol (SIP) user agent (UA), use the **show sip-ua status**command in privileged EXEC mode.

show sip-ua status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	The statistics portion of the output was removed and included in the **show sip-ua statistics** command.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	Command output was enhanced to display if media or signaling binding is enabled, and the style of the DNS SRV query (1 for RFC 2052; 2 for RFC 2782).
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua** command.
12.2(11)T	Command output was enhanced to display information on Session Description Protocol (SDP) application configuration. This command was supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(13)T	Command output was enhanced to display the following: Information on redirection message handling. Information on handling of 180 responses with SDP.
12.2(15)T	Command output was enhanced to display Suspend and Resume support.
12.2(15)ZJ	Command output was enhanced to display information on the duration of dual-tone multifrequency (DTMF) events.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	Command output was enhanced to display Reason Header support.
12.4(22)T	Command output was updated to show IPv6 information.

Release	Modification
Cisco IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use this command to verify SIP configurations.

Examples

The following is sample output from the **show sip-ua status** command:

```
Router# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv4
SDP application configuration:
 Version line (v=) required
 Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

The following is sample output from the **show sip-ua status** command showing IPv6 information:

```
Router# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv6
SDP application configuration:
```

```
 Version line (v=) required
Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

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

Table 9: show sip-ua status Field Descriptions

Field	Description
SIP User Agent Status	UA status.
SIP User Agent for UDP	User Datagram Protocol (UDP) is enabled or disabled.
SIP User Agent for TCP	TCP is enabled or disabled.
SIP User Agent bind status (signaling)	Binding for signaling is enabled or disabled.
SIP User Agent bind status (media)	Binding for media is enabled or disabled.
SIP early-media for 180 responses with SDP	Early media cut-through treatment for 180 responses with SDP can be enabled (the default treatment) or disabled, with local ringback provided.
SIP max-forwards	Value of max-forwards of SIP messages.
SIP DNS SRV version	Style of the DNS SRV query: 1 for RFC 2052 or 2 for RFC 2782.
NAT Settings for the SIP-UA	Symmetric Network Address Translation (NAT) settings when the feature is enabled.
Role in SDP	Identifies the endpoint function in the connection setup procedure during symmetric NAT traversal. The endpoint role may be set to active, meaning that it initiates a connection, or to passive, meaning that it accepts a connection. A value of none in this field means that the feature is disabled.
Check media source packets	Media source packet checking is enabled or disabled.
Maximum duration for a telephone-event in NOTIFYs	Shows the time interval, in milliseconds (ms), between consecutive NOTIFY messages for a telephone event.
SIP support for ISDN SUSPEND/RESUME	Suspend and Resume support is enabled or disabled.
Redirection (3xx) message handling	Redirection can be enabled, which is the default status, according to RFC 2543. Or handling of redirection 3*xx* messages can be disabled, allowing the gateway to treat 3*xx* redirect messages as 4*xx* error messages.
Reason Header will override Response/Request Codes	Reason header is enabled or disabled.

Field	Description
protocol mode is ipv6	States whether the protocol being used is IPv6 or IPv4.
Version line (v=)	Indicates if the SDP version is required.
Owner line (o=)	Indicates if the session originator is required.
Timespec line (t=)	Indicates if the session start and stop times are required.
Media supported	Media information.
Network types supported	Always IN for Internet.
Address types supported	Identifies the Internet Protocol version.
Transport types supported	Identifies the transport protocols supported.

Related Commands

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

show sip-ua status refer-ood

To display the number of incoming and outgoing out-of-dialog REFER (OOD-R) connections, use the **show sip-ua status refer-ood** command in privileged EXEC mode.

show sip-ua status refer-ood

Syntax Description

This command has no arguments or keywords.

Command Modes

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

Use this command to verify OOD-R processing.

Examples

The following is sample output from the **show sip-ua status refer-ood** command:

```
Router# show sip-ua status refer-ood
Maximum allow incoming out-of-dialog refer 500
Current existing incoming out-of-dialog refer dialogs: 1
                 outgoing out-of-dialog refer dialogs: 0
```

The table below describes significant fields shown in this output.

Table 10: show sip-ua status refer-ood Field Descriptions

Field	Description
Maximum allow incoming out-of-dialog refer	Maximum number of incoming OOD-R sessions that the router is allowed. Value set by the **refer-ood enable** command. Default is 500.
Current existing incoming out-of-dialog refer dialogs	Number of currently active incoming OOD-R sessions.
outgoing out-of-dialog refer dialogs	Number of currently active outgoing OOD-R sessions used for line status updates.

Related Commands

Command	Description
refer-ood enable	Enables OOD-R processing.
show sip -ua retry	Displays SIP retry statistics.
show sip -ua statistics	Displays response, traffic, and retry SIP statistics.

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

show sip-ua timers

To display the current settings for the Session Initiation Protocol (SIP) user-agent (UA) timers, use the **show sip-ua timers** command in privileged EXEC mode.

show sip-ua timers

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	The output of this command was changed to reflect the various forms of the timers command.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	Command output was enhanced to display the following: Reliable provisional responses (PRACK/rel 1*xx*), Conditions met (COMET), and NOTIFY responses.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua**command found previously in this reference.
12.2(11)T	This command was supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)YT	Command output was enhanced to display Refer responses.
12.2(15)T	This command was supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.
12.3(1)	Command output was enhanced to display the SIP hold timer value.
12.2(15)ZJ	Command output was enhanced to display Register responses.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	Command output was enhanced to display the buffer-invite timer value and the connection aging timer value.
Cisco IOS XE Bengaluru 17.4.1a	Command output was enhanced to display the time to wait before establishing a TLS connection with the remote server.

Usage Guidelines

Use this command to verify SIP configurations.

Examples

The following is sample output from this command:

```
Router# show sip-ua timers
SIP UA Timer Values (millisecs unless noted)
trying 500, expires 180000, connect 500, disconnect 500
prack 500, rel1xx 500, notify 500, update 500
refer 500, register 500, info 500, options 500,hold 2880 minutes
, register-dns-cache 3600 seconds
tcp/udp aging 5 minutes
tls aging 60 minutes
tls establish 20 seconds
```

The table below describes significant fields shown in this output.

Table 11: show sip-ua timers Field Descriptions

Field	Description
SIP UA Timer Values (millisecs)	SIP UA timer status.
trying	Time to wait before a Trying message is retransmitted.
expires	Time to wait before an Expires message is retransmitted.
connect	Time to wait before a Connect message is retransmitted.
disconnect	Time to wait before a Disconnect message is retransmitted.
prack	Time to wait before a PRACK acknowledgment is retransmitted.
rel1xx	Time to wait before a Rel1*xx* response is retransmitted.
notify	Time to wait before a Notify response is retransmitted.
refer	Time to wait before a Retry request is retransmitted.
register	Time to wait before a Register request is retransmitted.
hold	Time to wait in minutes before a BYE request is sent.
buffer-invite	Time to buffer the INVITE while waiting for display information.
tcp/udp aging	Time to wait in minutes before a TCP or UDP connection is aged out.
tls aging	Time to wait in minutes before a TLS connection is aged out.
tls establish	Time to wait in seconds for establishing a TLS connection with the remote server.

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.

Command	Description
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP UA status.
sip-ua	Enables the SIP user-agent configuration commands.

show spe voice

To display voice-service-history statistics for a specified service processing element (SPE), use the **show spe voice** command in privileged EXEC mode.

show spe voice {[**active**] [*slot* | *slot*/*spe*] | **summary** [*slot* | *slot*/*spe*]}

Syntax Description

slot	All SPEs on the specified slot. Cisco AS5350 range: 1 to 3. Cisco AS5400 range: 1 to 7. Cisco AS5850 range: 0 to 13.
slot / *spe*	Specified SPE on the specified slot. Slot range: as above. SPE range as follows: • Cisco 5350 and Cisco 5400: 0 to 17 • Cisco 5850 (in a CT3_UP216 card): 0 to 35 • Cisco 5850 (in a UP324 card): 0 to 53 You must include the slash mark.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use the *slot* or *slot*/*spe* argument once to specify a single slot or SPE. Use it twice to specify the first and last of a range of slots or SPEs.

The following examples specify the following: a single SPE, a single slot, a range of SPEs in a slot, and a range of slots:

```
show spe voice 1/3
show spe voice 1
show spe voice 1/1 1/3
show spe voice 1 3
```

The **summary** keyword permits you to employ output modifiers to the command so as to write large amounts of data output directly to a file for later reference. You can save this file on local or remote storage devices such as flash, a SAN disk, or an external memory device. You can write output to a new file or append it to an existing file and, optionally at the same time, display it onscreen. Redirection is available using a pipe (|) character combined with the **redirect**, **append**, or **tee** keywords.

For more information on output modifiers, see *Show Command Output Redirection* at the following location: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftshowre.htm

Examples

The following example shows information for a single SPE (slot 2, SPE 1):

```
Router# show spe voice 2/1
#SPE 2/01
```

```
Cisco Universal SPE (Managed); Port 2/6 - 2/11
Last clearing of statistics counters          :  never
         0 Incoming calls                      0 Outgoing calls
   Voice:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 End-point Detection Errors          0 Packets Received Early
         0 Packets Received Late               0 Bad Protocol Headers
   Fax-relay:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 Buffer Underflow Errors             0 End-point Detection Errors
         0 Bad Protocol Headers
Codec         Calls   Codec     Calls   Codec           Calls   Codec     Calls
G.711 u-Law       0   G.729         0   G.723.1 6.3K        0   GSM FR        0
G.711 a-Law       0   G.729B        0   G.723.1 5.3K        0   GSM HR        0
G.726 40K         0   G.729A        0   G.723.1A 6.3K       0   GSM EFR       0
G.726 32K         0   G.729AB       0   G.723.1A 5.3K       0
G.726 24K         0   G.728         0   Clear Channel       0
G.726 16K         0
```

The following example shows summary information:

```
Router# show spe voice summary
Cisco Universal SPE (Managed); Port 1/0 - 1/107
Last clearing of statistics counters          :  never
         0 Incoming calls                      0 Outgoing calls
   Voice:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 End-point Detection Errors          0 Packets Received Early
         0 Packets Received Late               0 Bad Protocol Headers
   Fax-relay:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 Buffer Underflow Errors             0 End-point Detection
Errors
         0 Bad Protocol Headers
Codec         Calls   Codec     Calls   Codec           Calls   Codec       Calls
G.711 u-Law       0   G.729         0   G.723.1 6.3K        0   GSM FR      0
G.711 a-Law       0   G.729B        0   G.723.1 5.3K        0   GSM HR      0
G.726 40K         0   G.729A        0   G.723.1A 6.3K       0   GSM EFR     0
G.726 32K         0   G.729AB       0   G.723.1A 5.3K       0
G.726 24K         0   G.728         0   Clear Channel       0   G.726 16K   0
```

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

Table 12: show spe voice Command Field Descriptions

Field	Description
SPE	Slot and port number of the SPE.
Last Clearing of Statistics Counters	Last time the statistics counters were cleared by means of the **clear spe counters** command.
Buffer Overflow Errors	The digital-signal-processor (DSP) buffer has overflowed. If overflow continues, data will be lost and voice will be distorted (as concealment is added).
Endpoint Detection Errors	A voice frame has arrived after a predefined timer expires, causing the DSP to declare it late. If the frame consists of the SID/marker bit, it causes an endpoint detection error and the late packet is included as an endpoint detection error.

Field	Description
Packets Received Early	The number of frames held in the delay buffer exceeds the expected playout delay -- that is, the delay buffer is overrun (too many frames waiting to be played out for the expected playout delay). At this point, the buffer must reduce the excess delay using intelligent frame deletion to preserve audio continuity.
Packets Received Late	The DSP has received an out-of-sequence packet and started a timer for the missing packet. The packet has failed to arrive in time; it is marked as late and the statistic is incremented. The DSP does interpolative or silence concealment for any missing frames. This type of problem is apt to occur in a congested network and results in lost packets and diminished voice quality.
Bad Protocol Headers	Packets have been rejected for any of the following reasons: bad protocol header, incorrect length, unknown packet format, unknown Real-Time Transport Protocol synchronization source (SSRC), incorrect checksum (when the Extended header is used), cumulative number of packets with invalid RTP headers (the header extension exceeds the packet length), or an invalid User Datagram Protocol (UDP)/IP header if extended encapsulation is enabled.

Related Commands

Command	Description
show spe	Displays SPE status.
show spe modem	Displays modem service-history statistics for a specified SPE.
show spe version	Displays the firmware version on a specified SPE.

show ss7 mtp1 channel-id

To display information for a given session channel ID, use the **show ss7 mtp1 channel-id** command in privileged EXEC mode.

show ss7 mtp1 channel-id [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 23.

Command Default

Information for all channels is displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command is useful for determining which channel IDs have already been allocated.

Examples

The following sample output displays the name of the serial interface for the link, the assigned media gateway controller (MGC) port, whether the link is serial (12-in-1 port) or digital (E1/T1 trunk DS0), the assigned channel ID, and whether the link is stopped or started:

```
Router# show ss7 mtp1 channel-id
  SS7 MTP1 Session-channel [all]:
       channel  assigned interface
       -------  ------------------
           0      7/0:0  (digital)
           1        7/0   (serial)
           3      7/0:1  (digital)
```

The table below describes significant fields shown in this output.

Table 13: show ss7 mtp1 channel-id Field Descriptions

Field	Description
SS7 MTP1 Session-channel	Information about channel IDs.
all	Information on all assigned channel IDs if a particular ID is not specified.
channel	Channel ID assigned by use of the channel-id command.
assigned	Name of the interface serial object to which the channel ID is assigned.
interface	Whether the link type is digital or serial.

The following sample output concerns a specified channel-ID parameter:

```
Router# show ss7 mtp1 channel-id 1

serial interface:  7/0:1 (digital)
  SCC port:          2
  link state:        STARTED
  IDB state:         IDBS_UP
  rcv-pool:
     pool-name:      Rcv07:02
     congested:      FALSE
     in-use buffers: 16
     free buffers:   384
  tx-pool:
     pool-name:      SS7txB01
     in-use buffers: 64
     free buffers:   1236
```

The table below describes significant fields shown in this output.

Table 14: show ss7 mtp1 channel-id Field Descriptions (Specific Channel-ID Selected)

Field	Description
serial interface	Name of the interface serial object and its type (serial or digital).
SCC port	SCC port on the DFC card that was internally assigned by software to service that link (useful to resolve conflicts when trying to create a serial link).
link state	MTP1 link state is started (generally reflects the shutdown and no shutdown entry options.
IDB state	Actual state of the internal Interface Descriptor Block (IDB), which is useful for developers.
rcv-pool	Heading for receive buffer-pool information.
pool-name	Internal name for the pool.
congested	Whether the receive buffers are congested or not.
in-use buffers	How many of the receive buffers are currently in use.
free buffers	How many of the receive buffers are free (not in use).
tx-pool	Heading for transmit buffer-pool information.
pool-name	Internal name for the pool.
in-use buffers	How many of the transmit buffers are currently in use.
free buffers	How many of the transmit buffers are free (not in use).

Related Commands

Command	Description
channel-id	Assigns a session channel ID to an SS7 serial link.
show controllers serial	Displays information about the virtual serial interface.
show ss7 mtp1 links	Displays information for each provisioned SS7 link.

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP 2 Channel Control Block (CCB) information.
show ss7 mtp2 state	Displays internal SS7 Message Transfer Part level 2 (MTP 2) state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
show ss7 mtp2 timers	Displays durations of the SS7 MTP 2 state machine timers.
show ss7 mtp2 variant	Displays information about the SS7 MTP 2 protocol variant.
show ss7 sm session	Displays information about SS7 Session Manager session.
show ss7 sm set	Displays information about the SS7 failover timer.

show ss7 mtp1 links

To display information for each provisioned Signaling System 7 (SS7) link, use the **show ss7 mtp1 links** command in privileged EXEC mode.

show ss7 mtp1 links

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 on the Cisco AS5350 and Cisco AS5400.
12.2(15)T	This command was implemented on the Cisco 2600 series. Command output was also modified.

Usage Guidelines

Use this command to display the name of the serial interface for the link, the assigned media gateway controller (MGC) port, whether the link is serial (12-in-1 port) or digital (E1/T1 trunk DS0), the assigned channel ID, and whether the link is stopped or started. This command is useful for quickly letting you know what links have been assigned and what channel IDs are in use.

The output for this command has been modified for the Cisco AS5350 and Cisco AS5400 to show SS7 session set information. For the Cisco 2600 series, the SCC and state columns have been removed from the output.

Examples

The following sample output shows that there are four SS7 links (out of a platform maximum of four).

Note The SCC chip number is used by Cisco developers who are checking output from the debug ss7 mtp1 commands.

```
Router# show ss7 mtp1 links
     SS7 MTP1 Links [num = 4, platform max = 4]:
                                       session
       interface  type      SCC  state    channel
       ---------  --------  ---  -------  -------
       7/0:0      digital   7/3  STARTED  0
       7/0:1      digital   7/2  STARTED  1
       7/1:0      digital   7/1  STARTED  2
       7/1:1      digital   7/0  STARTED  3
```

The following example displays the interface, type (serial or digital), SCC port, state (started or stopped), SS7 session set (configured or not), and channel ID for all configured SS7 links on a Cisco AS5350 or Cisco AS5400.

```
Router# show ss7 mtp1 links
 SS7 MTP1 Links [num = 4, platform max = 4]:
                                    session session
```

```
 interface   type   SCC     state    channel   set
 --------- -------- --- ------------ ------- -------
    7/0:0  digital  7/3      STARTED     1       0
    7/0:1  digital  7/2      STOPPED    NA      NA
    7/0:2  digital  7/1      STARTED     3       0
      7/0   serial  7/0      STARTED     0       0
```

The following example displays the interface, type (serial or digital), SS7 session set (configured or not), and channel ID for all configured SS7 links on a Cisco 2611 or Cisco 2651. The SCC and state columns have been removed from the output for these platforms.

```
Router# show ss7 mtp1 links
 SS7 MTP1 Links [num = 4, platform max = 4]:
                        session session
    interface   type   channel   set
    --------- -------- ------- -------
         0/0   serial      0       0
         0/1   serial      1       0
       0/2:0  digital      2       1
       0/3:0  digital      3       1
```

The table below describes significant fields shown in this output.

Table 15: show ss7 mtp1 links Field Descriptions

Field	Description
interface	Name of the serial interface for the link.
type	Type of link: serial or digital.
SCC	Assigned MGC port. The SCC chip number is used by Cisco developers to check output from the **debug ss7 mtp1** command.
State	Whether the link is stopped or started.
channel	Assigned channel ID.
session channel	Assigned channel ID.
session set	Assigned SS7 session number.

Related Commands

Command	Description
channel-id	Assigns a session channel ID to an SS7 serial link.
show controllers serial	Displays information about the virtual serial interface.
show ss7 mtp1 links	Displays information for each provisioned SS7 link.
show ss7 mtp2 ccb	Displays SS7 MTP 2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP 2 state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
show ss7 mtp2 timers	Displays durations of the SS7 MTP2 state machine timers.

Command	Description
show ss7 mtp2 variant	Displays information about the SS7 MTP2 protocol variant.
show ss7 sm session	Displays information about an SS7 Session Manager session.
show ss7 sm set	Displays information about the SS7 failover timer.

show ss7 mtp2 ccb

To display Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) call-control block (CCB) information, use the **show ss7 mtp2 ccb**command in privileged EXEC mode.

show ss7 mtp2 ccb [*channel*]

Syntax Description

channel	(Optional) MTP2 serial channel number. Range is from 0 to 3. Default is 0

Command Default

Channel 0. The default is set when you first configure the MTP2 variant. The link must be out of service when you change the variant.

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.
12.3(2)T	The command output was modified to display the following new parameters for the PCR feature: PCR enabled, N2, forced retransmission, and octet count.

Usage Guidelines

The application and meaning of the output is dependent on the MTP2 variant. For example, Japanese Nippon Telephone and Telegraph Cellular System (NTT) and the Japanese Telecommunications Technology Committee (TTC) support only emergency alignment.

Examples

The following is sample output from this command. Output highlighted in bold is for the PCR feature.

```
Router# show ss7 mtp2 ccb 0
SS7 MTP2 Internal Channel Control Block Info for channel 0
Protocol version for channel 0 is Bellcore GR-246-Core Issue 2, Dec 1997
ModuloSeqNumber            = 128   (0x80  )
MaxSeqNumber               = 127   (0x7F  )
Unacked-MSUs (MaxInRTB)    = 127   (0x7F  )
MaxProvingAttempts         = 5     (0x5   )
error_control              = Basic
LSSU_Len                   = 1     (0x1   )
MSU_Len                    = 272   (0x110 )
SUERM-threshold            = 64    (0x40  )
SUERM-number-octets        = 16    (0x10  )
SUERM-number-SUs           = 256   (0x100 )
Tie-AERM-Emergency         = 1     (0x1   )
Tin-AERM-Normal            = 4     (0x4   )
MSU_FISU_Accepted_flag     = TRUE
LSSU_available             = TRUE
AbnormalBSN_flag           = FALSE
AbnormalBSN_flag           = FALSE
UnreasonableBSN            = FALSE
UnreasonableFSN            = FALSE
Abnormal_FIBR_flag         = FALSE
```

```
congestionDiscard           = FALSE
ThisIsA_MSU                 = FALSE
local_processor_outage      = FALSE
remote_processor_outage     = FALSE
provingEmergencyFlag        = TRUE
RemoteProvingEmergencyFlag  = FALSE
further_proving_required    = FALSE
ForceRetransmitFlag         = FALSE
RetransmissionFlag          = FALSE
link_present                = TRUE
Debug Mask                  = 0x0
TX Refc RTB Busy            = 0
TX Refc XTB Fault           = 0
TX Too Long Lost            = 0
TX Enqueue Too Large        = 0
TX Enqueue Failed           = 0
TX CountRTBSlotFull         = 0
TX MaxMSUinXTB              = 0
PCR Enabled                   = TRUE
Forced Retransmission Enabled = TRUE
Forced Retransmission Counts  = 0
N2 Threshhold                 = 4500 octets
N2 Octet-count                = 0 octets
SS7 MTP2 Statistics for channel 0
Protocol version for channel 0 is Bellcore GR-246-Core Issue 2, Dec 1997
OMIACAlignAttemptCount  = 0
OMIACAlignFailCount     = 0
OMIACAlignCompleteCount = 0
OMMSU_TO_XMIT_Count     = 0
OMMSU_XMIT_Count        = 0
OMMSU_RE_XMIT_Count     = 0
OMMSU_RCV_Count         = 0
OMMSU_Posted_Count      = 0
OMMSU_too_long          = 0
OMFISU_XMIT_Count       = 0
OMFISU_RCV_Count        = 0

OMLSSU_XMIT_Count       = 6670
OMLSSU_XMIT_SINCount    = 0
OMLSSU_XMIT_SIECount    = 0
OMLSSU_XMIT_SIOCount    = 6670
OMLSSU_XMIT_SIOSCount   = 0
OMLSSU_XMIT_SIPOCount   = 0
OMLSSU_XMIT_SIBCount    = 0
OMLSSU_RCV_Count        = 0
OMLSSU_RCV_SINCount     = 0
OMLSSU_RCV_SIECount     = 0
OMLSSU_RCV_SIOCount     = 0
OMLSSU_RCV_SIOSCount    = 0
OMLSSU_RCV_SIPOCount    = 0
OMLSSU_RCV_SIBCount     = 0
OMLSSU_RCV_InvalidCount = 0
OMRemote_PO_Count       = 0
OMRemote_Congestion_Cnt = 0
OMtimeINSV (secs)       = 0
OMtimeNotINSV (secs)    = 8
OMMSUBytesTransmitted   = 0
OMMSUBytesReceived      = 0
OMTransmitReqCount      = 7678
OMPDU_notAcceptedCount  = 0
OMPDU_NACK_Count        = 0
OMunreasonableFSN_rcvd  = 0
OMunreasonableBSN_rcvd  = 0
OMT1_TMO_Count          = 0
```

```
OMT2_TMO_Count          = 1
OMT3_TMO_Count          = 0
OMT4_TMO_Count          = 0
OMT5_TMO_Count          = 0
OMT6_TMO_Count          = 0
OMT7_TMO_Count          = 0
OMT8_TMO_Count          = 0
OMTA_TMO_Count          = 0
OMTF_TMO_Count          = 0
OMTO_TMO_Count          = 0
OMTS_TMO_Count          = 0
OMLostTimerCount        = 0
OMOMLostBackHaulMsgs    = 0
OMAERMCount             = 0
OMAERMFailCount         = 0
OMSUERMCount            = 0
OMSUERMFailCount        = 0
OMCongestionCount       = 0
OMCongestionBackhaulCnt = 0
```

The table below describes significant fields shown in this output.

Table 16: show ss7 mtp2 ccb Field Descriptions

Field	Description	Possible Values
PCR Enabled	Whether the error-correction method is set to PCR.	TRUE indicates that PCR is enabled. FALSE indicates that PCR is disabled.
Forced Retransmission	Whether forced retransmission is enabled or disabled.	TRUE indicates that forced-retransmission is enabled. FALSE indicates that forced-retransmission is disabled.
N2 Threshold N2 Octet-count	Status of the N2 parameter and maximum octets available. Number of octets stored in the RTB for an SS7 signaling channel.	--

Related Commands

Command	Description
show ss7 mtp2 state	Displays internal SS7 MTP2 state machine information.

show ss7 mtp2 state

To display internal Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) state-machine information, use the **show ss7 mtp2 state**command in privileged EXEC mode.

show ss7 mtp2 state [*channel*]

Syntax Description

channel	(Optional) MTP2 serial channel number. Range is from 0 to 3. Default is 0.

Command Default

Information for all channels is displayed.

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.
12.3(2)T	The command output was modified to display the following new parameters: PCR enabled and forced retransmission.

Examples

The following example displays the current state of forced retransmission and PCR-enabled flags (shown in bold in the output below):

```
Router# show ss7 mtp2 state 0

SS7 MTP2 states for channel 0
Protocol version for channel 0 is ITU-T Q.703 (1996) (White Book)
  MTP2LSC_INSERVICE        MTP2IAC_IDLE
  MTP2TXC_INSERVICE        MTP2RC_INSERVICE
  MTP2SUERM_MONITORING     MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul  = Abate
Remote Processor Outage  = FALSE
Forced Retransmission    = FALSE
PCR Enabled              = TRUE
N2                       = 800
```

The following is sample output from this command displaying MTP2 state machine information for two different channels:

```
Router# show ss7 mtp2 state 0
SS7 MTP2 states for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
  MTP2LSC_OOS              MTP2IAC_IDLE
  MTP2TXC_INSERVICE        MTP2RC_IDLE
  MTP2SUERM_IDLE           MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul  = Abate
Remote Processor Outage  = FALSE
```

```
Router# show ss7 mtp2 state 1
SS7 MTP2 states for channel 1
Protocol version for channel 1 is Japan NTT Q.703 Version 1-1
  MTP2LSC_OOS              MTP2IAC_IDLE
  MTP2TXC_INSERVICE        MTP2RC_IDLE
  MTP2SUERM_IDLE           MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul  = Abate
Remote Processor Outage  = FALSE
```

The table below describes significant fields shown in this output.

Table 17: show ss7 mtp2 state Field Descriptions

State	Description	Possible Values
MTP2LSC	Overall status of the link.	OOS--Link is out of service. INITIAL_ALIGNMENT--Link is in a transitional link alignment state. ALIGNED_READY--Link is in a transitional link alignment state. ALIGNED_NOT_READY--Link is in a transitional link alignment state. INSERVICE--Link is in service. PROCESSOR_OUTAGE--There is an outage in the local processor. This state implies that the link has been aligned. POWER_OFF--It is possible you don’t have the I/O memory set to at least 40 percent. There may not be enough memory for the SS7 MTP2 signaling.
MTP2IAC	Status of the initial alignment control state machine.	IDLE--State machine is idle. It is not aligning the link. NOT_ALIGNED--State machine has begun the alignment process. ALIGNED-- Link has exchanged the alignment handshake with the remote device. PROVING--Link alignment is being proven. This is a waiting period before the LSC state changes to INSERVICE.
MTP2TXC	Status of the transmission control state machine.	IDLE--State machine is inactive. INSERVICE--State machine is the active transmitter.
MTP2RC	Status of the receive control state machine.	IDLE--State machine is inactive. INSERVICE--State machine is the active receiver.

State	Description	Possible Values
MTP2SUERM	Status of the signal unit error monitor (SUERM).	IDLE--State machine is inactive. MONITORING--SUERM is active. SUERM uses a leaky-bucket algorithm to track link errors while the link is in service. If the number of link errors reaches the threshold, the link is taken out of service.
MTP2AERM	Status of the alignment error rate monitor state machine (AERM).	IDLE--State machine is inactive. MONITORING--Alignment error monitor is active. This is part of the alignment process.
MTP2CONGESTION	Status of the congestion control state machine.	IDLE--State machine is inactive. No congestion is detected; normal traffic flow. ACTIVE--Congestion has been declared. The Cisco 2600 series router is sending SIBs every T5, which indicates that the remote end should stop sending new MSUs until the local Cisco 2600 series router can catch up.
Congestion Backhaul	Congestion status of the backhaul link between the Cisco SLT and the media gateway controller.	Abate--Link between the Cisco 2600 series router and the media gateway controller is not under congestion. Onset--Link between the Cisco 2600 series router and the media gateway controller is under congestion. and the Media Gateway Controller should stop sending new MSUs until the local Cisco 2600 series router can catch up.
Remote Processor Outage	Processor outage status of the remote.	TRUE indicates that the remote is in processor outage. FALSE indicates that the remote has not declared processor outage.
Forced Retransmission	Whether forced retransmission is enabled or disabled.	TRUE--Indicates that forced retransmission is enabled. FALSE--Indicates that forced retransmission is disabled.
PCR Enabled	Whether the error-correction method is set to PCR.	TRUE--Indicates that PCR is enabled. FALSE--Indicates that PCR is disabled.
N2	Status of the N2 parameter.	Octet counts are specified.

Related Commands

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.

show ss7 mtp2 stats

To display Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) operational statistics, use the **show ss7 mtp2 stats** command in privileged EXEC mode.

show ss7 mtp2 stats [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 3.

Command Default

Information for all channels is displayed.

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 operations and maintenance (OM) statistics for MTP2 channel 0:

```
Router# show ss7 mtp2 stats 0
SS7 MTP2 Statistics for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
OMIACAlignAttemptCount  = 0
OMIACAlignFailCount     = 0
OMIACAlignCompleteCount = 0
OMMSU_TO_XMIT_Count     = 0
OMMSU_XMIT_Count        = 0
OMMSU_RE_XMIT_Count     = 0
OMMSU_RCV_Count         = 0
OMMSU_Posted_Count      = 0
OMMSU_too_long          = 0
OMFISU_XMIT_Count       = 0
OMFISU_RCV_Count        = 0
OMLSSU_XMIT_Count       = 17
OMLSSU_XMIT_SINCount    = 0
OMLSSU_XMIT_SIECount    = 0
OMLSSU_XMIT_SIOCount    = 0
OMLSSU_XMIT_SIOSCount   = 17
OMLSSU_XMIT_SIPOCount   = 0
OMLSSU_XMIT_SIBCount    = 0
OMLSSU_RCV_Count        = 0
OMLSSU_RCV_SINCount     = 0
OMLSSU_RCV_SIECount     = 0
OMLSSU_RCV_SIOCount     = 0
OMLSSU_RCV_SIOSCount    = 0
OMLSSU_RCV_SIPOCount    = 0
OMLSSU_RCV_SIBCount     = 0
OMLSSU_RCV_InvalidCount = 0
OMRemote_PO_Count       = 0
OMRemote_Congestion_Cnt = 0
```

```
OMtimeINSV (secs)       = 0
OMtimeNotINSV (secs)    = 9550
OMMSUBytesTransmitted   = 0
OMMSUBytesReceived      = 0
OMTransmitReqCount      = 33
OMPDU_notAcceptedCount  = 0
OMPDU_NACK_Count        = 0
OMunreasonableFSN_rcvd  = 0
OMunreasonableBSN_rcvd  = 0
OMT1_TMO_Count          = 0
OMT2_TMO_Count          = 0
OMT3_TMO_Count          = 0
OMT4_TMO_Count          = 0
OMT5_TMO_Count          = 0
OMT6_TMO_Count          = 0
OMT7_TMO_Count          = 0
OMT8_TMO_Count          = 0
OMTA_TMO_Count          = 0
OMTF_TMO_Count          = 0
OMTO_TMO_Count          = 0
OMTS_TMO_Count          = 477218
OMLostTimerCount        = 0
OMOMLostBackHaulMsgs    = 0
OMAERMCount             = 0
OMAERMFailCount         = 0
OMSUERMCount            = 0
OMSUERMFailCount        = 0
OMCongestionCount       = 0
OMCongestionBackhaulCnt = 0
```

The table below describes significant fields shown in this output.

Table 18: show ss7 mtp2 stats Field Descriptions

Field	Description
OMIACAlignAttemptCount OMIACAlignFailCount OMIACAlignCompleteCount	Counts for Initial Alignment Control (IAC) attempts.
OMMSU_TO_XMIT_Count	Related to the results of the **show ss7 sm stats** command's PDU_pkts_recieve_count statistic. The number shown in OMMSU_TO_XMIT_Count is less than the PDU_pkts_recieve_count because OMMSU_TO_XMIT_Count shows the number of PDUs going out on the link, while the PDU_pkts_recieve_count includes PDUs that are internal to MTP2.
OMMSU_RCV_Count	Related to the results of the **show ss7 sm stats** command's packets_send_count.

Field	Description
OMLSSU_XMIT_Count OMLSSU_XMIT_SINCount OMLSSU_XMIT_SIECount OMLSSU_XMIT_SIOCount OMLSSU_XMIT_SIOSCount OMLSSU_XMIT_SIPOCount OMLSSU_XMIT_SIBCount	Number of times that MTP 2 has posted the specific Link Status Signal Unit (LSSU) to MTP 1. They do *not* show the number of LSSUs actually sent over the link.
OMLSSU_RCV_Count OMLSSU_RCV_SINCount OMLSSU_RCV_SIECount OMLSSU_RCV_SIOCount OMLSSU_RCV_SIOSCount OMLSSU_RCV_SIPOCount OMLSSU_RCV_SIBCount OMLSSU_RCV_InvalidCount	Number of LSSUs received by MTP 2 from MTP 1. Because of MTP 1 filtering, this is *not* the same as the actual LSSUs sent over the link.
OMT1_TMO_Count OMT2_TMO_Count OMT3_TMO_Count OMT4_TMO_Count OMT5_TMO_Count OMT6_TMO_Count OMT7_TMO_Count OMT8_TMO_Count OMTA_TMO_Count OMTF_TMO_Count OMTO_TMO_Count OMTA_TMO_Count OMLostTimerCount	Information about timers in use.
OMLostBackhaulMsgs	How many messages received from the Media Gateway Controller have been lost because of a lack of resources in the Cisco 2600 series router. This count is related to the results of the **show ss7 sm stats** command’s PDU_pkts_recieve_count statistic. For example, if the Media Gateway Controller sends 100 MSUs and the Cisco 2600 series router only has 65 free buffers, 35 MSUs might be lost.

Related Commands

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.
show ss7 mtp2 state	Displays SS7 MTP2 state-machine information.
show ss7 mtp2 timer	Displays durations of the SS7 MTP2 state-machine timers.
show ss7 mtp2 variant	Displays information about the SS7 MTP2 protocol variant.

show ss7 mtp2 timer

To display durations of the Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) state-machine timers, use theshow ss7 mtp2 timer command in privileged EXEC mode.

show ss7 mtp2 timer [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 3.

Command Default

Information for all sessions is displayed.

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

MTP2 uses eight different timers on each link. Throughout the link-state transitions, multiple timers are active. An in-service MTP2 link requires timers that are constantly started, stopped, and restarted. Use this command to display the configured timer durations.

Note All MTP2 configuration parameters are set at the Cisco SLT command-line interface. Media gateway controller parameter data files are no longer used to configure the Cisco SLT.

Note The eight timers whose status is displayed using this command are set on the media gateway controller using MML commands. The timers are then downloaded from the controller to the Cisco signaling link terminal (SLT).

Examples

The following is sample output from this command displaying timer information for channel 0:

```
Router# show ss7 mtp2 timer 0
SS7 MTP2 Timers for channel 0 in milliseconds
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
    T1 aligned/ready = 15000
      T2 not aligned = 5000
          T3 aligned = 3000
T4 Emergency Proving = 3000
   T4 Normal Proving = 3000
      T5 sending SIB = 200
      T6 remote cong = 3000
 T7 excess ack delay = 2000
  T8 errored int mon = 0
```

```
TA SIE timer = 20
       TF FISU timer = 20
        TO SIO timer = 20
       TS SIOS timer = 20
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.
show ss7 mtp2 state	Displays SS7 MTP2 state-machine information.
show ss7 mtp2 stats	Displays SS7 MTP2 operational statistics.
show ss7 mtp2 variant	Displays information about the SS7 MTP2 protocol variant.

show ss7 mtp2 variant

To display information about the Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) protocol variant, use theshow ss7 mtp2 variant command in privileged EXEC mode.

show ss7 mtp2 variant [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 3.

Command Default

Information for all channels is displayed.

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.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5350 and Cisco AS5400.

Usage Guidelines

This command can take an optional channel ID at the end (for example, show ss7 mtp2 variant 0). If the optional channel ID is omitted, the command displays the SS7 variant for all configured SS7 links.

Each country specifies its own variant of SS7, and the Cisco SLT supports several variants of the MTP2 protocol. The selected variant can affect the MTP2 statistics displayed by various commands. The Cisco SLT support the following variants:

- Telcordia Technologies (formerly Bellcore)
- ITU: International Telecommunication Union
- NTT: Japanese Nippon Telephone and Telegraph Cellular System
- TTC: Japanese Telecommunications Technology Committee

Each channel can be configured to any one of the protocol variants. When you change from one variant to another, for example from Bellcore to NTT, the MTP2 parameters default to those specified by NTT. You can then change the defaults as required.

Examples

The following is sample output from this command showing protocol-variant information for channel 1:

```
Router# show ss7 mtp2 variant 1
Protocol version for channel 1 is Bellcore GR-246-Core Issue 2, Dec 1997
```

The following is sample output showing the SS7 variant for the SS7 link whose channel ID is 2:

```
Router# show ss7 mtp2 variant 2
Protocol version for channel 2 is Bellcore GR-246-Core Issue 2, Dec 1997
```

The following is sample output showing the SS7 variant for all configured links:

```
Router# show ss7 mtp2 variant
Protocol version for channel 0 is Bellcore GR-246-Core Issue 2, Dec 1997
Protocol version for channel 1 is Bellcore GR-246-Core Issue 2, Dec 1997
Protocol version for channel 2 is Bellcore GR-246-Core Issue 2, Dec 1997
Protocol version for channel 3 is Bellcore GR-246-Core Issue 2, Dec 1997
```

Field descriptions should be self-explanatory. Note, however, the following:

- In each case, all SS7 links are clearly provisioned to use the Bellcore variant (see the ss7 mtp2 variant bellcore command).
- Command output shows that the MTP2 variant is being used for each of the SS7 links and that the Telcordia Technologies (formerly Bellcore) version is implemented; it also shows where the links are identified by their assigned channel IDs.

Related Commands

Command	Description
show controllers serial	Displays information about the virtual serial interface.
show ss7 mtp1 channel-id	Displays information for a given session channel ID.
show ss7 mtp2 ccb	Displays SS7 MTP 2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP 2 state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
show ss7 mtp2 timers	Displays durations of the SS7 MTP 2 state machine timers.
show ss7 sm session	Displays information about SS7 Session Manager session.
show ss7 sm set	Displays information about the SS7 failover timer.
show ss7 mtp2 ccb	Displays SS7 MTP 2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP 2 state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
ss7 mtp2 variant bellcore	Configures the device for Telcordia Technologies (formerly Bellcore) standards.

show ss7 sm session

To display information about a Signaling System 7 (SS7) Session Manager session, use the show ss7 sm session command in privileged EXEC mode.

show ss7 sm session [*session*]

Syntax Description

session	(Optional) Session. Range is from 0 to 3.

Command Default

Information for all sessions is displayed.

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.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support for up to four Session Manager sessions was added.

Usage Guidelines

If no sessions are configured, the message "No Session is configured" appears.

Support for up to four Session Manager sessions was added in Cisco IOS Release 12.2(11)T. Session Manager sessions are now numbered from 0 to 3. The Cisco Signalling Link Terminal Dual Ethernet feature changes the command-line-interface syntax and adds sessions 2 and 3.

Examples

The following is sample output from this command displaying session information for both sessions:

```
Router# show ss7 sm session
Session[0]: Remote Host 255.255.251.254:8060, Local Host 255.255.255.254:8060
      retrans_t = 600
      cumack_t  = 300
      kp_t      = 2000
      m_retrans = 2
      m_cumack  = 3
      m_outseq  = 3
      m_rcvnum  = 32
Session[1]: Remote Host 255.255.251.255:8061, Local Host 255.255.255.254:8061
      retrans_t = 600
      cumack_t  = 300
      kp_t      = 2000
      m_retrans = 2
      m_cumack  = 3
      m_outseq  = 3
      m_rcvnum  = 32
```

The table below describes significant fields shown in this output.

Table 19: show ss7 sm session Field Descriptions

Field	Description
Remote Host, Local Host	IP address and port number for the session.
retrans_t	Retransmission timer value.
cumack_t	Cumulative acknowledgment timer value.
m_cumack	Maximum number of segments that can be received before the RUDP sends an acknowledgment.
m_outseq	Maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
m_rcvnum	Maximum number of segments that the remote end can send before receiving an acknowledgment.

Related Commands

Command	Description
ss7 session	Establishes a session.
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.

show ss7 sm set

To display information about the Signaling System 7 (SS7) session set state, failover timer , member sessions, and SS7 links that belong to an SS7 session set or range of SS7 session sets, use the show ss7 sm set command in privileged EXEC mode.

show ss7 sm set [*ss-id-range*]

Syntax Description

ss -id -range	(Optional) Displays the SS7 session set ID, state, member sessions, and SS7 links that belong to an SS7 session set or range of SS7 session sets.

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.
12.2(15)T	The ss - id - range argument was added. This command previously displayed only the failover-timer value and had no arguments.

Usage Guidelines

This command is available on all Cisco Signaling Link Terminal (SLT) platforms.

If the optional ss-id-range argument is omitted, information is displayed for all SS7 session sets. The following are valid SS7 session set ranges. The default is 3 seconds.

1	Selects SS7 session set 1 .
0, 2, 3	Selects SS7 session sets 0, 2, and 3.
0-2	Selects SS7 session sets 0, 1, and 2.
0, 2-3	Selects SS7 session sets 0, 2, and 3.
0, 2	Selects SS7 session sets 0 and 2.

Examples

The following is sample output from this command displaying failover timer information; the failover timer is set to the default of 3 seconds:

```
Router# show ss7 sm set
Session Manager Set
      failover timer = 3 seconds
```

The following example displays the SS7 session set state, failover-timer, member sessions, and SS7 links that belong to a range of SS7 session sets:

```
Router# show ss7 sm set
Session-set:0
```

```
  State          = ACTIVE
  Failover-timer = 5 secs.
  2 Sessions:
    session 0  session-state ACTIVE   remote-host 172.16.0.0:5555
    session 1  session-state STANDBY  remote-host 172.31.255.255:4444
  3 SS7 Links:
       7/0 (ser.)    chan-id 0  variant Bellcore   link-state INSERVICE
       7/0:0 (dig.)  chan-id 1  variant Bellcore   link-state INSERVICE
       7/0:2 (dig.)  chan-id 3  variant Bellcore   link-state INITIAL_ALIGNMENT
Session-set:1
  State          = IDLE
  Failover-timer = 5 secs.
  0 Sessions:
  0 SS7 Links:
Session-set:2
  State          = ACTIVE
  Failover-timer = 5 secs.
  2 Sessions:
    session 2  session-state ACTIVE   remote-host 172.16.0.0:6666
    session 3  session-state STANDBY  remote-host 172.31.255.255:7777
  1 SS7 Links:
       7/0:1 (dig.)  chan-id 2  variant Bellcore   link-state INSERVICE
Session-set:3
  State          = IDLE
  Failover-timer = 5 secs.
0 Sessions:
  0 SS7 Links:
```

The table below describes significant fields in this output.

Table 20: show ss7 sm set Field Descriptions

Field	Description
Session-set:0	One of four SS7 session sets is configured.
State	The session is ACTIVE.
Failover-timer	`The number of seconds is set to 5.`
2 Sessions:	• Session 0--session state is ACTIVE and connected to port 5555 of remote-host 172.16.0.0 • Session 1--session state is STANDBY and connected to port 4444 of remote-host 172.31.255.255
3 SS7 Links:	• SS7 link at serial interface 7/0 has channel ID 0 and current MTP2 link state of INSERVICE. • SS7 link at serial interface 7/0:0 has channel ID 1 and current MTP2 link state of INSERVICE. • SS7 link at serial interface 7/0:2 has channel ID 3 and current MTP2 link state of INITIAL_ALIGNMENT.
Session-set:1	One of four SS7 session sets is configured.
State	The session is IDLE.
Failover-timer	The number is set to 5 seconds.

Field	Description
0 Sessions:	No sessions are configured.
0 SS7 Links:	No SS7 links are configured.
Session-set:2	One of four SS7 session sets is configured.
State	The session is ACTIVE.
Failover-timer	`The number is set to 5 seconds.`
2 Sessions:	• Session 2 is ACTIVE and connected to port 6666 of remote host 172.16.0.0 • Session 3 is STANDBY and connected to port 7777 of remote host 172.31.255.255.
1 SS7 Links :	SS7 link at serial interface 7/0:1 has channel ID 2 and current MTP2 link state of INSERVICE.
Session-set:3	One of four SS7 session sets is configured.
State	The session is IDLE.
Failover-timer	The number is set to 5 seconds.
0 Sessions:	No sessions are configured.
0 SS7 Links:	No SS7 links are configured.

Related Commands

Command	Description
ss7 session	Creates a Reliable User Datagram Protocol (RUDP) session and explicitly adds an RUDP session to a Signaling System 7 (SS7) session set.
ss7 set	Independently selects failover-timer values for each session set and specifies the amount of time that the SS7 Session Manager waits for the active session to recover or for the standby media gateway controller (MGC) to indicate that the Cisco Signaling Link Terminal (SLT) should switch traffic to the standby session.
ss7 set failover timer	Specifies the amount of time that the Session Manager waits for the session to recover before declaring the session inactive.

show ss7 sm stats

To display Signaling System 7 (SS7) Session Manager session statistics, use theshow ss7 sm stats command in privileged EXEC mode.

show ss7 sm stats

Syntax Description

There are no arguments or keywords for this command.

Command Default

The command shows information for both sessions.

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

If no sessions are configured, the message "No Session is configured" appears.

Examples

The following is sample output from this command displaying SS7 Session Manager statistics. The fields are self-explanatory and show information about the session state, protocol data units (PDUs) packets sent and received, and SS7 Reliable User Datagram Protocol (RUDP) performance:

```
Router# show ss7 sm stats
-------------------- Session Manager  --------------------
Session Manager state             = SESSION SET STATE-ACTIVE
Session Manager Up count          = 1
Session Manager Down count        = 0
   lost control packet count      = 0
              lost PDU count      = 0
 failover timer expire count      = 0
 invalid_connection_id_count      = 0
Session[0] statistics  SM SESSION STATE-STANDBY:
Session Down count               = 0
   Open Retry count              = 0
   Total Pkts receive count      = 1
   Active Pkts receive count     = 0
   Standby Pkts receive count    = 1
   PDU Pkts receive count        = 0
   Unknown Pkts receive count    = 0
Pkts send count               = 0
   Pkts requeue count            = 0
    -Pkts window full count      = 0
    -Pkts resource unavail count = 0
    -Pkts enqueue fail count     = 0
   PDUs dropped (Large)          = 0
   PDUs dropped (Empty)          = 0
   RUDP Not Ready Errs           = 0
   RUDP Connection Not Open      = 0
   RUDP Invalid Conn Handle      = 0
   RUDP Unknown Errors           = 0
```

```
   RUDP Unknown Signal           = 0
   NonActive Receive count       = 0
Session[1] statistics  SM SESSION STATE-ACTIVE:
Session Down count               = 0
   Open Retry count              = 0
   Total Pkts receive count      = 2440
   Active Pkts receive count     = 1
   Standby Pkts receive count    = 0
   PDU Pkts receive count        = 2439
   Unknown Pkts receive count    = 0
   Pkts send count               = 2905
   Pkts requeue count            = 0
    -Pkts window full count      = 0
    -Pkts resource unavail count = 0
    -Pkts enqueue fail count     = 0
   PDUs dropped (Large)          = 0
   PDUs dropped (Empty)          = 0
   RUDP Not Ready Errs           = 0
   RUDP Connection Not Open      = 0
   RUDP Invalid Conn Handle      = 0
   RUDP Unknown Errors           = 0
   RUDP Unknown Signal           = 0
   NonActive Receive count       = 0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clear ss7 sm-stats	Clears the counters that track Session Manager statistics for the show ss7 sm stats command.
ss7 session	Establishes a session.

show stcapp buffer-history

To display event logs for SCCP Telephony Control Application (STCAPP) analog voice ports, use the **show stcapp buffer-history**command in privileged EXEC mode.

show stcapp buffer-history {**all** | **port** *port*}

Syntax Description

all	Displays event records for all analog voice ports.
port *port*	Displays event records for only the specified analog voice port. **Note** *Port* syntax is platform-dependent; type ? to determine.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

To display event logs with this command, you must first enable event logging using the **debug voip application stcapp buffer-history** command.

Note Using the **all** keyword with this command could increase CPU utilization by as much as 40%.

Examples

The following is sample output from the **show sctapp buffer-history** command showing voice port 2/3 registering with the call-control system, going offhook, and then disconnecting:

```
Router# show stcapp buffer-history port 2/3
1. [2/3], 00:00:44.467
IS [DEVICE_UNREGISTERING] --> IS
2. [2/3], 00:00:44.467
IS [DEVICE_RESETTING] --> OOS
3. [2/3], 00:00:44.467
OOS [DEVICE_DESTROYED] --> STATE_NONE
4. [2/3], 00:00:46.455
STATE_NONE [DEVICE_CREATED] --> OOS
5. [2/3], 00:00:46.455
OOS [DEVICE_REGISTERING] --> INIT
6. [2/3], 00:00:46.607
INIT [STCAPP_DC_EV_DEVICE_REGISTER_DONE] --> INIT
7. [2/3], 00:00:46.607
INIT [STCAPP_DC_EV_DEVICE_CAP_REQ] --> INIT
8. [2/3], 00:00:46.883
INIT [STCAPP_DC_EV_DEVICE_BUTTON_TEMP_RES] --> INIT
9. [2/3], 00:00:46.883
INIT [STCAPP_DC_EV_DEVICE_FORWARD_STAT_RES] --> INIT
10. [2/3], 00:00:47.151
```

```
INIT [STCAPP_DC_EV_DEVICE_LINE_STAT_RES] --> INIT
11. [2/3], 00:00:47.163
INIT [STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS] --> INIT
12. [2/3], 00:00:47.419
IS [STCAPP_DC_EV_DEVICE_DEFINE_DATE_TIME_RES] --> IS
13. [2/3], 00:00:57.079
IDLE [STCAPP_DC_EV_DEVICE_CALL_STATE_ONHOOK] --> IDLE
14. [2/3], 00:00:57.079
IDLE [STCAPP_DC_EV_DEVICE_CALL_STATE_ONHOOK] --> IDLE
15. [2/3], 00:00:57.079
IS [STCAPP_DC_EV_DEVICE_SET_LAMP] --> IS
16. [2/3], 00:00:57.079
IS [STCAPP_DC_EV_DEVICE_SET_LAMP] --> IS
17. [2/3], 00:06:00.923
IDLE [STCAPP_CC_EV_CALL_SETUP_IND] --> OFFHOOK
18. [2/3], 00:06:01.019
OFFHOOK [STCAPP_DC_EV_DEVICE_CALL_STATE_OFFHOOK (245)] --> OFFHOOK
19. [2/3], 00:06:01.023
IS [STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS] --> IS
20. [2/3], 00:06:01.023
OFFHOOK [STCAPP_DC_EV_DEVICE_START_TONE (245)] --> OFFHOOK
21. [2/3], 00:06:01.023
OFFHOOK [STCAPP_CC_EV_CALL_REPORT_DIGITS_DONE] --> OFFHOOK
22. [2/3], 00:06:03.083
OFFHOOK [STCAPP_CC_EV_CALL_DISCONNECTED] --> ONHOOK_DISCONNECT
23. [2/3], 00:06:03.295
IS [STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS] --> IS
24. [2/3], 00:06:03.295
ONHOOK_DISCONNECT [STCAPP_DC_EV_DEVICE_CALL_STATE_ONHOOK (245)] --> IDLE
25. [2/3], 00:06:03.299
IDLE [STCAPP_DC_EV_DEVICE_STOP_TONE (245)] --> IDLE
26. [2/3], 00:06:03.303
IDLE [STCAPP_CC_EV_CALL_DISCONNECT_DONE] --> IDLE
```

Related Commands

Command	Description
debug voip application stcapp buffer-history	Enables event logging for STCAPP analog voice ports.
show stcapp statistics	Displays call statistics for STCAPP analog voice ports.

show stcapp device

To display configuration information about Skinny Client Control Protocol (SCCP) telephony control (STC) application (STCAPP) analog voice ports, use the **show stcapp device** command in privileged EXEC mode.

show stcapp device {**name** *device-name* | **summary** | **voice-port** *port*}

Syntax Description

name *device-name*	Displays information for the analog voice port with the specified device name. The device name is the unique device ID that is assigned to the port when it registers with the call-control system.
summary	Displays a summary of all voice ports.
voice-port *port*	Displays information for the specified analog voice port. **Note** The *port* syntax is platform-dependent; type ? to determine appropriate port numbering.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	This command was modified. Command output was enhanced to display call control block (CCB) and call-control device information.
12.4(4)T	This command was modified. Command output was enhanced to display supported modem transport capability.
12.4(6)XE	This command was modified. Command output was enhanced to display visual message waiting indicator (VMWI) and information for Dial Tone After Remote Onhook feature.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.
15.0(1)XA	This command was modified. Cancel Call Waiting information was added to the command output.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. Command output was enhanced to display the call waiting tone configuration.

Usage Guidelines

Use this command to display configuration and voice interface card (VIC)-specific port information. The Active Call Info field is populated only if a call is active on the voice port.

Examples

The following is a sample output showing IPv6 addresses for the local and remote sites:

```
Router# show stcapp device voice-port 2/0
Port Identifier: 2/0
Device Type: ALG
Device Id: 1
Device Name: AN1AE2853624400
Device Security Mode : None
Modem Capability: None
Device State: IS
Diagnostic: None
Directory Number: 1000
Dial Peer(s): 1000
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event: STCAPP_DC_EV_DEVICE_CALL_INFO
Line State: ACTIVE
Hook State: OFFHOOK
mwi: DISABLE
vmwi: OFF
PLAR: DISABLE
Number of CCBs: 1
Global call info:
Total CCB count = 2
Total call leg count = 4
Call State for Connection 1: TsConnected
Connected Call Info:
Call Reference: 22690511
Local IPv6 Addr: 2001:DB8:C18:1:218:FEFF:FE71:2AB6
Local IP Port: 17424
Remote IPv6 Addr: 2001:DB8:C18:1:218:FEFF:FE71:2AB6
Remote IP Port: 18282
Calling Number: 1000
Called Number:
Codec: g729br8
SRTP: off
```

The following is a sample output from the **show stcapp device** command for an SCCP analog port with VMWI while the Dial Tone After Remote Onhook Feature is activated:

```
Router# show stcapp device voice-port 2/4
Port Identifier:  2/4
Device Type:      ALG
Device Id:        4
Device Name:      AN0C863967C9404
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 7204
Dial Peer(s):     4
Dialtone after remote onhook feature: activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Hook State:       ONHOOK
mwi:              ENABLE
vmwi:             ON
PLAR:             DISABLE
Number of CCBs:   0
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port on a VIC2-2FXS voice interface card specified by the port number:

```
Router# show stcapp device voice-port 1/0/0
Port Identifier:  1/0/0
Device Type:      ALG
Device Id:        3
Device Name:      AN1EBEEB6070200
Device Security Mode : None
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 2099
Dial Peer(s):     999100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
ccw_on:           FALSE
mwi:              DISABLE
vmwi:             OFF
PLAR:             DISABLE
Callback State:   DISABLED
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
    Total call leg count = 0
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port:

```
Router# show stcapp device name AN0C863972F5401
Port Identifier:  2/1
Device Type:      ALG
Device Id:        25
Device Name:      AN0C863972F5401
Device State:     IS
Diagnostic:       None
Directory Number: 9101
Dial Peer(s):     2
Last Event:       STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:       ACTIVE
Hook State:       OFFHOOK
Number of CCBs:   1
Global call info:
    Total CCB count      = 3
    Total call leg count = 6
Call State for Connection 1: TsConnected
Connected Call Info:
   Call Reference: 16777509
   Local IP Addr:  10.1.0.1
   Local IP Port:  18768
   Remote IP Addr: 10.1.0.1
   Remote IP Port: 18542
   Calling Number: 9101
   Called Number:  9102
   Codec:          g711ulaw
```

The following is a sample output from the **show stcapp device** command for STCAPP analog voice ports:

```
Router# show stcapp device summary
Total Devices:           24
```

```
Total Calls in Progress: 3
Total Call Legs in Use:  6
Port       Device          Device   Call          Dev  Directory   Dev
Identifier Name            State    State         Type Number      Cntl
---------- --------------- -------- ------------- ---- ----------- ----
2/1        AN0C863972F5401 IS       ACTIVE         ALG  9101       CCM
2/2        AN0C863972F5402 IS       ACTIVE         ALG  9102       CCM
2/3        AN0C863972F5403 IS       ACTIVE         ALG  9103       CCM
2/0        AN0C863972F5400 IS       IDLE           ALG  9100       CCM
2/4        AN0C863972F5404 IS       IDLE           ALG  9104       CCM
2/5        AN0C863972F5405 IS       IDLE           ALG  9105       CCM
2/6        AN0C863972F5406 IS       IDLE           ALG  9106       CCM
2/7        AN0C863972F5407 IS       IDLE           ALG  9107       CCM
2/8        AN0C863972F5408 IS       IDLE           ALG  9108       CCM
2/9        AN0C863972F5409 IS       IDLE           ALG  9109       CCM
2/10       AN0C863972F540A IS       IDLE           ALG  9110       CCM
2/11       AN0C863972F540B IS       IDLE           ALG  9111       CCM
2/12       AN0C863972F540C IS       IDLE           ALG  9112       CCM
2/13       AN0C863972F540D IS       IDLE           ALG  9113       CCM
2/14       AN0C863972F540E IS       IDLE           ALG  9114       CCM
2/15       AN0C863972F540F IS       IDLE           ALG  9115       CCM
2/16       AN0C863972F5410 IS       IDLE           ALG  9116       CCM
2/17       AN0C863972F5411 IS       IDLE           ALG  9117       CCM
2/18       AN0C863972F5412 IS       IDLE           ALG  9118       CCM
2/19       AN0C863972F5413 IS       IDLE           ALG  9119       CCM
2/20       AN0C863972F5414 IS       IDLE           ALG  9120       CCM
2/21       AN0C863972F5415 IS       IDLE           ALG  9121       CCM
2/22       AN0C863972F5416 IS       IDLE           ALG  9122       CCM
2/23       AN0C863972F5417 IS       IDLE           ALG  9123       CCM
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port:

```
Router# show stcapp device name AN0C86385E3D400
Port Identifier: 2/0
Device Type:      ALG
Device Id:        1
Device Name:      AN0C86385E3D400
Device Security Mode : None
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 2400
Dial Peer(s):     2000
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
mwi:              DISABLE
vmwi:             OFF
mwi config:       Both
Privacy:          Not configured
PLAR:             DISABLE
Callback State:   IDLE
CWT Repetition Interval: 0 second(s)
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
Total call leg count = 0
```

The table below describes the significant fields shown in these displays, in alphabetical order.

Table 21: show stcapp device Field Descriptions

Field	Description
Active Call Info	Displays only when an active call is in progress.
Call Reference	Reference number created by Cisco Unified Communications Manager to track messages associated with a specific call.
Call State	Call processing state: • ACTIVE--Established call connection • IDLE--No call connection • UNREGISTERED--Device is not registered with the Cisco Unified Communications Manager
Called Number	Device called number.
Calling Number	Device calling number.
ccw_on	Displays status of Cancel Call Waiting feature: • False--Inactive on port. • True--Active on port.
Codec	Displays codec type.
CWT Repetition Interval	Displays the call waiting tone configuration.
Dev Cntl	Call-control device that is managing the analog endpoints. CCM represents Cisco Unified Communications Manager. CME represents Cisco Unified Communications Manager Express.
Device Id	Identifier used between the Cisco Unified Communications Manager and gateway to uniquely identify an endpoint.
Device Name	Unique device ID of the analog endpoint. The device ID is derived from an algorithm using the MAC address of the SCCP interface on the voice gateway and the hexadecimal translation of the port's slot number and port number.

Field	Description
Device State	Displays whether device is available for use: • ACTIVE_PENDING--Call is pending certain events before going active. • INFO_RCVD--Call information is received from the Cisco Unified Communications Manager during call setup. • INIT--Waiting to reinitialize. • IS--In service. • OFFHOOK--Device is off-hook. • OFFHOOK_TIMEOUT--Digit timeout occurred while the device is off-hook. • ONHOOK_PENDING--Call is pending certain events before going to the on-hook state. • OOS--Out of service. • PROCEED--Dialed number translation is complete and call setup is in progress. • REM_ONHOOK_PENDING--Call is pending certain events before going to the on-hook state. • RINGING--An incoming call has invoked ringing of the receiving device.
Device Type	Shows phone type: • ALG--Analog. • BRI--ISDN BRI.
Diagnostic	Reason code for a device error condition.
Dial Peer(s)	Dial peer name.
Dialtone after remote onhook feature	Displays feature status: • Activated • Not activated
Directory Number	Assigned to the device by the Cisco Unified Communications Manager.
Last Event	Last event processed by this port.
Local IP Addr	IPv4 address of this gateway used to stream audio using the Real-Time Transport Protocol (RTP).
Local IPv6 Addr	IPv6 address of this gateway used to stream audio using the RTP.

Field	Description
Local IP Port	IP port of this gateway used to stream audio using RTP.
Port Identifier	Identifies the physical voice port.
Remote IP Addr	IPv4 address of the far-end gateway that streams audio using RTP.
Remote IPv6 Addr	IPv6 address of the far-end gateway that streams audio using RTP.
Remote IP Port	IP port of the far-end gateway that streams audio using RTP.
vmwi	Displays LED status: • On • Off

Related Commands

Command	Description
show stcapp statistics	Displays call statistics for STCAPP devices.

show stcapp feature codes

To display current values for feature access codes (FACs), feature speed-dials (FSDs), and feature callback in the SCCP telephony control (STC) application, use the **show stcapp feature codes** command in privileged EXEC mode.

show stcapp feature codes

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(6)T	This command was modified. Speed-dial output was expanded to include number of digits.
12.4(6)XE	This command was modified. This command was enhanced to display standard and feature call-control modes.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(20)YA	This command was modified. Command output was enhanced to include values for callback and meetme-conference.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.0(1)XA	This command was modified. Cancel Call Waiting information was added to the command output.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

This command shows all values for the following in standard and feature mode, depending on the configuration on the Cisco IOS gateway:

- feature access codes (FACs)
- feature speed-dials (FSD)
- feature callback in the STC application

You can enable FACs and FSDs by using the **stcapp feature access-code** and **stcapp feature speed-dial** commands.

You can enable callback by using the **stcapp feature callback** command.

Examples

The following example displays the values for STC application feature codes if FACs and FSDs are not enabled:

```
Router# show stcapp feature codes
```

```
  stcapp feature access-code disabled
  stcapp feature speed-dials disabled
 stxcapp call-control mode is standard
```

The following example shows that feature mode for call-control is enabled:

```
Router# show stcapp feature codes

  stcapp feature speex-dial disabled
  stacapp call-control mode is feature mode
    #1 -- hangup last active call
    #2 - transfer
    #3 - conference
    #4 -- drop last conferee
    #5 -- toggle between two calls
```

The following example displays the default values for all STC application feature codes, including CallBack on Busy and SCCP Meet-Me Conference:

```
Router# show stcapp feature codes

  stcapp feature access-code
    malicious call ID (MCID) ***
    prefix **
    call forward all **1
    call forward cancel **2
    pickup local group **3
    pickup different group **4
    meetme-conference **5
    pickup direct **6
    cancel call waiting **8
  stcapp feature speed-dial
    prefix *
    redial *#
    speeddial number of digit(s) 1
    voicemail *0
    speeddial1 *1
    speeddial2 *2
    speeddial3 *3
    speeddial4 *4
    speeddial5 *5
    speeddial6 *6
    speeddial7 *7
    speeddial8 *8
    speeddial9 *9
  stcapp feature callback
    key #1
    timeout 30
```

The table below describes significant fields shown in the output of this command, in alphabetical order.

Table 22: show stcapp feature codes Field Descriptions

Field	Description
call forward all	FAC prefix plus FAC set by the **call forward all** command.

Field	Description
call forward cancel	FAC prefix plus FAC set by the **call forward cancel**command.
cancel call waiting	FAC prefix plus FAC set by the **cancel-call-waiting**command.
key	Code set for call back on Busy by the **activation-key** command.
meetme-conference	FAC prefix plus FAC set by the **meetme-conference**command.
pickup different group	FAC prefix plus FAC set by the **pickup group** command.
pickup direct	FAC prefix plus FAC set by the **pickup direct**command.
pickup local group	FAC prefix plus FAC set by the **pickup local**command.
prefix	FAC prefix set by the **prefix** (stcapp-fsd) command or by the **prefix (stcapp-fac)**command.
redial	FSD prefix plus FSD code set by the **redial** command.
speeddial number of digit(s)	FSD digit length set by the **digit** command.
speeddial*x*	FSD prefix plus FSD code from the range set by the **speed dial** command.
timeout	Period in seconds for ringing timer set for Call back on Busy by using the **ringing-timeout** command.
voicemail	FSD prefix plus FSD code set by the **voicemail** command.

Related Commands

Command	Description
activation-key	Defines the activation key for Callback on Busy.
call forward all	Designates an STC application feature access code to activate the forwarding of all calls.
call forward cancel	Designates an STC application feature access code to cancel the forwarding of all calls.
digit	Designates the number of digits for STC application feature speed-dial codes.
meetme-conference	Designates an STC application feature access code for meetme-conference.
pickup direct	Designates an STC application feature access code for directed call pickup.
pickup group	Designates an STC application feature access code for group call pickup from another group.
pickup local	Designates an STC application feature access code for group call pickup from the local group.
prefix (stcapp-fac)	Designates a prefix to precede the dialing of an STC application feature access code.

Command	Description
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
ringing-timeout	Defines ringing timer for Callback on Busy.
speed dial	Designates a range of STC application feature speed-dial codes.
stcapp feature callback	Enables CallBack on Busy and enters the STC application feature callback configuration mode
stcapp feature access-code	Enters STC application feature access code configuration mode to set feature access codes.
stcapp feature speed-dial	Enters STC application feature speed-dial configuration mode to set feature speed-dial codes.
voicemail (stcapp-fsd)	Designates an STC application feature speed-dial code to dial the voice-mail number.

show stcapp statistics

To display call statistics for SCCP Telephony Control Application (STCAPP) voice ports, use the s**how stcapp statistics** command in privileged EXEC mode.

show sctapp statistics [**all** | **voice-port** *port-number*]

Syntax Description

voice-port *port-number*	(Optional) Displays information for a specific voice port. • *port-number*-- Number of the port on the interface. Refer to the appropriate platform manual or online help for port numbers on your networking device.
all	(Optional) Displays a summary of all voice ports.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to display call statistics for STCAPP voice ports.

Examples

The following is sample output for the **show sctapp statistics**command for STCAPP voice port 1/0/0.1:

```
Router# show stcapp statistics voice-port 1/0/0.1
STCAPP Device/Call Statistics
    OA = Origination Attempts, TA = Termination Attempts
    Err = Call Errors, PE = Call PreEmptions
Port       DevErr   CallOA   CallTA   CallErr  CallPE
--------- -------- -------- -------- -------- --------
1/0/0.1 0        7        0        0        0
```

The following is sample output for the **show stcapp statistics**command for all STCAPP voice ports:

```
Router# show stcapp statistics all
STCAPP Device/Call Statistics
    OA = Origination Attempts, TA = Termination Attempts
    Err = Call Errors, PE = Call PreEmptions
Port       DevErr   CallOA   CallTA   CallErr  CallPE
--------- -------- -------- -------- -------- --------
1/0/0            0        7        0        0        0
1/0/1            0        0        7        0        0
1/0/3            0        0        0        0        0
1/1/0.1          0        0        0        0        0
1/1/1.1          0        0        0        0        0
1/0/2            0        0        0        0        0
```

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

Table 23: show stcapp statistics Field Descriptions

Field	Description
DevErr	Device errors.
CallOA	Call origination attempts.
CallTA	Call termination attempts.
CallErr	Call errors.
CallPE	Call preemptions.

Related Commands

Command	Description
show stcapp device	Displays configuration information about STCAPP voice ports.

show subscription

To display information about Application Subscribe/Notify Layer (ASNL)-based and non-ASNL-based SIP subscriptions, use the show subscription command in user EXEC or privileged EXEC mode.

show subscription {**asnl session** {**active** | **history** [**errors** | **session-id** *session-id* | **url**] | **statistics**} | **sip**} [**summary**]

Syntax Description

asnl session	ASNL-based subscriptions.
active	Active subscriptions
history	ASNL history table in detailed format.
errors	(Optional) Subscription or notification errors available in the history table.
session-id *session-id*	(Optional) Details of subscriptions matched by session id.
url	(Optional) ASNL subscriptions on a per-URL basis.
statistics	ASNL-based subscriptions.
sip	Both ASNL and non-ASNL based subscriptions.
summary	(Optional) ASNL history table in compact format.

Command Default

No default behavior or values.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to specify options for displaying ASNL and SIP subscription information. If you have a TCL application that uses the SUBSCRIBE and NOTIFY for External Triggers feature, you can use either the show subscription sip or show subscription asnl command to display subscription information. However, the asnl keyword provides more display options.

Examples

The following examples show ASNL-based active subscriptions. The first example displays the information in detail. The second example displays the information in summary form:

```
Router# show subscription asnl session active
ASNL Active Subscription Records Details:
=========================================
Number of active subscriptions: 1
URL: sip:user@10.7.104.88
  Event Name : stress
```

```
  Session ID : 8
  Expiration Time : 50 seconds
  Subscription Duration : 5 seconds
  Protocol : ASNL_PROTO_SIP
  Remote IP address : 10.7.104.88
  Port : 5060
  Call ID : 5
  Total Subscriptions Sent : 1
  Total Subscriptions Received: 0
  Total Notifications Sent : 0
  Total Notifications Received  : 2
  Last response code : ASNL_NOTIFY_RCVD
  Last error code : ASNL_NONE
  First Subscription Time : 10:55:12 UTC Apr 9 2000
  Last Subscription Time : 10:55:12 UTC Apr 9 2000
  First Notify Time : 10:55:12 UTC Apr 9 2000
  Last Notify Time : 10:55:17 UTC Apr 9 2000
  Application that subscribed : stress
  Application receiving notification: stress
Router# show subscription asnl session active summary
ASNL Active Subscription Records Summary:
 =========================================
Number of active subscriptions: 104
SubId      CallId     Proto          URL                                 Event
-----      ------     -----          ---                                 -----
14090      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88                 newstress
14091      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88                 newstress
14092      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88                 newstress
14093      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88                 newstress
14094      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88                 newstress
Subscription HISTORY command (detailed display)
Router# show subscription asnl session history
ASNL Subscription History Records Details:
==========================================
Total history records                            = 1
Total error count                                = 0
Total subscription requests sent                 = 1
Total subscription requests received             = 0
Total notification requests sent                 = 0
Total notification requests received             = 3
URL: sip:user@10.7.104.88
  Event Name : stress
  Session ID : 8
  Expiration Time : 50 seconds
  Subscription Duration : 10 seconds
  Protocol : ASNL_PROTO_SIP
  Remote IP address : 10.7.104.88
  Port : 5060
  Call ID : 5
  Total Subscriptions Sent : 1
  Total Subscriptions Received: 0
  Total Notifications Sent : 0
  Total Notifications Received : 3
  Last response code : ASNL_UNSUBSCRIBE_SUCCESS
  Last error code : ASNL_NONE
  First Subscription Time : 10:55:12 UTC Apr 9 2000
  Last Subscription Time : 10:55:12 UTC Apr 9 2000
  First Notify Time : 10:55:12 UTC Apr 9 2000
  Last Notify Time : 10:55:22 UTC Apr 9 2000
Subscription HISTORY (Summary display)
Router# show subscription asnl session history summary
ASNL Subscription History Records Summary:
==========================================
Total history records = 2
```

```
Total error count = 0
Total subscription requests sent = 2
Total subscription requests received = 0
Total notification requests sent = 0
Total notification requests received = 6
URL                                               Session ID  Call ID
---              ----------  -------
sip:user@10.7.104.88                               9           5
sip:user@10.7.104.88                               8           5
```

The table below describes significant fields in the displays.

Table 24: show subscription Field Descriptions

Field	Description
Last response code	ASNL response codes: ASNL_NONE--Subscription request was initiated. No response has been received from the subscription server. ASNL_SUBSCRIBE_SUCCESS--Subscription request was successful. ASNL_SUBSCRIBE_PENDING--Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED--Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for Transmission Control Protocol (TCP) only. ASNL_SUBSCRIBE_DNS_ERR--Domain Name Server (DNS) error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only.

Field	Description
Last response code (continued)	ASNL_SUBSCRIBE_INTERNAL_CLIENT_ERR--Internal software error occurred while initiating subscription request. ASNL_SUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED--Subscription expired. ASNL_SUBSCRIBE_CLEANUP--Subscription termination initiated from command line interface (CLI). ASNL_UNSUBSCRIBE_SUCCESS--Subscription termination request was successful. ASNL_UNSUBSCRIBE_PENDING--Subscription termination request was sent out. Waiting for a response. ASNL_UNSUBSCRIBE_FAILED --Subscription termination request failed. ASNL_UNSUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription termination request was initiated. ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR--Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription termination request from the client. ASNL_NOTIFY_RCVD--Received a notification request from the subscription server.

Field	Description
Last error code	Subscription error codes: ASNL_SUBSCRIBE_PENDING--Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED--Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_SUBSCRIBE_DNS_ERR--DNS error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_SUBSCRIBE_INTERNAL_CLIENT_ERR--Internal software error occurred while initiating subscription request. ASNL_SUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED--Subscription expired. ASNL_UNSUBSCRIBE_FAILED --Subscription termination request failed. ASNL_UNSUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription termination request was initiated. ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR--Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription termination request from the client.

Related Commands

Command	Description
clear subscription	Clears all active subscriptions or a specific subscription.
debug asnl events	Traces event logs in the ASNL.
subscription asnl session history	Specifies how long to keep ASNL subscription history records and how many history records to keep in memory.

Command	Description
subscription maximum	Specifies the maximum number of outstanding subscriptions to be accepted or originated by a gateway.

show subscription local

To show all the LOCAL Subscribe/Notify Service Provider (SNSP) subscriptions, use the **show subscription local** command in privileged EXEC mode.

show subscription local [**aaa**] [**summary**]

Syntax Description

aaa	(Optional) Subscriptions for voice authentication, authorization, and accounting (AAA) server applications under local SNSP.
summary	(Optional) Summary of all subscriptions.

Command Default

All LOCAL SNSP subscriptions are displayed in detailed format.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display all the subscriptions for voice AAA server applications under LOCAL SNSP in a detailed or summary format.

Examples

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

```
Router# show subscription local
ASNL Active Subscription Records Details:
=========================================
Number of active subscriptions:2
URL:local://aaa
  Event Name                  :accounting-notification
  Session ID                  :1
  Expiration Time             :5000 seconds
  Subscription Duration       :0 seconds
  Protocol                    :ASNL_PROTO_LOCAL
  Call ID                     :N/A
  Total Subscriptions Sent    :1
  Total Notifications Received:1
  Last response code          :ASNL_NOTIFY_RCVD
  Last error code             :ASNL_NONE
  First Subscription Time     :00:48:12 UTC Dec 18 2002
  Last Subscription Time      :00:48:12 UTC Dec 18 2002
  First Notify Time           :00:48:12 UTC Dec 18 2002
  Last Notify Time            :00:48:12 UTC Dec 18 2002
  Application that subscribed       :GAS
  Application receiving notification:N/A
URL:local://aaa
  Event Name                  :accounting-notification
  Session ID                  :2
  Expiration Time             :5000 seconds
  Subscription Duration       :0 seconds
  Protocol                    :ASNL_PROTO_LOCAL
```

```
  Call ID                     :N/A
  Total Subscriptions Received:1
  Total Notifications Sent    :1
  Last response code          :ASNL_NOTIFY_ACCEPT
  Last error code             :ASNL_NONE
  First Subscription Time     :00:48:12 UTC Dec 18 2002
  Last Subscription Time      :00:48:12 UTC Dec 18 2002
  First Notify Time           :00:48:12 UTC Dec 18 2002
  Last Notify Time            :00:48:12 UTC Dec 18 2002
  Server Application   :Voice AAA
  notificationMList    :ml1
  notificationPeriod   :limited
  notificationType     :start-update-stop-accounting-on
  reportAcctFailure    :yes
  subscritpion state   :notify_acked
  notification started :no
```

The following is sample output from the **show subscription local aaa**command:

```
Router# show subscription local aaa
ASNL Active Subscription Records Details:
=========================================
Number of active subscriptions:2
URL:local://aaa
  Event Name                  :accounting-notification
  Session ID                  :2
  Expiration Time             :5000 seconds
  Subscription Duration       :140 seconds
  Protocol                    :ASNL_PROTO_LOCAL
  Call ID                     :N/A
  Total Subscriptions Received:1
  Total Notifications Sent    :2
  Last response code          :ASNL_NOTIFY_ACCEPT
  Last error code             :ASNL_NONE
  First Subscription Time     :00:48:12 UTC Dec 18 2002
  Last Subscription Time      :00:48:12 UTC Dec 18 2002
  First Notify Time           :00:48:12 UTC Dec 18 2002
  Last Notify Time            :00:50:32 UTC Dec 18 2002
  Server Application   :Voice AAA
  notificationMList    :ml1
  notificationPeriod   :limited
  notificationType     :start-update-stop-accounting-on
  reportAcctFailure    :yes
  subscritpion state   :notify_acked
  notification started :yes
```

The table below describes significant fields shown in the displays.

Table 25: show subscription local aaa Field Descriptions

Field	Description
Last response code	ASNL response codes. The field can be one of the following values: ASNL_NONE--Subscription request was initiated. No response has been received from the subscription server. ASNL_SUBSCRIBE_SUCCESS--Subscription request was successful. ASNL_SUBSCRIBE_PENDING--Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED--Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for Transmission Control Protocol (TCP) only. ASNL_SUBSCRIBE_DNS_ERR--Domain Name Server (DNS) error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_SUBSCRIBE_INTERNAL_ERR--Internal software error occurred while initiating subscription request. ASNL_SUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED--Subscription expired. ASNL_SUBSCRIBE_CLEANUP--Subscription termination initiated from command line interface (CLI). ASNL_UNSUBSCRIBE_SUCCESS--Subscription termination request was successful. ASNL_UNSUBSCRIBE_PENDING--Subscription termination request was sent out. Waiting for a response. ASNL_UNSUBSCRIBE_FAILED --Subscription termination request failed.
Last response code (continued)	ASNL_UNSUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription termination request was initiated.

Field	Description
	ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR--Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription termination request from the client. ASNL_NOTIFY_RCVD--Received a notification request from the subscription server.
Last error code	Subscription error codes. The field can be one of the following values: ASNL_SUBSCRIBE_PENDING--Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED--Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_SUBSCRIBE_DNS_ERR--DNS error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_SUBSCRIBE_INTERNAL_ERR--Internal software error occurred while initiating subscription request.

Field	Description
Last error code (continued)	ASNL_SUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED--Subscription expired. ASNL_UNSUBSCRIBE_FAILED --Subscription termination request failed. ASNL_UNSUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription termination request was initiated. ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR--Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription termination request from the client.
notificationMList	String name of the method list of this subscription.
notificationPeriod	• limited--Notifications are started when the first failure status is received while the server is reachable and stopped when the server changes from unreachable to reachable. • infinite--Notifications are started when the subscription begins and stop only when the subscription expires.
notificationType	Type of accounting record for which notification is sent: start, stop, update, or accounting-on.
reportAcctFailure	Indicates whether to send accounting failure responses to the individual application call script before the method list is declared unreachable.
subscription state	When a subscription is completed successfully, the state is notify_acked.

Related Commands

Command	Description
show subscription	Displays information about ASNL-based and non-ASNL-based SIP subscriptions.

show tbct

To display two b-channel transfer (TBCT) related parameters, use the **show tbct** command in privileged EXEC mode.

show tbct

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show tbct** command. The fields in the output are self-explanatory.

```
Router# show tbct
TBCT:
        Maximum no. of TBCT calls allowed: No limit
        Maximum TBCT call duration: No limit
There are no TBCT calls currently being monitored.
```

Related Commands

Command	Description
tbct clear call	Terminates billing statistics for one or more active TBCT calls.
tbct max calls	Sets the maximum number of active calls that can use TBCT.

show tdm mapping

To display digital signal 0 (DS0) to resource mapping information for a time-division multiplexing (TDM) connection, use the **show tdm mapping** command in user EXEC or privileged EXEC mode.

show tdm mapping [**controller** [**e1** *number*] | **slot** *number*]

Syntax Description

controller	(Optional) Displays information about the T1 or E1 controller.
e1	(Optional) Displays information about the E1 controller.
number	(Optional) Specifies the E1 controller unit number.
slot	(Optional) Displays information about a particular modem card slot.
number	(Optional) Specifies the modem card slot number.

Command Default

If no argument is specified, information for all controllers and slots are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Examples

The following is sample output from the **show tdm mapping** command. The fields in the display are self-explanatory.

```
Router# show tdm mapping

T1 1/0:1 is up:
Loopback: NONE
DS0      Resource    Call Type
-----------------------------------
 1        Freedm      DATA
 2        Freedm      DATA
 3        Freedm      DATA
 4        Freedm      DATA
 5        Freedm      DATA
 6        Freedm      DATA
 7        Freedm      DATA
 8        Freedm      DATA
 9        Freedm      DATA
10        Freedm      DATA
11        Freedm      DATA
12        Freedm      DATA
13        Freedm      DATA
14        Freedm      DATA
15        Freedm      DATA
16        0             DATA
17        0             DATA
```

```
18        0            DATA
19        0            DATA
20        0            DATA
21        0            DATA
22        0            DATA
23        0            DATA
24        Freedm       Signaling
T1 1/0:2 is up:
Loopback: NONE
DS0      Resource    Call Type
-----------------------------------
 1        Freedm      DATA
 2        Freedm      DATA
 3        Freedm      DATA
 4        Freedm      DATA
 5        Freedm      DATA
 6        Freedm      DATA
 7        Freedm      DATA
 8        Freedm      DATA
 9        Freedm      DATA
10        Freedm      DATA
11        Freedm      DATA
12        Freedm      DATA
13        Freedm      DATA
14        Freedm      DATA
15        Freedm      DATA
16        0            DATA
17        0            DATA
18        0            DATA
19        0            DATA
20        0            DATA
21        0            DATA
22        0            DATA
23        0            DATA
24        Freedm       Signaling
```

Related Commands

Command	Description
show tdm connections	Displays a snapshot of the TDM bus connection memory in a Cisco access server or displays information about the connection memory programmed on the Mitel TDM chip in a Cisco AS5800 access server.

show tgrep neighbors

To display information about the configured Telephony Gateway Registration Protocol (TGREP) neighbors, use the **show tgrep neighbor**s command in privileged EXEC mode.

show tgrep neighbors {*****_ip-address_}

Syntax Description

*	Displays all neighbors.
ip -address	IP address of the individual neighbor.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Examples

The following is sample output from the **show tgrep neighbors** command:

```
Router# show tgrep neighbors *
There are 1 nbrs configured
------------------ NBR:192.0.2.0----------------------
TIMERS:
        Keepalive :  Timer Stopped
        Hold Timer :  Timer Stopped
        Connect Retry :  Running, time remaining in ms, 20698
SYNC IN PROGRESS
STATE: TRIPS_IDLE
QUEUES:
        writeQ : 0
        sec_writeQ : 0
        readQ : 0
SOCKET FDs:
prim socket -1, sec socket -1
tgrep_update_version : 0
LAST RESET: USER_INITIATED
Router#
Router#!!!! Trip Connection is setup here...
------------------------ OPEN DUMP BEGINS ------------------------
 0x1 0xFFFFFFFF 0x0 0xFFFFFFB4 0x0
 0x0 0x4 0x58 0x6 0x7
 0xFFFFFF98 0xFFFFFFA9 0x0 0xC 0x0
 0x1 0x0 0x8 0x0 0x2
 0x0 0x4 0x0 0x0 0x0
 0x3
        Version    :1
        Hold Time    :180
        My ITAD      :1112
        TRIP ID      :101161129
                 Option Paramater #1
                 Param Type: Capability
```

```
                  Length 8
                          Cap Code :Send Receive Capability
                          Cap Len  :4
                                 Send Rec Cap: RCV ONLY MODE
         -->All route types supported
------------------------ OPEN DUMP ENDS ------------------------
```

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

Table 26: show tgrep neighbors Field Descriptions

Field	Description
TIMERS	Settings for specified timers.
STATE	State of the connection.
QUEUES	The number of writeQ, sec_writeQ, and readQueues are specified in the following three rows.
SOCKET	Socket field description.
LAST RESET	Last reset state.

Related Commands

Command	Description
neighbor (tgrep)	Creates a TGREP session with another device.

show translation-rule

To display the contents of the rules that have been configured for a specific translation name, use the **show translation-rule** command in privileged EXEC mode.

show translation-rule [*name-tag*]

Syntax Description

name -tag	(Optional) Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is from 1 to 2147483647.

Command Default

This command gives detailed information about configured rules under a specific rule name. If the name tag is not entered, a complete display of all the configured rules is shown.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on the Cisco AS5300.
12.0(7)XK	This command was implemented for the following voice technologies on the following platforms: • VoIP (Cisco 2600 series, Cisco 3600 series, and Cisco MC3810) • VoFR (Cisco 2600 series, Cisco 3600 series, and Cisco MC3810) • VoATM (Cisco 3600 series and Cisco MC3810)
12.1(1)T	This command was implemented for VoIP on the Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, and Cisco 7500.
12.1(2)T	This command was implemented for the following voice technologies on the following platforms: • VoIP (Cisco MC3810) • VoFR (Cisco 2600 series, Cisco 3600 series, and Cisco MC3810) • VoATM (Cisco 3600 series and Cisco MC3810)
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following is sample output from this command:

```
Router# show translation-rule
Translation rule address:0x61AB94F8
Tag name:21
Translation rule in_used 1
```

```
**** Xrule rule table *******
        Rule :1
        in_used state:1
        Match pattern:555.%
        Sub  pattern:1408555
        Match  type:subscriber
        Sub type:international
**** Xrule rule table *******
        Rule :2
        in_used state:1
        Match pattern:8.%
        Sub  pattern:1408555
        Match  type:abbreviated
        Sub type:international
Translation rule address:0x61C2E6D4
Tag name:345
Translation rule in_used 1
**** Xrule rule table *******
        Rule :1
        in_used state:1
        Match pattern:.%555.%
        Sub  pattern:7
        Match  type:ANY
        Sub type:abbreviated
```

The table below describes significant fields in this output.

Table 27: show translation-rule Field Descriptions

Translation rule address	Translation rule address in hex.
Tag name	Translation rule tag name.
Translation rule in_used	Translation rule in which the tag is used.
**** Xrule rule table *******	Beginning of the display for a specific rule.
Rule:x	Number of the rule.
in_used state:	Input-searched-pattern.
Match pattern:	Match pattern of the rule.
Sub pattern:	Substituted pattern.
Match type:	Match type.
Sub type:	Substituted pattern match type.

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.

Command	Description
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

show trunk group

To display information for one or more trunk groups, use the **show trunk group** command in user EXEC or privileged EXEC mode.

show trunk group [*name* [**cic**] [**sort** [**ascending** | **descending**]]]

Syntax Description

name	(Optional) Trunk group to display.
cic	(Optional) Displays the Circuit Identification Code (CIC) number.
sort	(Optional) Sorts the output by trunk group number, in ascending or descending order.
ascending	(Optional) Specifies ascending display order for the trunk groups. This is the default.
descending	(Optional) Specifies descending display order for the trunk groups.

Command Default

Trunk groups display in ascending order.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.3(11)T	This command was modified. This command was enhanced to support dial-out trunk groups.
12.4(4)XC	This command was implemented on the Cisco 2600XM series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
15.0(1)XA	This command was modified. The output was enhanced to show the logical partitioning class of restriction (LPCOR) policy for incoming and outgoing calls.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **cic**keyword was added.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Examples

The following sample output shows that for trunk group 1, preemption is enabled, with a preemption tone timer of 10 seconds, and the preemption level is flash.

```
Router# show trunk group 1
Trunk group: 1
        Description:
        trunk group label: 1
        Translation profile (Incoming):
        Translation profile (Outgoing):
```

```
        LPCOR (Incoming): local_group
        LPCOR (Outgoing): local_group
        Preemption is enabled
        Preemption Tone Timer is 10 seconds
        Preemption Guard Timer is 60 milliseconds
        Hunt Scheme is least-used
        Max Calls (Incoming):   NOT-SET (Any)   NOT-SET (Voice) NOT-SET
(Data)
        Max Calls (Outgoing):   NOT-SET (Any)   NOT-SET (Voice) NOT-SET
(Data)
        Retries: 0
        Trunk Se0/3/0:15        Preference DEFAULT
                Member Timeslots : 1-5
                Total channels available : 5
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 5
        Trunk Se0/3/1:15        Preference DEFAULT
                Member Timeslots : 1-2
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
        Trunk Se1/0/0:15        Preference DEFAULT
                Member Timeslots : 1-31
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
        Trunk Se1/0/1:15        Preference DEFAULT
                Member Timeslots : 1-10
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
        Total calls for trunk group: Data = 0, Voice = 0, Modem = 0
                                     Pend = 0, Free = 5
        Preemption Call Type:   Active  Pending
                Flash-Override  NA      0
                Flash           0       0
                Immediate       0       0
                Priority        0       0
                Routine         0       0
                Total           0       0
        Active preemption call-type shows the number of calls
        of each priority level which can be preempted by
        higher preemption level calls.
        Pending preemption call-type shows the number of calls
        of each priority level which are pending for the completion
        of call preemption.
        advertise_flag 0x00000040, capacity timer 25 sec tripl_config_mask 0x00000000
        AC_curr 5, FD_curr 0, SD_curr 0
        succ_curr 0 tot_curr 1
        succ_report 0 tot_report 1
        changed 1 replacement position 0
```

The table below describes the significant fields shown in the output. Fields are listed in alphabetical order.

Table 28: show trunk group Field Descriptions

Field	Description
Description	Description of the trunk group if entered with the **description**(trunk group) command.
trunk group label	Name of the trunk group.
Translation profile (Incoming)	List of incoming translation profiles.

Field	Description
Translation profile (Outgoing)	List of outgoing translation profiles.
LPCOR (Incoming)	Setting of the **lpcor incoming** command.
LPCOR (Outgoing)	Setting of the **lpcor outgoing** command.
Preemption is	Indicates whether preemption is enabled or disabled.
Preemption level	The preemption level for voice calls to be preempted by a DDR call.
Preemption tone timer	The expiry time for the preemption tone for the outgoing calls being preempted by a DDR call.
Hunt Scheme	Name of the idle channel hunt scheme used for this trunk group.
Max calls (incoming)	Maximum number of incoming calls handled by this trunk group.
Max calls (outgoing)	Maximum number of outgoing calls handled by this trunk group.
Retries	Number of times the gateway tries to complete the call on the same trunk group.
Total calls for trunk group	List of the total calls across all trunks in the trunk group.
Preemption Call Type	List of preemption levels for active and pending calls.
Data	Number of currently used data channels on the trunk or total data calls used by the trunk group.
Free	Number of currently available channels on the trunk or total available calls for the trunk group.
Member timeslots	Member timeslots for this trunk.
Pending	Number of pending channels.
Preference	Preference of the trunk in the trunk group. If DEFAULT appears, the trunk does not have a defined preference.
Total channels available	Number of available channels for the trunk.
Trunk group	ID of the trunk group member.
Voice	Number of currently used voice channels on the trunk or total voice calls used by the trunk group.

Related Commands

Command	Description
description (trunk group)	Includes a specific description of the trunk group interface.
hunt-scheme least-idle	Specifies the method for selecting an available incoming or outgoing channel.

Command	Description
trunk group	Initiates a trunk group definition.
trunk group timeslots	Directs an outbound synchronous or asynchronous call initiated by DDR to use specific DS0 channels of an ISDN circuit.

show trunk hdlc

To show the state of the HDLC controllers, use the **show trunk hdlc**command in privileged EXEC mode.

show trunk hdlc {**all** | **ds0** | **slot number**}

Syntax Description

all	Displays information about all the slots with HDLC controllers.
ds0	Displays Ds0 channel availability.
slot	Displays HDLC information about a specific slot.
number	Trunk card slot number.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

The output of the command shows the number of calls on each HDLC controller chip and link. If HDLC calls are failing, this command can help determine if the problem is due to a hardware fault and which controller chip may be responsible.

Examples

The following example displays HDLC controller information for all slots:

```
Router# show trunk hdlc all
HDLC Controller information for slot(s): 0 - 13
  Slot 3:
  Sub-   HDLC   HDLC ctrlrs   TDM links (streams): avail DS0s/total DS0s
  slot   Chip   Avail Total   Link0 Link1 Link2 Link3 Link4 Link5 Link6 Link7
  0      0      128   128     31/31 31/31 31/31 31/31 31/31 31/31 31/31  n/a
  0      1      128   128     31/31 31/31 31/31 31/31 31/31 31/31 31/31  n/a
  Slot 12:
  Sub-   HDLC   HDLC ctrlrs   TDM links (streams): avail DS0s/total DS0s
  slot   Chip   Avail Total   Link0 Link1 Link2 Link3 Link4 Link5 Link6 Link7
  0      0      124   124     31/31 31/31 31/31 31/31  n/a   n/a   n/a   n/a
  0      1      124   124     31/31 31/31 31/31 31/31  n/a   n/a   n/a   n/a
```

Table 29: show trunk hdlc Field Descriptions

Field	Description
Subslot	The DFC slot number upon which the controller resides
HDLC Chip	The chip number within the subslot

Field	Description
HDLC available	The number of HDLC channels available on the chip
ctrlrs total	The total number of HDLC channels on the chip
TDM links	The TDM links connected to the chip
avail DS0s	The number of available DS0s
total DS0s	The total number of DS0s

Related Commands

Command	Description
debug trunk hdlc	Turns on debugging for the HDLC controllers.