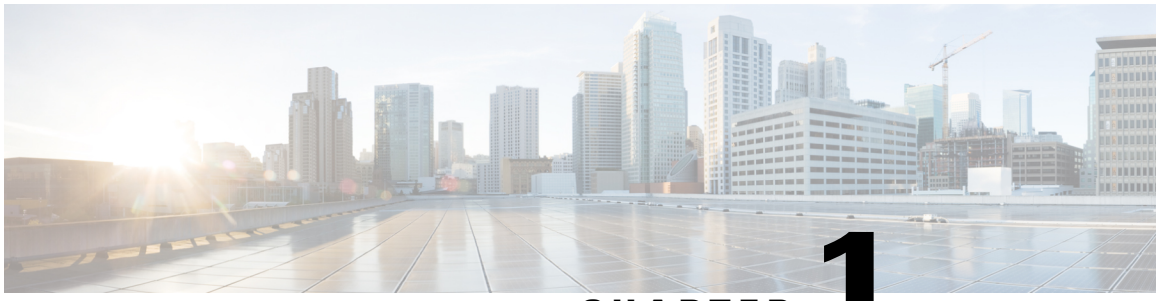
Cisco Unified Border Element (Enterprise) Management Configuration Guide, Cisco IOS XE Release 3S

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco Unified Border Element Enterprise Management

This Cisco Unified Border Element (Enterprise) is a special Cisco IOS XE software image that runs on Cisco ASR1000. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking. This chapter describes basic gateway functionality, software images, topology, and summarizes supported features.

Note Cisco Product Authorization Key (PAK)--A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license .

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Configuration of Cisco UBE Management Features

This chapter contains the following configuration topics:

Monitoring the SIP Trunk

- Out-of-dialog SIP OPTIONS

SNMP Management

- MIB to report call volume and call rate related statistics
- Voice Media Quality MIB

Billing/Accounting

- CDR

Voice Quality Media Statistics

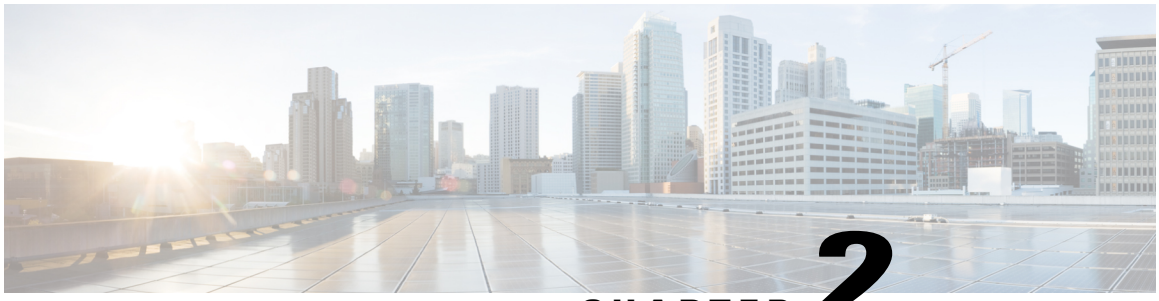
- PCM Capture for ASP and NR

Redundancy - High Availability (HA)

- Stateful Switchover Between Redundancy Paired Intra or Inter-Box Devices

Protocol Monitoring

- Media Inactivity timer based on RTP
- SIP: SIP Support for Options
- The Clearable SIP-US Statistics feature adds MIB support.



CHAPTER 2

Cisco UBE Out-of-dialog OPTIONS Ping

The Cisco Unified Border Element Out-of-dialog (OOD) Options Ping feature provides a keepalive mechanism at the SIP level between any number of destinations.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Out-of-dialog SIP OPTIONS Ping

The following are required for OOD Options ping to function. If any are missing, the Out-of-dialog (OOD) Options ping will not be sent and the dial peer is reset to the default active state.

- Dial-peer should be in active state

- Session protocol must be configured for SIP
- Configure Session target or outbound proxy must be configured. If both are configured, outbound proxy has preference over session target.

Cisco Unified Border Element

- Cisco IOS Release 15.0(1)M or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router

Restrictions for Cisco Out-of-dialog SIP OPTIONS Ping for Specified SIP Servers or Endpoints

- The Cisco Unified Border Element OOD Options ping feature can only be configured at the VoIP Dial-peer level.
- All dial peers start in an active (not busied out) state on a router boot or reboot.
- If a dial-peer has both an outbound proxy and a session target configured, the OOD options ping is sent to the outbound proxy address first.
- Though multiple dial-peers may point to the same SIP server IP address, an independent OOD options ping is sent for each dial-peer.
- If a SIP server is configured as a DNS hostname, OOD Options pings are sent to all the returned addresses until a response is received.
- Configuration for Cisco Unified Border Element OOD and TDM Gateway OOD are different, but can co-exist.

Information about Cisco UBE Out-of-dialog OPTIONS Ping

The Out-of-dialog (OOD) Options Ping feature provides a keepalive mechanism at the SIP level between any number of destinations. A generic heartbeat mechanism allows Cisco Unified Border Element to monitor the status of SIP servers or endpoints and provide the option of busying-out a dial-peer upon total heartbeat failure. When a monitored endpoint heartbeat fails, the dial-peer is busied out. If an alternate dial-peer is configured for the same destination pattern, the call is failed over to the next preferred dial peer, or else the on call is rejected with an error cause code.

The table below describes error codes option ping responses considered unsuccessful and the dial-peer is busied out for following scenarios:

Table 1: Error Codes that busyout the endpoint

Error Code	Description
503	service unavailable
505	sip version not supported
no response	i.e. request timeout

All other error codes, including 400 are considered a valid response and the dial peer is not busied out.

Note The purpose of this feature is to determine if the SIP session protocol on the endpoint is UP and available to handle calls. It may not handle OPTIONS message but as long as the SIP protocol is available, it should be able to handle calls.

When a dial-peer is busied out, Cisco Unified Border Element continues the heartbeat mechanism and the dial-peer is set to active upon receipt of a response.

Configuring Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **voice-class sip options-keepalive** {**up-interval** *seconds* | **down-interval** *seconds* | **retry** *retries*}
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 200 voip`	Enters dial-peer configuration mode for the VoIP peer designated by tag.
Step 4	**voice-class sip options-keepalive** {**up-interval** *seconds* | **down-interval** *seconds* | **retry** *retries*} **Example:** `Device(config-dial-peer)# voice-class sip options-keepalive up-interval 12 down-interval 65 retry 3`	Monitors connectivity between endpoints. • **up-interval seconds** -- Number of up-interval seconds allowed to pass before marking the UA as unavailable.The range is 5-1200. The default is 60. • **down-interval seconds** -- Number of down-interval seconds allowed to pass before marking the UA as unavailable.The range is 5-1200. The default is 30. • **retry retries** -- Number of retry attempts before marking the UA as unavailable. The range is 1 to 10. The default is 5 attempts.
Step 5	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits the current mode.

Troubleshooting Tips

The following commands can help troubleshoot the OOD Options Ping feature:

- **debug ccsip all** --shows all Session Initiation Protocol (SIP)-related debugging.
- **show dial-peer voice x** --shows configuration of keepalive information.

```
Device# show dial-peer voice | in options
voice class sip options-keepalive up-interval 60 down-interval 30 retry 5
voice class sip options-keepalive dial-peer action  = active
```

- **show dial-peer voice summary** --shows Active or Busyout dial-peer status.

```
Device# show dial-peer voice summary
          AD                      PRE PASS
TAG TYPE  MIN  OPER PREFIX    DEST-PATTERN KEEPALIVE
111 voip  up     up              0 syst   active
9  voip   up    down             0 syst   busy-out
```

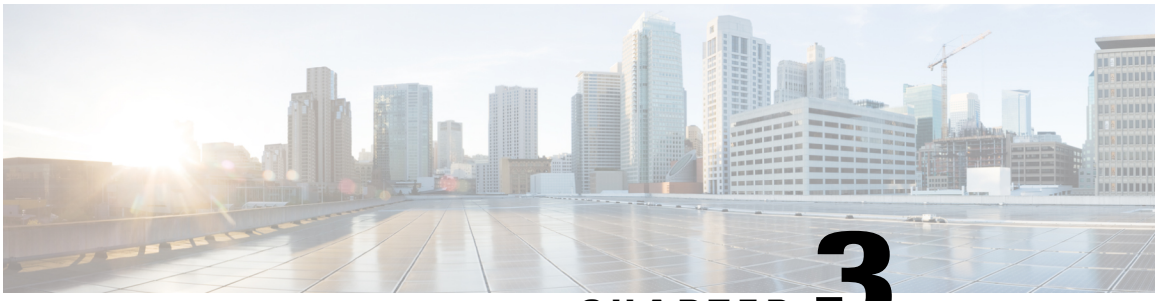
Feature Information for Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints

Feature Name	Releases	Feature Information
Out-of-dialog OPTIONS Ping to Monitor Dial-peers to Specified SIP Servers and Endpoints	15.0(1)M 12.4(22)YB	This feature provides a keepalive mechanism at the SIP level between any number of destinations. The generic heartbeat mechanism allows Cisco UBE to monitor the status of SIP servers or endpoints and provide the option of busying-out associated dial-peer upon total heartbeat failure. In Cisco IOS Release 15.0(1)M, this feature was implemented on the Cisco Unified Border Element. The following command was introduced: **voice-class sip options-keepalive**
Out-of-dialog OPTIONS Ping to Monitor Dial-peers to Specified SIP Servers and Endpoints	Cisco IOS XE Release 3.1S	This feature provides a keepalive mechanism at the SIP level between any number of destinations. The generic heartbeat mechanism allows Cisco UBE to monitor the status of SIP servers or endpoints and provide the option of busying-out associated dial-peer upon total heartbeat failure. In Cisco IOS XE Release 3.1S, this feature was implemented on the Cisco Unified Border Element (Enterprise). The following command was introduced: **voice-class sip options-keepalive**



CHAPTER 3

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about PCM Audio Capture

PCM Audio Capture

The following are the enhancements to the PCM Audio Capture feature:

- Separate PCM capture and Banjo logger feature so that they do not share the same data (.dat) file; they have their own data file.
- One PCM call per data file is generated dynamically. The filename contains information such as voice port type and number, call ID, calling and called number, GUID, DSP channel number, and time stamp.
- A user on the TDM-TDM or TDM-VoIP call can dynamically enable and disable PCM capture by entering predefined start and stop Dual Tone Multi-Frequency (DTMF) digits.
- More test points or streams can be captured.

Note PCM capture is a CPU-intensive feature, and you must not enable several PCM capture sessions while running heavy traffic.

How to Configure PCM Audio Capture

Configuring PCM Audio Capture

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice pcm capture buffer** *number*
4. **voice pcm capture destination** *url*
5. **voice pcm capture on-demand-trigger**
6. **voice pcm capture user-trigger-string** *start-string stop-string* **stream** *bitmap* **duration** *call-duration*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice pcm capture buffer** *number* **Example:** `Router(config)# voice pcm capture buffer 10`	Configures the number of PCM capture buffers. The Range is from 0 to 200000. To change the PCM capture buffer size, you must first configure it with 0 and then configure it with the desired number.
Step 4	**voice pcm capture destination** *url* **Example:** `Router(config)# voice pcm capture destination tftp://10.10.1.2/acphan/`	Configures or changes the destination URL for storing captured data.

	Command or Action	Purpose
Step 5	**voice pcm capture on-demand-trigger** **Example:** `Router(config)# voice pcm capture on-demand-trigger`	Configures user-triggered PCM capture.

Step 6	**voice pcm capture user-trigger-string** *start-string stop-string* **stream** *bitmap* **duration** *call-duration*
	
	Example:
	`Router(config)# voice pcm capture #132 #543 stream ff duration 230`
		Changes the default user trigger PCM capture start and stop string, stream, and duration.
		• The start and stop string must have different values.
		• PCM stream bitmap is in hexadecimal. The range is from 1 to FFFFFFF.
		• The stream bitmap definitions are as follows:
		  • bit 0—Rin
		  • bit 1—Sin
		  • bit 2—Sout
		  • bit 3—nonNLP Sout
		  • bit 4—fax modem in
		  • bit 5—fax modem out
		  • bit 6—from IP network to TDM earpiece direction: ASP input
		  • bit 7—from IP network to TDM earpiece direction: ASP output
		  • bit 8—NR in
		  • bit 9—NR out
		  • bit 10—from TDM mic to IP network: ASP in
		  • bit 11—from TDM mic to IP network: ASP out

Step 7	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Verifying PCM Audio Capture

Perform this task to verify the configuration for the PCM Audio Capture feature.

SUMMARY STEPS

1. **enable**
2. **show voice pcm capture**

DETAILED STEPS

Step 1 **enable**

Example:
```
Router> enable
```

Enables privileged EXEC mode.

Step 2 **show voice pcm capture**

Example:
```
Router# show voice pcm capture

PCM Capture is on and is logging to URL tftp://10.10.1.2/acphan/
50198 messages sent to URL, 0 messages dropped
Message Buffer (total:inuse:free) 200000:0:200000
Buffer Memory: 68000000 bytes, Message size: 340 bytes
```

Displays the configured PCM capture buffer and destination, number of saved messages/packets, number of dropped messages/packets, and number of buffers allocated, both used and free.

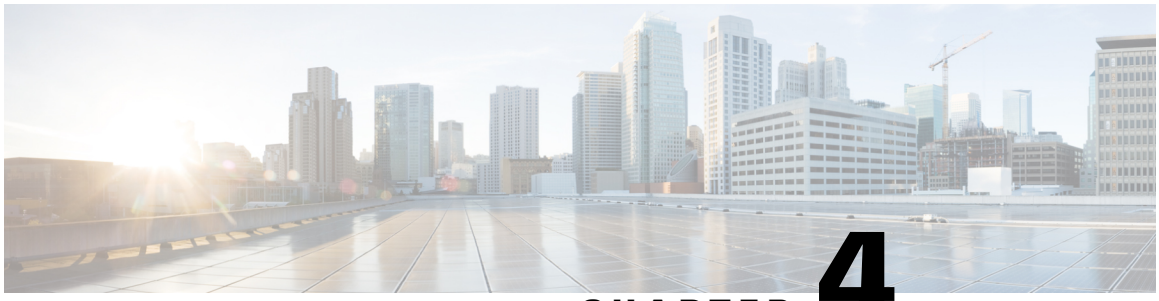
Feature Information for Pulse Code Modulation (PCM) Audio Capture

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for Pulse Code Modulation (PCM) Audio Capture

Feature Name	Releases	Feature Information
Pulse Code Modulation (PCM) Audio Capture	15.2(2)T	The PCM Capture feature is used for debugging audio quality issues. In Cisco IOS Release 15.2(2)T, this feature was implemented on the Cisco Unified Border Element . The following commands were introduced or modified: show voice pcm capture, voice pcm capture.
Pulse Code Modulation (PCM) Audio Capture	Cisco IOS XE Release 3.6S	The PCM Capture feature is used for debugging audio quality issues. In Cisco IOS XE Release 3.6S, this feature was implemented on the Cisco Unified Border Element (Enterprise) The following commands were introduced or modified: show voice pcm capture, voice pcm capture.



CHAPTER 4

Cisco UBE Serviceability

The Cisco UBE Serviceability feature captures the performance metrics of Cisco Unified Border Element (Cisco UBE) periodically based on certain parameters and collects consolidated or filtered information about active calls and Cisco UBE-related configurations.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Cisco UBE Serviceability

Cisco Unified Border Element

- Cisco IOS Release 15.3(1)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.8S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information About Cisco UBE Serviceability

Resource Volume Monitoring

You can use the Cisco UBE Serviceability feature for resource volume monitoring (RVM); that is, you can capture the performance metrics of the Cisco Unified Border Element (Cisco UBE) based on various parameters. The following parameters are supported by Cisco UBE:

- Active calls—The number of concurrent or active calls on the Cisco UBE; these calls may have voice or video media flowing through Cisco UBE and describe the load on memory.
- Call rate—The number of incoming calls handled by Cisco UBE per second. Call rate is crucial to understand the incoming call load.
- Call-leg rate—Call-leg rate is an extension of call legs, where the number of call legs is counted instead of the number of calls. Call legs refer to end-to-end logical connections between two routers or between a telephony device and a router in a VoIP network.
- Short-duration calls—The number of short-duration calls (configurable), indicative of audio issues or dropped calls.
- Session Initiation Protocol (SIP) message rate—The number of SIP messages handled per second. The messages can be received across any transport mechanism and includes all messages received by Cisco UBE.

Each of these parameters is presented in a histogram or tabular format over the past 60 seconds, 60 minutes, and 72 hours. You can also view the call watermarks, that is, the peak values of a parameter (calls or message rate) over a duration.

Consolidated Information of Active Calls and Cisco UBE Configurations

You can combine and filter the output of several **show** commands. It is not required to know several disparate commands related to Session Initiation Protocol (SIP), H.323, audio, video, and so on. You can enter a single command that will consolidate information based on the type of calls that are present at that time. Static configurations pertaining to digital signal processor (DSP) farm and redundancy are also consolidated. You can filter the potentially huge output and display information only for a specific call, called-number, or port. While troubleshooting a specific call, you may find it useful to have a single command that provides all signaling and media information related to that call. The **show cube global** command is used to display the consolidated output.

Monitoring Cisco UBE Serviceability

Perform this task to monitor Cisco UBE serviceability for some parameters. Depending on your requirements, you can capture the performance metrics of the Cisco Unified Border Element (Cisco UBE) based on several parameters or you can collect consolidated information of active calls and configurations related to Cisco UBE. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show call history stats cps table**
3. **show call history watermark cps table**
4. **show sip-ua history stats message-rate**
5. **show cube calls called-number** *called-number*
6. **show cube global**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

Example:
```
Device> enable
```

Step 2 **show call history stats cps table**
Displays the call rate per second for Cisco UBE. The following sample output displays the tabular output of call rate per second for the last 60 seconds, 60 minutes, and 72 hours.

Example:
```
Device# show call history stats cps table

Call switching rate / CPS (last 60 seconds)
Period     Actual     Average
-----------------------------
 1-5          61         12
 6-10         60         12
11-15         60         12
16-20         60         12
21-25         59         12
26-30         60         12
31-35         61         12
36-40         60         12
41-45         60         12
46-50         59         12
51-55         61         12
56-60         61         12

Call switching rate / CPS (last 60 minutes)
Period     Average       Max
---------------------------
 1-5          12         14
 6-10         12         13
11-15         12         13
16-20         12         14
21-25         12         13
26-30         12         14
31-35         12         12
36-40         12         12
41-45         12         12
46-50         12         12
51-55         12         12
56-60         12         12

Call switching rate / CPS (last 72 hours)
```

```
Period     Average       Max
---------------------------
 1-5           7          44
 6-10          0           0
11-15          0           0
16-20          0           0
21-25          0           0
26-30          0           0
31-35         11          52
36-40          0           0
41-45          0           0
46-50          0           0
51-55          0           0
56-60          0           0
61-65          0           0
66-70          0           0
71-72          0           0
```

Step 3 **show call history watermark cps table**

Displays the watermarks for calls per second for Cisco UBE. This following sample output displays in a tabular format the calls per second watermarks (peak values) for the last 60 seconds, 60 minutes, and 72 hours.

Example:

```
Device# show call history watermark cps table

================================================
   Calls Per Second / CPS
================================================
------- The WaterMark Table for Second --------
_____ _____ _____ _____ _____ _____ _____ _____
Value : 0, ts : [Thu, 01 Nov 2012 13:15:24 GMT]
Value : 0, ts : [Thu, 01 Nov 2012 13:15:25 GMT]
Value : 0, ts : [Thu, 01 Nov 2012 13:15:26 GMT]
Value : 1, ts : [Thu, 01 Nov 2012 13:15:27 GMT]
Value : 1, ts : [Thu, 01 Nov 2012 13:15:28 GMT]
================================================

------- The WaterMark Table for Minute-------
_____ _____ _____ _____ _____ _____ _____ _____
Value : 150, ts : [Thu, 01 Nov 2012 13:15:24 GMT]
Value : 120, ts : [Thu, 01 Nov 2012 13:02:20 GMT]
Value : 119, ts : [Thu, 01 Nov 2012 13:25:39 GMT]
Value : 101, ts : [Thu, 01 Nov 2012 13:55:24 GMT]
Value : 101, ts : [Thu, 01 Nov 2012 13:42:28 GMT]
================================================

------- The WaterMark Table for Hour --------
_____ _____ _____ _____ _____ _____ _____ _____
Value : 309, ts : [Wed, 31 Oct 2012 13:15:24 GMT]
Value : 222, ts : [Wed, 31 Oct 2012 16:00:00 GMT]
Value : 169, ts : [Thu, 01 Nov 2012 13:00:30 GMT]
Value : 111, ts : [Thu, 01 Nov 2012 20:10:40 GMT]
Value : 101, ts : [Fri, 01 Nov 2012 17:20:00 GMT]
================================================
```

Step 4 **show sip-ua history stats message-rate**

Displays the incoming SIP messages for Cisco UBE. This following sample output displays in a histogram format the incoming SIP messages for the last 60 seconds, 60 minutes, and 72 hours.

Example:

```
Device# show sip-ua history stats message-rate

      111111111111111111111111111111111111111111111111111111111111111111
      212322221322221222312312313222131322122232132222231213132132
```

```
  20
  19
  18
  17
  16
  15
  14
  13    *     *        *  *  * *    * *      *  *     *   * *  *
  12 * ****** ***** **** ** ** **** * *** ***** ******* * * ** **
  11 ************************************************************
  10 ************************************************************
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
          SIP messages switching rate (last 60 seconds)
         # = SIP Messages entering the module per second


     1111111111111111111111111111111111111111111111111111111111
     3433333333333333333422223242322222222222222222222222222222
  20
  19
  18
  17
  16
  15
  14  *                *      *
  13 ******************    * * *
  12 ###*########################################################
  11 ############################################################
  10 ############################################################
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
         SIP messages switching rate (last 60 minutes)
         * = maximum sip messages/s    # = average sip messages/s



     114                             225
     224                             652
 100
  90
  80
  70
  60
  50                                   *
  40   *                               *
  30   *                              ***
  20   *                              *##
  10 ###                              ###
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
              0    5    0    5    0    5    0    5    0    5    0    5    0
         SIP messages switching rate (last 72 hours)
         * = maximum sip messages/s    # = average sip messages/s
```

Step 5 **show cube calls called-number** *called-number*

Displays the call IDs, calling number, and total number of RTP sessions associated with the called number.

Example:

```
Device# show cube calls media called-number 8000

called number: 8000  info are as the following:
============================================================
============================================================
Phone number 8000 has the following callID associated to it:
============================================================
```

```
callID: 5120, calling number: 2000
callID: 5121, calling number: 2000
=============================================================
A total of 2 rtp sessions for number 8000
=============================================================
```

Step 6 **show cube global**

Displays an overview of the static configurations related to Cisco UBE.

Example:

```
Device# show cube global

This command consolidates the output from the following commands:
-----------------------------------------------------------------------
         show voip rtp high-availability stats
         show sccp all
         show dspfarm all
         show diag
         show redundancy

------------------ show diag ------------------


Slot 0:
        C2951 Mother board 3GE, integrated VPN and 4W Port adapter, 4 ports
        Port adapter is analyzed
        Port adapter insertion time 1w0d ago
        EEPROM contents at hardware discovery:
        PCB Serial Number        : FOC16065YF2
        Hardware Revision        : 1.1
        Part Number              : 73-11836-07
        Top Assy. Part Number    : 800-30793-05
        Board Revision           : B0
        Deviation Number         : 122364
        Fab Version              : 03
        Product (FRU) Number     : CISCO2951/K9
        Version Identifier       : V05
        CLEI Code                : CMMBM00ARC
        Processor type           : C8
        Chassis Serial Number    : FGL161011YC
        Chassis MAC Address      : 442b.0371.9720
        MAC Address block size   : 96
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF C1 8B 46 4F 43 31 36 30 36 35 59 46 32 40
          0x10: 06 15 41 01 01 82 49 2E 3C 07 C0 46 03 20 00 78
          0x20: 49 05 42 42 30 88 00 01 DD FC 02 03 CB 8C 43 49
          0x30: 53 43 4F 32 39 35 31 2F 4B 39 89 56 30 35 20 D9
          0x40: 04 40 C1 CB C2 C6 8A 43 4D 4D 42 4D 30 30 41 52
          0x50: 43 09 C8 C2 8B 46 47 4C 31 36 31 30 31 31 59 43
          0x60: C3 06 44 2B 03 71 97 20 43 00 60 C4 08 00 00 00
          0x70: 00 00 00 00 00 F3 00 03 40 01 63 FF FF FF FF FF
          0x80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x90: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xA0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xB0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xC0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xD0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xE0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xF0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        Internal Power Supply information
        Top Assy. Part Number    : 341-0226-03
        Deviation Number         : 0
        PCB Serial Number        : DCA1552K3AE
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
```

```
RMA History              : 00
Version Identifier       : V03
Product (FRU) Number     : PWR-2921-51-AC
CLEI Code                : 0000000000
Board Revision           : A0
EEPROM format version 4
EEPROM contents (hex):
  0x00: 04 FF 40 05 E2 DF 45 01 55 00 E2 03 88 00 00 00
  0x10: 00 C1 8B 44 43 41 31 35 35 32 4B 33 41 45 03 00
  0x20: 81 00 00 00 00 04 00 89 56 30 33 20 CB 8E 50 57
  0x30: 52 2D 32 39 32 31 2D 35 31 2D 41 43 C6 8A 30 30
  0x40: 30 30 30 30 30 30 30 30 F3 00 59 41 01 22 42 00
  0x50: 05 F8 00 50 01 F3 18 3B 02 F0 19 D9 03 E8 1B 76
  0x60: 04 E2 1C 49 05 D9 1D 1B 06 D8 1D ED 07 CF 1E BF
  0x70: 08 CE 1F 40 09 C2 1F B8 0A B8 20 34 0B B7 20 B0
  0x80: 0D AF 21 0C 0F 9F 21 67 11 91 21 94 13 87 21 C0
  0x90: 17 6E 21 DB 1B 57 21 EA 1F 3F 21 E2 23 28 21 D4
  0xA0: 27 0A 21 CD 42 41 30 FF FF FF FF FF FF FF FF FF
  0xB0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0xC0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0xD0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0xE0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0xF0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

PVDM Slot 0:
32-channel (G.711) Voice/Fax PVDM3 DSP DIMM PVDM daughter card
Hardware Revision        : 1.0
Part Number              : 73-11577-03
Board Revision           : C0
Deviation Number         : 0
Fab Version              : 03
PCB Serial Number        : FOC16093RJM
RMA Test History         : 00
RMA Number               : 0-0-0-0
RMA History              : 00
Processor type           : 00
Product (FRU) Number     : PVDM3-32
Version Identifier       : V01
EEPROM format version 4
EEPROM contents (hex):
  0x00: 04 FF 40 05 D9 41 01 00 82 49 2D 39 03 42 43 30
  0x10: 88 00 00 00 00 02 03 C1 8B 46 4F 43 31 36 30 39
  0x20: 33 52 4A 4D 03 00 81 00 00 00 00 04 00 09 00 CB
  0x30: 8F 50 56 44 4D 33 2D 33 32 20 20 20 20 20 20 20
  0x40: 89 56 30 31 20 D9 02 40 C1 FF FF FF FF FF FF FF
  0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

WIC Slot 3:
HWIC CSU/DSU WAN daughter card
Hardware Revision        : 1.0
Board Revision           : 01
Deviation Number         : 0-0
Fab Version              : 02
PCB Serial Number        : FHH1132004E
RMA Test History         : 00
RMA Number               : 0-0-0-0
RMA History              : 00
Processor type           : 02
Top Assy. Part Number    : 800-28804-01
Product (FRU) Number     : HWIC-1DSU-T1
Version Identifier       : V01
CLEI Code                : TBD
EEPROM format version 4
EEPROM contents (hex):
  0x00: 04 FF 40 05 8A 41 01 00 42 30 31 80 00 00 00 00
  0x10: 02 02 C1 8B 46 48 48 31 31 33 32 30 30 34 45 03
  0x20: 00 81 00 00 00 00 04 00 09 02 C0 46 03 20 00 70
  0x30: 84 01 CB 8C 48 57 49 43 2D 31 44 53 55 2D 54 31
  0x40: 89 56 30 31 00 D9 02 40 C1 C6 8A 54 42 44 00 00
```

```
          0x50: 00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Slot 1:
        Services Module with Services Ready Engine Port adapter, 1 port
        Port adapter is analyzed
        Port adapter insertion time 1w0d ago
        EEPROM contents at hardware discovery:
        Hardware Revision        : 1.0
        Part Number              : 73-13642-01
        Top Assy. Part Number    : 800-35252-01
        Board Revision           : B0
        Deviation Number         : 0
        Fab Version              : 04
        PCB Serial Number        : FOC160308Z3
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Product (FRU) Number     : SM-SRE-910-K9
        Version Identifier       : V01
        CLEI Code                : IPUCA2VBTA
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 07 2D 41 01 00 82 49 35 4A 01 C0 46 03
          0x10: 20 00 89 B4 01 42 42 30 88 00 00 00 00 02 04 C1
          0x20: 8B 46 4F 43 31 36 30 33 30 38 5A 33 03 00 81 00
          0x30: 00 00 00 04 00 CB 8D 53 4D 2D 53 52 45 2D 39 31
          0x40: 30 2D 4B 39 89 56 30 31 20 D9 03 40 C1 CB C6 8A
          0x50: 49 50 55 43 41 32 56 42 54 41 C4 08 00 00 00 00
          0x60: 00 00 00 00 F3 00 06 40 0B E3 43 00 32 FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF


Embedded Service Engine 0/0 :
  Total platform memory : 1048576K bytes
  Total 2nd core memory : 0K bytes
  Start of physical address for 2nd core : 0x20000000
  Number of blocks of memory for 2nd core : 1
  2nd core configured disabled
  L2 cache ways for 2nd core : 0


------------------ show voip rtp high-availability stats ------------------

------------
ACTIVE stats
------------
RTP HA ACTV
(per call leg):     add       mod        del
--------------- ---------- ---------- ----------
                          0          0          0

ACTIVE call-leg stats:


-------------
STANDBY stats
-------------
RTP HA STBY
(per call leg):     add     mod-chg   mod-nochg  del-RBTreeEnt del-freeGccb
--------------- ---------- ---------- ---------- ------------- -------------
                          0          0          0             0             0

STANDBY call-leg stats:


---------------------
STANDBY session stats
---------------------
```

```
RTP HA STBY
(per call):    add        mod        del
---------- ---------- ---------- ----------
                    0          0          0

STANDBY call session stats:


------------------ show sccp all ------------------

SCCP Admin State: DOWN
Gateway Local Interface: None
IP Precedence: 5
User Masked Codec list: None
There is no CCM group configured.

Total number of active session(s) 0, and connection(s) 0


Total number of active session(s) 0, and connection(s) 0


Total number of active session(s) 0, connection(s) 0, and callegs 0

SCCP Application Service(s) Statistics Summary:
Total Conferencing Sessions: 0, Connections: 0
Total Transcoding Sessions: 0, Connections: 0
Total MTP Sessions: 0, Connections: 0
Total ALG-Phone Sessions: 0, Connections: 0
Total BRI-Phone Sessions: 0, Connections: 0
Total SCCP Sessions: 0, Connections: 0
Total Video Conferencing Sessions: 0, Connections: 0
Total Video Transcoding Sessions: 0, Connections: 0


 Total active sessions 0, connections 0, rsvp sessions 0
Statistic                  Count
-------------------------  -----------
Send queue enqueue error   0
Socket send error          694
Msgs discarded upon error  704


------------------ show dspfarm all ------------------

Total number of DSPFARM DSP channel(s) 0


------------------ show redundancy ------------------


Redundant System Information :
------------------------------
       Available system uptime = 0 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = unsupported

                 Hardware Mode = Simplex
             Maintenance Mode = Disabled
               Communications = Down      Reason: Failure

Current Processor Information :
-------------------------------
               Active Location = slot 0
        Current Software state = ACTIVE
       Uptime in current state = 1 week, 2 hours, 10 minutes
                 Image Version = Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version
15.3(BENELLI_PI21_DEV_CBAS_20120903)T, EARLY DEPLOYMENT DEVELOPMENT BUILD, synced to
BEGIN_PI21_SRTG_UC_INDIA
Copyright (c) 1986-2012 by Cisco Systems, Inc.
```

```
Compiled Mon 03-Sep-12 06:40 by nshivamu
                         BOOT = flash0:c2951-universalk9-mz.SSA.BENELLI_PI21_DEV_20120903,1;
        Configuration register = 0x2102

Peer (slot: 0) information is not available because it is in 'DISABLED' state


------------------ show redundancy application group all ------------------


------------------ show redundancy state ------------------

       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
        Unit ID = 0

     Maintenance Mode = Disabled
    Manual Swact = disabled (system is simplex (no peer unit))
 Communications = Down      Reason: Simplex mode

   client count = 12
 client_notification_TMR = 60000 milliseconds
          keep_alive TMR = 4000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 7
           RF debug mask = 0x0


------------------ show redundancy inter-device ------------------

Redundancy inter-device not configured
```

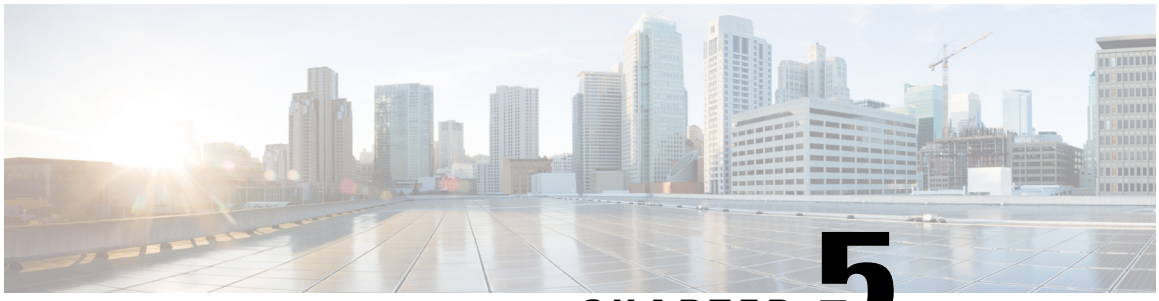
Feature Information for Cisco UBE Serviceability

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for Cisco UBE Serviceability

Feature Name	Releases	Feature Information
Cisco UBE Serviceability	15.3(1)T	The Cisco UBE Serviceability feature captures the performance metrics of Cisco UBE periodically based on certain parameters and collects consolidated or filtered information of active calls and Cisco UBE-related configurations. The following commands were introduced or modified: **show call history stats**, **show call history watermark**, **show cube calls**, **show cube global**, **show sip-ua history**, **voice call duration monitor threshold**, and **voice watermark table-size**.
Cisco UBE Serviceability	For Cisco IOS XE Release 3.8S	The Cisco UBE Serviceability feature captures the performance metrics of Cisco UBE periodically based on certain parameters and collects consolidated or filtered information of active calls and Cisco UBE-related configurations. The following commands were introduced or modified: **show call history stats**, **show call history watermark**, **show cube calls**, **show cube global**, **show sip-ua history**, **voice call duration monitor threshold**, and **voice watermark table-size**.



CHAPTER 5

Cisco UBE Serviceability for Event Logging and Debug Classification

The Cisco Unified Border Element (Cisco UBE) Serviceability for Event Logging and Debug Classification feature helps support, test, and development engineers to troubleshoot during high-density call volumes without significantly impacting performance. This feature introduces a new mechanism for tracing the calls and issues, and generating and collecting needed information, on Cisco UBE via Event Logging.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions

- Traces captured and not written to files will be lost during HA switchover (but they are captured in core).
- Enabling serviceability will write the content to file. As file read/write operation is slow, there will be an impact on performance.
- The dump folder must be reconfigured if cube_et_folder_map.info and et_fold_size files are deleted from flash.
- The dump folder commands must be reconfigured if folder permissions are modified.

Information About Cisco UBE Serviceability for Event Logging and Debug Classification

Serviceability

In a Cisco Unified Border Element (Cisco UBE) system, serviceability refers to the ability of technical support and engineering personnel to troubleshoot issues and restore the service to customers in a high call-volume systems. Cisco UBE includes the following:

- Enhacements to the existing debug logging mechanisms to allow SIP-INFO-DEBUG to be sub-categorized based on importance level (Verbose, Info, Notify, and Critical) and the feature set.
- Cisco UBE Event Trace Manager, which supports tracing for Voice over IP (VoIP) networks.

Event Tracing

Cisco Unified Border Element (Cisco UBE) event tracing enables support, test, and development engineers to debug specific issues related to Cisco UBE. For example, they can use it to identify the root cause of issues that occur in the past. Event -tracing allows various VoIP/SIP events related to the SIP signaling layer of the VoIP call to be traced as they occur. Event tracing provides flexibility to configure the mechanism to a specific customer topology and deployment, including the ability to filter the traces based on call-parameters and time.

Note The event tracing mechanism allows event-trace messages to be written in raw (binary) or encoded (pretty) format.

Debug Message Categories

The Cisco Unified Border Elelment (Cisco UBE) debug categorization mechanism enhances the existing debug framework by adding more filters to control the verbosity. These categories apply to the existing INFO debugs. The messages are subcategorized to control the amount of information logged when info logging in enabled. Therefore, INFO debugs comprise of the following subcategories based on their importance:

- Critical—These errors are feature specific.
- Notification—These errors provide information on important milestones reached.
- Information—These errors provide details to help an engineer understand the workflow.
- Verbose—These errors provide detailed information on all of the above.

The debug messages can also be subcategorized based on a selected feature set (such as SIP profile, fax, audio, or video).

Note Only one level can be selected. By default Verbose level is enabled. The amount of information provided by the debug messages grows in the increasing order of their listing. For example, Notification provides additional information to that provided by the previous category (Critical) and so on.

Dump File and Folder Management

- Event trace generates multiple files for a single call (5 files per call leg for binary dump and 2 files per call leg for text or pretty dump). A CUBE processing calls for a long time can dump a lot of files into a single folder making it difficult to manage the files. Dumping of event traces to folders results in efficient management of event trace files.
- The following storage can be used for creating event trace files.
  - File system: Flash, hard-disk, USB
  - Network storage: FTP, TFTP
- The user must create a directory in the storage before configuring the dump-file.

Note Folder management applies to device storage and external storage where folders can be created and deleted as per configuration. For FTP and TFTP, all files are dumped into a single folder.

New Events and CCSIP Formatting

The following new events are captured by event traces:

- Out-of-band digits.
- Various error conditions (such as codec mismatch, DNS failure are captured to show more details about a call failure).
- Source of call disconnection (disconnect cause code information is captured). Example—*Feb 25 07:21:09.782: sip_misc : CUBE_ET: TYPE = MISC : Call Disconnect: Initiated at: 0x2600674, Originated at:0x2600675, Cause Code = 22*. This example shows the sample event trace captured for call disconnect, which shows cause code and the hexadecimal line number which initiated call disconnect. This is useful for identifying the trigger for call disconnect.

CCSIP Formatting Details—You can export CCSIP formatting details into an XML format based on the release. This can be used to write a decoder to read the content from the binary event trace files.

High Availability Support

- No data is check pointed between the active and standby device.
- Active and standby creates dump files independently.
- You must create the dump-folder manually on both the active and standby devices before configuring the dump folder.
- In a high availability setup, first configure the event trace on the standby device.

How to Configure Cisco UBE Serviceability for Event Logging and Debug Classification

How to Configure Event Tracing

Controlling Cisco UBE Serviceability Event Tracing

Perform this task to disable, clear, and re-enable event traces, export CCSIP formatting details, and to allow the event traces to be stored permanently to secondary or network storage.

SUMMARY STEPS

1. **enable**
2. **monitor event-trace voip ccsip all dump** [**pretty**]
3. **monitor event-trace voip ccsip all disable**
4. **monitor event-trace voip ccsip all clear**
5. **monitor event-trace voip ccsip all enable**
6. **monitor event-trace voip ccsip export format-xml**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**monitor event-trace voip ccsip all dump** [**pretty**]	Writes the event trace results in ASCII format to the file configured with the global configuration **monitor event-trace voip ccsip**

	Command or Action	Purpose
	Example: `Device# monitor event-trace voip ccsip all dump pretty`	**dump-file** command. If you do not specify the **pretty** keyword, the trace messages are saved in binary format.
Step 3	**monitor event-trace voip ccsip all disable** **Example:** `Device# monitor event-trace voip ccsip all disable`	Stops all API, Finite State Machine (FSM), Communicating Nested FSM (CNFSM), message and miscellaneous event tracing.
Step 4	**monitor event-trace voip ccsip all clear** **Example:** `Device# monitor event-trace voip ccsip all clear`	Clear the traces for active calls captured so far.
Step 5	**monitor event-trace voip ccsip all enable** **Example:** `Device# monitor event-trace voip ccsip all enable`	If event-tracing is disabled, this command reenables event tracing for API, FSM, CNFSM, message and miscellaneous events that are configured through global configuration mode. This command does not re-enable global or history event tracing.
Step 6	**monitor event-trace voip ccsip export format-xml** **Example:** `Device# monitor event-trace voip ccsip export format-xml`	Exports CCSIP formatting details into an XML format based on the release. This format can be used to write a decoder to read the content from the binary event trace files. Use this command to get release-specific XML format. This command dumps the XML into the configured event trace folder.

Configuring Cisco UBE Serviceability Event Tracing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor event-trace voip ccsip** *trace-type* [**size** *number*]
4. **monitor event-trace voip ccsip dump** *dump-type*
5. **monitor event-trace voip ccsip dump-file** *file-name*
6. **monitor event-trace voip ccsip limit connections** *max-connections*
7. **monitor event-trace voip ccsip limit memory** *size*
8. **monitor event-trace voip ccsip stacktrace** *number*
9. **monitor event-trace voip ccsip dump-folder size** *size*
10. **monitor event-trace voip ccsip max-dump-limit** *size_in_MB*
11. **monitor event-trace voip ccsip dump all periodic**
12. **monitor event-trace voip ccsip dump marked**
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**monitor event-trace voip ccsip** *trace-type* [**size** *number*] **Example:** `Device(config)# monitor event-trace voip ccsip api size 50`	Enables event tracing for various Voice Over IP (VoIP) CCSIP API events. Event tracing for other events, such as Finite State Machine (FSM), Communicating Nested FSM (CNFSM), miscellaneous, message, and global events can be enabled in a similar way.
Step 4	**monitor event-trace voip ccsip dump** *dump-type* **Example:** `Device(config)# monitor event-trace voip ccsip dump marked`	(Optional) Specifies the automatic dump policy for VoIP CCSIP events. Available options are **marked**, **all**, or **none** (default).

	Command or Action	Purpose

Step 5	**monitor event-trace voip ccsip dump-file** *file-name*
	
	Example:
	
	`Device(config)# monitor event-trace voip ccsip dump-file slot0:ccsip-dump-file`
	`OR`
	`Device(config)#monitor event-trace voip ccsip dump-file ftp://username:password@server_ip//path/ccsip-dump-file`
	
	`OR`
	`Device(config)#monitor event-trace voip ccsip dump-file tftp://server_ip//path/ccsip-dump-file.txt`
		(Optional) Specifies the file where event trace messages are written from memory to permanent storage. You can also configure the folder for the dump-file using the **monitor event-trace voip ccsip dump-file** *folder_path* command. The folder path can be flash:*folder_name*
		
		or bootflash:*folder_name*, usb0:*folder_name*, or harddisk:*folder_name*.
		
		• If there is a failure in configuring the dump file, then a syslog is generated as follows: *%SIP-5-EVENT_TRACE_PATH_ERR: Event Trace Dump PATH "tftp://223.255.254.254/eventtrace" not accesible. Verify credentials, directory path and network connectivity.*

Step 6	**monitor event-trace voip ccsip limit connections** *max-connections* **Example:** `Device(config)# monitor event-trace voip ccsip limit connections 500`	(Optional) Limits the resources used by the event tracing mechanism based on the number of connections or call legs. The default limit is 1000 connections.
Step 7	**monitor event-trace voip ccsip limit memory** *size* **Example:** `Device(config)# monitor event-trace voip ccsip limit memory 50`	(Optional) Limits the resources used by the event tracing mechanism to 50 MBytes.
Step 8	**monitor event-trace voip ccsip stacktrace** *number* **Example:** `Device(config)# monitor event-trace voip ccsip stacktrace 9`	(Optional) Enables the stack trace at tracepoints and specifies the depth of the stack trace stored.

Step 9	**monitor event-trace voip ccsip dump-folder size** *size*
	
	Example:
	
	`Device(config)# monitor event-trace voip ccsip dump-folder size 20`
	`OR`
	`Device(config)# monitor event-trace voip ccsip dump-folder time 500`
		(Optional) Configures the dump-folder size (or time) based on the storage available for the rotation of files. You can also configure the dump-folder time using the **monitor event-trace voip ccsip dump-folder time***time* command.
		
		• Sub-folders are created by CUBE under the user-created folder based on timestamp. When one of the above conditions (size or time) is met, folder rotation happens creating a new folder, and CUBE continues to dump the new event trace files to the new folder.

	Command or Action	Purpose
		• Each folder contains a file et_fold_size, which captures the size of the folder that is used for folder rotation.
Step 10	**monitor event-trace voip ccsip max-dump-limit** *size_in_MB* **Example:** `Device(config)# monitor event-trace voip ccsip max-dump-limit 1000`	(Optional) Sets the limit of the maximum size of event traces. • This command creates a file in flash with the name et_fold_size, which is used to store the current size used by event traces. • Once the event trace size reaches the configured maximum dump limit, then the event trace folder is automatically purged. The folder created first (oldest) is purged first. All files under a folder are deleted in a purge. • Select the maximum-dump-limit based on the space available in storage.
Step 11	**monitor event-trace voip ccsip dump all periodic** **Example:** `Device(config)# monitor event-trace voip ccsip dump all periodic`	(Optional) Dumps the buffer content to file when the buffer is full. • When the buffer is full, the content is written or appended to same file so that all event traces for a particular leg is available in a single file. • Periodic dump is applicable for all and marked dumping. • Periodic dump can be configured for binary or pretty format.
Step 12	**monitor event-trace voip ccsip dump marked** **Example:** `Device(config)# monitor event-trace voip ccsip dump marked`	(Optional) Configures dumping of marked traces. • There are certain conditions, which handle fatal and unexpected events; the call will be disconnected abnormally in such cases. Trace-marks are added to capture these details in event trace. These trace-marks are pre-defined in CUBE and you can configure to dump these traces.
Step 13	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Monitoring Cisco UBE Serviceability Event Tracing

Perform this task to monitor Cisco Unified Border Element (Cisco UBE) serviceability for event tracing and logging parameters. Depending on your requirements, you can view the event traces of the Cisco UBE based on several parameters. The commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show monitor event-trace voip ccsip** *trace-type* **filter called-num** *filter-value* **all**
3. **show monitor event-trace voip ccsip** *trace-type* **all**
4. **show monitor event-trace voip ccsip summary**
5. **show monitor event-trace voip history all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**show monitor event-trace voip ccsip** *trace-type* **filter called-num** *filter-value* **all** **Example:** `Device# show monitor event-trace voip ccsip api filter called-num 88888 all`	Displays the captured event traces for API events for in-progress calls made to the specified number.
Step 3	**show monitor event-trace voip ccsip** *trace-type* **all** **Example:** `Device# show monitor event-trace voip ccsip fsm all`	Displays the captured event traces for Finite State Machine (FSM) and Communicating Nested FSM (CNFSM) events.
Step 4	**show monitor event-trace voip ccsip summary** **Example:** `Device# show monitor event-trace voip ccsip summary`	Displays a summary of all captured event traces.
Step 5	**show monitor event-trace voip history all** **Example:** `Device# show monitor event-trace voip ccsip history all`	Displays the captured traces for completed calls.

Configuring Cisco UBE Serviceability Debug Classification

Perform this task to classify debug messages to support Cisco Unified Border Element (Cisco UBE) serviceability features, and to display Cisco UBE debug category code information.

SUMMARY STEPS

1. **enable**
2. **debug ccsip info**
3. **debug ccsip feature** *feature-name feature-name feature-name feature-name feature-name*
4. **debug ccsip level critical**
5. **show cube debug category codes**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ccsip info** **Example:** `Device# debug ccsip info`	Enables CCSIP INFO debugging.
Step 3	**debug ccsip feature** *feature-name feature-name feature-name feature-name feature-name* **Example:** `Device# debug ccsip feature audio cac dtmf fax registration`	Enables filtering of CCSIP INFO debugs based on various features. Debugs for specified and enabled features are printed.
Step 4	**debug ccsip level critical** **Example:** `Device# debug ccsip level critical`	Enables CCSIP critical level debugging messages.
Step 5	**show cube debug category codes** **Example:** `Device# show cube debug category codes`	Displays Cisco Unified Border Element debug category code information.

Monitoring Active Calls

Perform this task to monitor and display information on the total number of active calls in the system.

SUMMARY STEPS

1. **show call active total-calls**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**show call active total-calls**
	
	Example:
	`Device# show call active total-calls`
	`Total Number of Active Calls : 110`
		Displays the total number of active calls in the system.

Configuration Examples for Cisco UBE Serviceability for Event Logging and Debug Classification

Example: Controlling Cisco UBE Serviceability Event Tracing

The following example shows how to allow the event traces to be stored permanently to secondary storage and how to control event trace logging:

```
Device> enable
Device# monitor event-trace voip ccsip all dump pretty
Device# monitor event-trace voip ccsip all disable
Device# monitor event-trace voip ccsip all clear
Device# monitor event-trace voip ccsip all enable
```

Example: Configuring Cisco UBE Serviceability Event Tracing

The following example shows how to configure event tracing in the system:

```
Device> enable
Device# configure terminal
Device(config)# monitor event-trace voip ccsip api size 50
Device(config)# monitor event-trace voip ccsip fsm size 100
Device(config)# monitor event-trace voip ccsip global size 100
Device(config)# monitor event-trace voip ccsip misc size 50
Device(config)# monitor event-trace voip ccsip msg size 50
Device(config)# monitor event-trace voip ccsip dump marked
```

```
Device(config)# monitor event-trace voip ccsip dump-file slot0:ccsip-dump-file
Device(config)# monitor event-trace voip ccsip limit connections 1000
Device(config)# monitor event-trace voip ccsip stacktrace 9
Device(config)# exit
```

Example: Monitoring Cisco UBE Serviceability Event Tracing

The following example shows how to monitor event tracing in the system:

```
Device> enable
Device# show monitor event-trace voip ccsip api filter called-num 88888 all
Device# show monitor event-trace voip ccsip fsm all
Device# show monitor event-trace voip ccsip summary
Device# show monitor event-trace voip ccsip history all
```

Example: Configuring Cisco UBE Serviceability Debug Classification

The following example shows how to configure debug messages for Cisco Unified Border Element (Cisco UBE) serviceability features:

```
Device> enable
Device# debug ccsip info
SIP Call info tracing is enabled
Device# debug ccsip feature audio cac dtmf fax registration
audio debugging for ccsip info is enabled (active)
fax debugging for ccsip info is enabled (active)
dtmf debugging for ccsip info is enabled (active)
cac debugging for ccsip info is enabled (active)
registration debugging for ccsip info is enabled (active)
Device# debug ccsip level critical
critical mode tracing for ccsip info is enabled (active)
Device# show cube debug category codes

|-----------------------------------------------
| show cube debug category codes values.
|-----------------------------------------------
| Indx |  Debug Name           |   Value
|-----------------------------------------------
|  01  |  SDP Debugs           |   1
|  02  |  Audio Debugs         |   2
|  03  |  Video Debugs         |   4
|  04  |  Fax Debugs           |   8
|  05  |  SRTP Debugs          |   16
|  06  |  DTMF Debugs          |   32
|  07  |  SIP Profiles Debugs  |   64
|  08  |  SDP Passthrough Deb  |   128
|  09  |  Transcoder Debugs    |   256
|  10  |  SIP Transport Debugs |   512
|  11  |  Parse Debugs         |   1024
|  12  |  Config Debugs        |   2048
|  13  |  Control Debugs       |   4096
|  14  |  Miscellaneous Debugs |   8192
|  15  |  Supp Service Debugs  |   16384
|  16  |  Misc  Features Debugs|   32768
|  17  |  SIP Line-side Debugs |   65536
|  18  |  CAC Debugs           |   131072
|  19  |  Registration Debugs  |   262144
|-----------------------------------------------
```

Example: Monitoring Active Calls

The following example shows how to view all active calls in the system:

```
Device> enable
Device# show call active total-calls
Total Number of Active Calls : 110
```

Additional References for Cisco UBE Serviceability for Event Logging and Debug Classification

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Voice commands	• Cisco IOS Voice Command Reference - A through C • Cisco IOS Voice Command Reference - D through I • Cisco IOS Voice Command Reference - K through R • Cisco IOS Voice Command Reference - S Commands • Cisco IOS Voice Command Reference - T through Z Commands

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

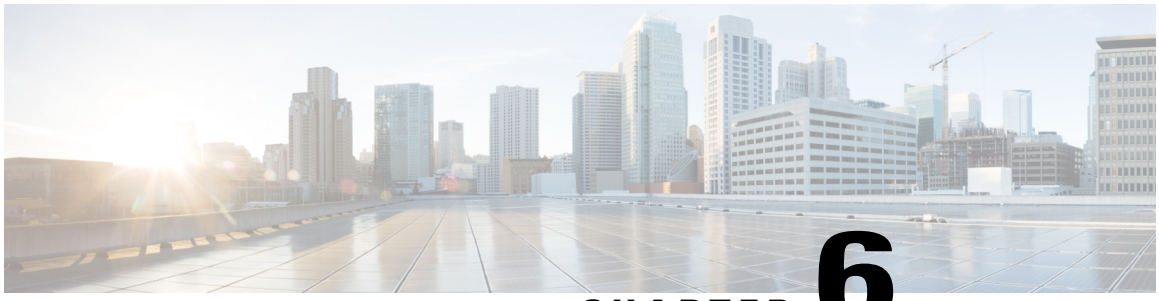
Feature Information for Cisco UBE Serviceability for Event Logging and Debug Classification

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for Cisco UBE Serviceability for Event Logging and Debug Classification

Feature Name	Releases	Feature Information
Cisco UBE Serviceability for Event Logging and Debug Classification	15.3(3)M Cisco IOS Release XE 3.10S	The Cisco Unified Border Element (Cisco UBE) Serviceability for Event Logging and Debug Classification feature helps support, test, and development engineers to troubleshoot during high-density call volumes without significantly impacting performance. This feature introduces a new mechanism for tracing the calls and issues, and generating and collecting needed information, on Cisco UBE via Event Logging. The following commands were introduced or modified: **debug ccsip feature**, **debug ccsip level**, **monitor event-trace voip ccsip**, **monitor event-trace voip ccsip (EXEC)**, **monitor event-trace voip ccsip dump-file**, **monitor event-trace voip ccsip dump**, **monitor event-trace voip ccsip limit**, **monitor event-trace voip ccsip stacktrace**, **show call active total-calls**, **show cube debug category codes**, and **show monitor event-trace voip ccsip (EXEC)**.
Cisco UBE Serviceability Enhancements	15.4(2)T Cisco IOS XE Release 3.12S	The event trace functionality was enhanced with the following: • Dump file and folder management • New events • New dump policy • New trace-mark points for auto-dumping • CCSIP formatting details



CHAPTER 6

StatefulSwitchoverBetweenRedundancyPaired Intra- or Inter-box Devices

Stateful switchover provides protection for network edge devices with dual Route Processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Stateful Switchover Between Redundancy Paired Intra- or Inter-box Devices

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.2 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Cisco Unified Border Element

- Cisco IOS Release 15.2(3)T or a later release must be installed and running on your Cisco Unified Border Element.

Restrictions for Stateful Switchover Between Redundancy Paired Intra- or Inter-box Devices

- Transcoding calls are not check pointed: when failover happens; these calls will not be persevered. The expected behavior is for the SPA card to reset the DSPs and start the firmware download.
- Call escalation and de-escalation are not supported in REFER consumption mode on the Cisco Unified Border Element (Cisco UBE).
- Session Description Protocol (SDP) passthru calls are not supported in REFER consumption mode on the Cisco UBE.
- Secure Real-Time Transport Protocol (SRTP)-Real-Time Transport Protocol (RTP) internetworking between one or multiple Cisco UBEs is not supported.
- SRTP passthrough is not supported on the Cisco UBE.
- Resource Reservation Protocol (RSVP) is not supported on the Cisco UBE.
- Alternative Network Address Types (ANAT) for IPv4 or IPv6 interworking is not supported on the Cisco UBE.
- SDP passthrough calls are not supported for media forking.
- Media flow-around fork calls are not checkpointed.
- For high availability PROTECTED mode, redundancy group (RG) is not supported on cross-over cable. However, if cross-over cable is used and the connection flaps or if the RG link is connected using a switch and the switch resets, or if there is a switchover, then both the devices will go into PROTECTED mode resulting in no VoIP functionality.

Information About Stateful Switchover Between Redundancy Paired Intra- or Inter-box Devices

In specific Cisco networking devices that support dual RPs, stateful switchover takes advantage of Route Processor redundancy to increase network availability. When two route processors (RPs) are installed, one RP acts as the active RP, and the other acts as a backup, or standby RP. Following an initial synchronization between the two processors if the active RP fails, or is manually taken down for maintenance or removed, the standby RP detects the failure and initiates a switchover. During a switchover, the standby RP assumes control of the router, connects with the network interfaces, and activates the local network management interface and system console. Stateful switchover dynamically maintains Route Processor state information between them.

The following conditions and restrictions apply to the current implementation of SSO:

- Calls that are handled by nondefault session application (TCL/VXML) will not be checkpointed prebridge.
- Calls that require a DSP to be inserted (for example: Transcoded Calls) will not be checkpointed.
- Flow-through calls whose state has not been accurately checkpointed will be cleared with media inactivity-based clean up. This condition could occur if active failure happens when:
  - Some check point data has not yet been sent to the standby.
  - The call leg was in the middle of a transaction.
  - Flow around calls whose state has not been accurately checkpointed (due to either of the reasons mentioned above) can be cleared with the **clear call voice causecode** command.

For more information about the Stateful Switchover feature and for detailed procedures for enabling this feature, see the "Configuring Stateful Switchover" chapter of the Cisco IOS High Availability Configuration Guide, Release 12.2SR

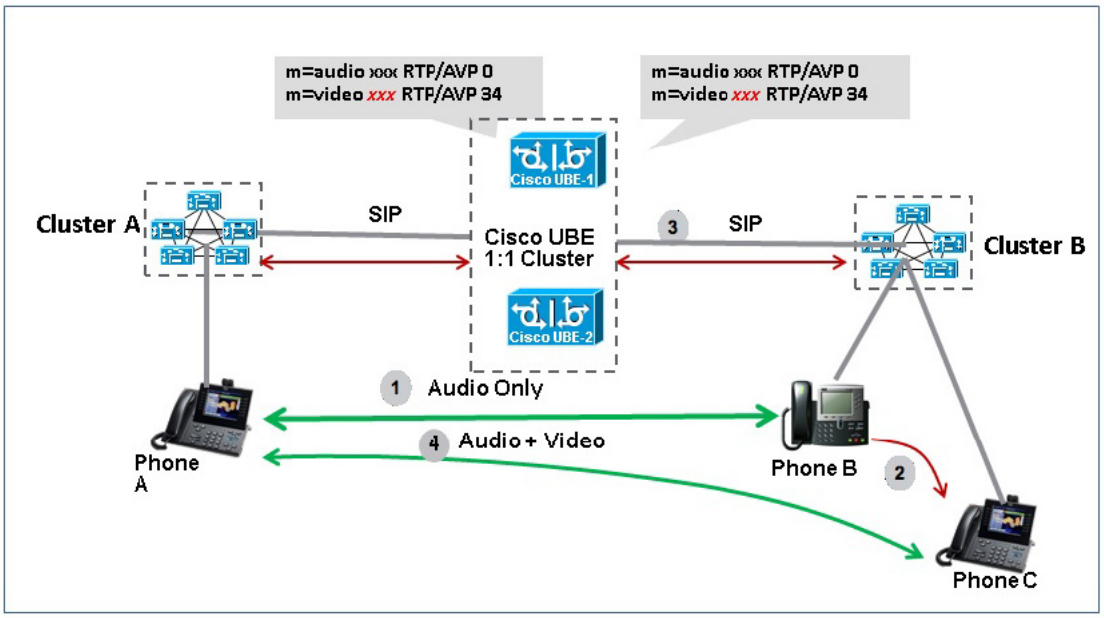
Call Escalation with Stateful Switchover

The call escalation workflow is as follows:

1. The call starts as an audio call between Phone A (video-capable) and Phone B (only audio-capable) registered to two different Cisco Unified Communications Manager (CUCM) clusters connected using Cisco Unified Border Element (Cisco UBE).
2. The call is then transferred to Phone C, which is a video-capable phone.
3. The media parameters within the reinvite are renegotiated end-to-end.
4. The call is escalated to a video call.

Note If the Cisco UBE switchover happens at any instance, then audio calls will be preserved before escalation and video calls will be preserved after escalation.

Figure 1: Call Escalation



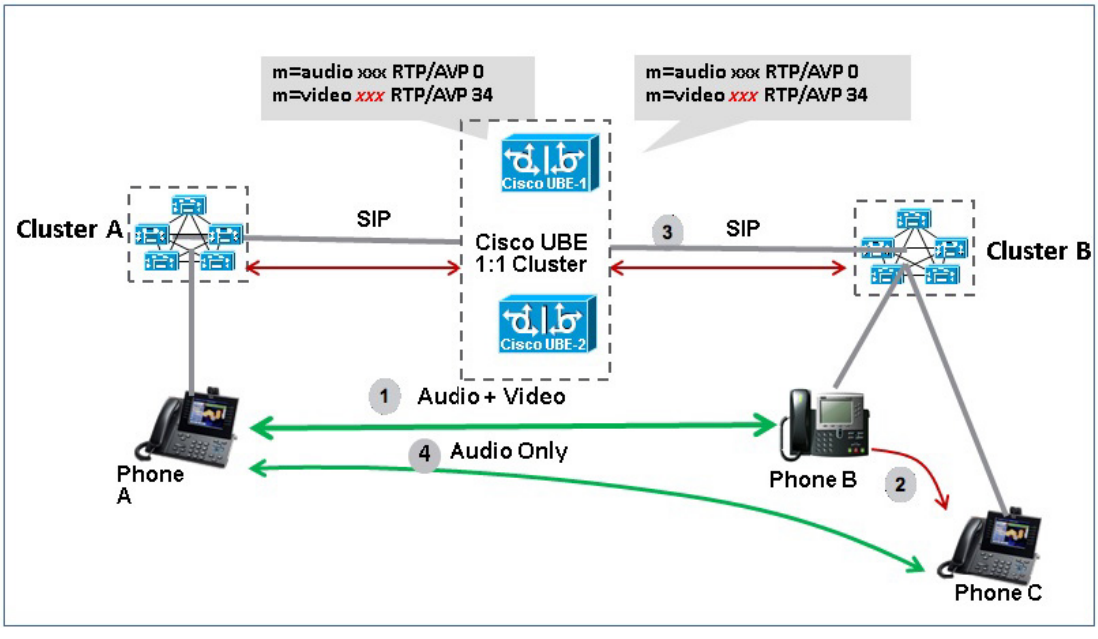
Call De-escalation with Stateful Switchover

The call de-escalation workflow is as follows:

1. The call starts as a video call between Phone A and Phone B registered to two different Cisco Unified Communications Manager (CUCM) clusters connected using Cisco Unified Border Element (Cisco UBE).
2. The call is then transferred to Phone C, which is an audio-only phone.
3. The media parameters within the reinvite are renegotiated end-to-end.
4. The call is de-escalated to an audio-only call.

Note If the Cisco UBE switchover happens at any instance, then video calls will be preserved before de-escalation and audio calls will be preserved after de-escalation.

Figure 2: Call De-escalation



Media Forking with High Availability

Media forking with high availability is supported on ISR G2 and ASR platforms. When a primary call is connected and a forked call-leg is established on an active Cisco UBE device, both the primary and the forked call-leg will be checkpointed in the standby Cisco UBE device. If the active device goes down, the standby device ensures that the forking call is active and is able to exchange further transactions with the recording server with preserved calls such as hold/resume, transfer, conference, and so on. A recording server is a Session Initiation Protocol (SIP) user agent that archives media for extended durations, providing search and retrieval of the archived media. The recording server is a storage place of the recorded session metadata.

The active and standby devices must have the same configurations for checkpointing to happen correctly. The recorder can be configured both ways with a media profile and directly on a media class. The media profile can be associated under media class, and the media class can be applied to the incoming or outgoing dial-peer to start recording.

For more information, see the “Network-based Recording Using Cisco UBE” module in the *Cisco Unified Border Element Protocol-Independent Features and Setup Configuration Guide*.

High Availability Protected Mode and Box-to-Box Redundancy for ASR

To configure box-to-box high availability (HA) support for ASRs, use the **mode rpr** command (rpr is route processor redundancy) in **redundancy** configuration mode.

Note

- Use the same hardware for both the ASR boxes in the active or standby pair to ensure compatibility before and after failover.
- A separate physical interface must be used for checkpointing calls between the active and standby devices.

Self-reload in a voice HA-enabled device helps to recover the box-to-box HA pair from out-of-sync conditions. Instead of self-reload, you can configure the device to transition into protected mode. In protected mode:

- Bulk sync request, call checkpointing, and incoming call processing are disabled.
- The device in protected mode needs to be manually reloaded to come out of this state.

To enabled the protected mode, use the **no redundancy-reload** command under "voice service voip" configuration mode. The default is **redundancy-reload**, which reloads control when the redundancy group (RG) fails.

Monitoring Call Escalation and De-escalation with Stateful Switchover

Perform this task to monitor calls before and after escalation or de-escalation and before and after stateful switchover on active and standby Cisco UBE devices. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show call active voice compact**
3. **show call active video compact**
4. **show call active voice stats**
5. **show call active video stats**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

Example:
```
Device> enable
```

Step 2 **show call active voice compact**
Displays a compact version of call information for the voice calls in progress.

Example:

```
Device# show call active voice compact

<callID>  A/O FAX T<sec> Codec       type        Peer Address       IP R<ip>:<udp>
Total call-legs: 2
       512 ANS     T1     g711ulaw    VOIP        Psipp       9.45.38.39:6016
       513 ORG     T1     g711ulaw    VOIP        P123    10.104.46.222:6000
```

Step 3 **show call active video compact**

Displays a compact version of call information for the video calls in progress.

Example:

```
Device# show call active video compact

<callID>  A/O FAX T<sec> Codec       type        Peer Address       IP R<ip>:<udp>
Total call-legs: 2
       512 ANS     T19    H263        VOIP-VIDEO  Psipp       9.45.38.39:1699
       513 ORG     T19    H263        VOIP-VIDEO  P123    10.104.46.222:1697
```

Step 4 **show call active voice stats**

Displays information about digital signal processing (DSP) voice quality metrics.

Example:

```
Device# show call active voice stats

dur 00:00:16 tx:2238/85044 rx:1618/61484 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 9.45.25.33:58300 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: No
dur 00:00:16 tx:1618/61484 rx:2238/85044 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 9.45.25.33:58400 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: No
```

Step 5 **show call active video stats**

Displays information about digital signal processing (DSP) video quality metrics.

Example:

```
Device# show call active video stats

dur 00:00:00 tx:27352/1039376 rx:36487/1386506 dscp:0 media:0 audio tos:0xB8 video tos:0x88
IP 9.45.25.33:1697 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms H264 TextRelay: off Transcoded:
 No
dur 00:00:00 tx:36487/1386506 rx:27352/1039376 dscp:0 media:0 audio tos:0xB8 video tos:0x88
IP 9.45.25.33:1699 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms H264 TextRelay: off Transcoded:
 No
```

Monitoring Media Forking with High Availability

Perform this task to monitor media forking calls with high availability on active and standby Cisco UBE devices. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show call active voice compact**
3. **show voip rtp connections**
4. **show voip recmsp session**
5. **show voip rtp forking**
6. **show voip rtp forking**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

Example:
```
Device> enable
```

Step 2 **show call active voice compact**
Displays a compact version of call information for the voice calls in progress. In the output shown, the first and second connections are for the basic call and the third connection is for the forked leg.

Example:
```
Device# show call active voice compact

 <callID>  A/O FAX T<sec> Codec       type        Peer Address       IP R<ip>:<udp>
Total call-legs: 3
      4423 ANS     T28    g711ulaw    VOIP        P9538390040    173.39.67.102:22792
      4424 ORG     T28    g711ulaw    VOIP        P708090      9.42.30.189:26300
      4426 ORG     T27    g711ulaw    VOIP        P9876    10.104.46.201:56356
```

Step 3 **show voip rtp connections**
Displays real-time transport protocol (RTP) named event packets. In the output shown, two additional call legs are shown on the Cisco UBE device. Both the active and standby devices will have the same number of connections.

Example:
```
Device# show voip rtp connections

VoIP RTP active connections :
No. CallId     dstCallId  LocalRTP RmtRTP   LocalIP                 RemoteIP
1     4439       4440       16646    19022  10.104.46.251           173.39.67.102
2     4440       4439       16648    22950  9.42.30.213             9.42.30.189
3     4442       4441       16650    36840  10.104.46.251           10.104.46.201
4     4443       4441       16652    54754  10.104.46.251           10.104.46.201
Found 4 active RTP connections
```

Step 4 **show voip recmsp session**
Displays active recording Media Service Provider (MSP) session information. In the output shown, the fork leg details and the number of forking calls are displayed. Both the active and standby devices will have the same call information.

Example:

```
Device# show voip recmsp session

RECMSP active sessions:
MSP Call-ID              AnchorLeg Call-ID        ForkedLeg Call-ID
4441                     4440                     4442
Found 1 active sessions
```

Step 5 **show voip rtp forking**

Displays the RTP media-forking connections. In the output shown, on the active device, packets will be sent.

Example:

```
Device# show voip rtp forking

VoIP RTP active forks :
 Fork 1
   stream type voice-only (0): count 0
   stream type voice+dtmf (1): count 0
   stream type dtmf-only (2): count 0
   stream type voice-nearend (3): count 1
     remote ip 10.104.46.201,  remote port 36840,  local port 16650
       codec g711ulaw,  logical ssrc 0x53
       packets sent 30788,  packets received 0
   stream type voice+dtmf-nearend (4): count 0
   stream type voice-farend (5): count 1
     remote ip 10.104.46.201,  remote port 54754,  local port 16652
       codec g711ulaw,  logical ssrc 0x55
       packets sent 30663,  packets received 0
   stream type voice+dtmf-farend (6): count 0
   stream type video (7): count 0
   stream type application (8): count 0
```

Step 6 **show voip rtp forking**

Displays the RTP media-forking connections. In the output shown, on the standby device, packets will not be sent. After the switchover happens, packets will be sent from the new active device.

Example:

```
Device# show voip rtp forking

VoIP RTP active forks :
 Fork 1
   stream type voice-only (0): count 0
   stream type voice+dtmf (1): count 0
   stream type dtmf-only (2): count 0
   stream type voice-nearend (3): count 1
     remote ip 10.104.46.201,  remote port 36840,  local port 16650
       codec g711ulaw,  logical ssrc 0x53
       packets sent 0,  packets received 0
   stream type voice+dtmf-nearend (4): count 0
   stream type voice-farend (5): count 1
     remote ip 10.104.46.201,  remote port 54754,  local port 16652
       codec g711ulaw,  logical ssrc 0x55
       packets sent 0,  packets received 0
   stream type voice+dtmf-farend (6): count 0
   stream type video (7): count 0
   stream type application (8): count 0
```

Verifying the High Availability Protected Mode

Perform this task to verify the configuration for high availability protected mode, assuming the local device is ACTIVE and the peer device went into PROTECTED mode.

SUMMARY STEPS

1. **enable**
2. **show voice high-availablity rf-client** (active device)
3. **show voice high-availablity rf-client** (standby device)

DETAILED STEPS

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

Step 2 **show voice high-availablity rf-client** (active device)

Example:

```
Device# show voice high-availablity rf-client

FUNCTIONING RF DOMAIN: 0x2

-----
RF Domain: 0x0
Voice HA Client Name: VOIP RF CLIENT
Voice HA RF Client ID: 1345
Voice HA RF Client SEQ: 128
My current RF state ACTIVE (13)
Peer current RF state DISABLED (1)

Current VOIP HA state [LOCAL / PEER] :
        [(ACTIVE (13) / UNKNOWN (0)]

-----
RF Domain: 0x2 [RG: 1]
Voice HA Client Name: VOIP RG CLIENT
Voice HA RF Client ID: 4054
Voice HA RF Client SEQ: 448
My current RF state ACTIVE (13)
Peer current RF state STANDBY HOT (8)

Current VOIP HA state [LOCAL / PEER] :
        [(ACTIVE (13) / PROTECTED (7)]
```

Step 3 **show voice high-availablity rf-client** (standby device)

Example:

```
Device# show voice high-availablity rf-client

RF Domain: 0x0
```

```
Voice HA Client Name: VOIP RF CLIENT
Voice HA RF Client ID: 1345
Voice HA RF Client SEQ: 128
My current RF state ACTIVE (13)
Peer current RF state DISABLED (1)

Current VOIP HA state [LOCAL / PEER] :
        [(ACTIVE (13) / PROTECTED (0)]

-----
RF Domain: 0x2 [RG: 1]
Voice HA Client Name: VOIP RG CLIENT
Voice HA RF Client ID: 4054
Voice HA RF Client SEQ: 448
My current RF state STANDBY HOT (8)
Peer current RF state ACTIVE (13)

Current VOIP HA state [LOCAL / PEER] :
        [PROTECTED (7) / ACTIVE (13)]
```

Troubleshooting Tips

Use the following commands to troubleshoot call escalation and de-escalation with stateful switchover:

- **debug voip ccapi all**
- **debug voip ccapi service**
- **debug voice high-availability all**
- **debug voip rtp error**
- **debug voip rtp inout**
- **debug voip rtp high-availability**
- **debug voip rtp function**
- **debug ccsip all**

Use the following commands to troubleshoot media forking support on high availability:

- **debug ccsip all**
- **debug voip high-availability all**
- **debug voip ccapi inout**
- **debug voip recmsp all**

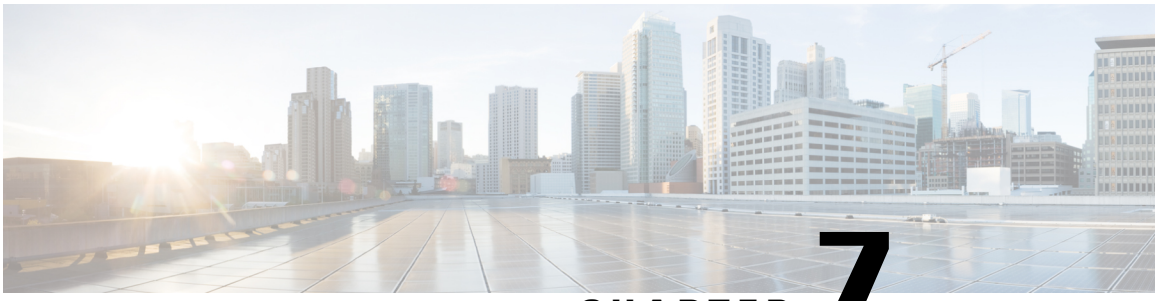
Use the following commands to troubleshoot PROTECTED mode on high availability:

- **debug voice high-availability rf**
- **debug voice high-availability inout**
- **debug redundancy progression**

- **debug redundancy application group faults all**
- **debug redundancy application group protocol all**
- **debug voip ccapi inout**
- **debug cch323 session**
- **debug cch323 function**
- **debug cch323 error**
- **debug ccsip all**

Feature Information for Stateful Switchover Between Redundancy Paired Intra- or Inter-box Devices

Feature Name	Releases	Feature Information
Stateful Switchover Between Redundancy Paired Intra or Inter-box Devices	Cisco IOS XE Release 3.2S	Provides protection for network edge devices with dual Route Processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.
Stateful Switchover Between Redundancy Paired Intra or Inter-box Devices	Cisco IOS Release 15.2(3)T	Provides protection for network edge devices with dual Route Processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.
Stateful Switchover Between Redundancy Paired Intra or Inter-box Devices (Call Escalation and De-escalation with Stateful Switchover)	Cisco IOS XE Release 3.8S 15.3(1)T	Provides support for call escalation and de-escalation with stateful switchover.
Stateful Switchover Between Redundancy Paired Intra or Inter-box Devices (Media Forking with High Availability)	Cisco IOS XE Release 3.8S 15.3(1)T	Provides support for media forking with high availability mechanism.
High Availability Protected Mode and Box-to-Box HA Support	Cisco IOS XE Release 3.11S	Provides support for enabling the PROTECTED mode on a Voice HA-enabled ASR.



CHAPTER 7

SIP-to-SIP Extended Feature Functionality for Session Border Controllers

The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:

- Call Admission Control (based on CPU, memory, and total calls)
- Delayed Media Call
- ENUM support
- Configuring SIP Error Message Pass Through
- Interoperability with Cisco Unified Communications Manager 5.0 and BroadSoft
- Lawful Intercept
- Media Inactivity
- Modem Passthrough over VoIP, on page 56
- TCP and UDP interworking
- Tcl scripts with SIP NOTIFY VoiceXML with SIP-to-SIP
- Transport Layer Security (TLS)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for SIP-to-SIP Extended Feature Functionality for Session Border Controllers

Cisco Unified Border Element

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Modem Passthrough over VoIP

The Modem Passthrough over VoIP feature provides the transport of modem signals through a packet network by using pulse code modulation (PCM) encoded packets.

Prerequisites for the Modem Passthrough over VoIP Feature

- VoIP enabled network.
- Cisco IOS Release 12.1(3)T must run on the gateways for the Modem Passthrough over VoIP feature to work.
- Network suitability to pass modem traffic. The key attributes are packet loss, delay, and jitter. These characteristics of the network can be determined by using the Cisco IOS feature Service Assurance Agent.

Cisco Unified Border Element

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.3S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for the Modem Passthrough over VoIP Feature

Cisco Unified Border Element (Enterprise)

- If call started as g729, upon modem tone (2100Hz) detection both the outgoing gateway (OGW) and the trunking gateway (TGW) will genearate NSE packets towards peer side and up speed to g711 as Cisco UBE(Enterprise) passes these packets to the peer side.

Note That OGW and TGW display the new codec, but the Cisco UBE (Enterprise) continues to show the original codec g729 in the show commands.

Information about Configuring Modem Passthrough over VoIP

The Modem Passthrough over VoIP feature performs the following functions:

- Represses processing functions like compression, echo cancellation, high-pass filter, and voice activity detection (VAD).
- Issues redundant packets to protect against random packet drops.
- Provides static jitter buffers of 200 milliseconds to protect against clock skew.
- Discriminates modem signals from voice and fax signals, indicating the detection of the modem signal across the connection, and placing the connection in a state that transports the signal across the network with the least amount of distortion.
- Reliably maintains a modem connection across the packet network for a long duration under *normal* network conditions.

For further details, the functions of the Modem Passthrough over VoIP feature are described in the following sections.

Modem Tone Detection

The gateway is able to detect modems at speeds up to V.90.

Passthrough Switchover

When the gateway detects a data modem, both the originating gateway and the terminating gateway roll over to G.711. The roll over to G.711 disables the high-pass filter, disables echo cancellation, and disables VAD. At the end of the modem call, the voice ports revert to the prior configuration and the digital signal processor (DSP) goes back to the state before switchover. You can configure the codec by selecting the **g711alaw** or **g711ulaw** option of the **codec** command.

See also the How to Configure Modem Passthrough over VoIP, on page 58 section in this document.

Controlled Redundancy

You can enable payload redundancy so that the Modem Passthrough over VoIP switchover causes the gateway to emit redundant packets.

Packet Size

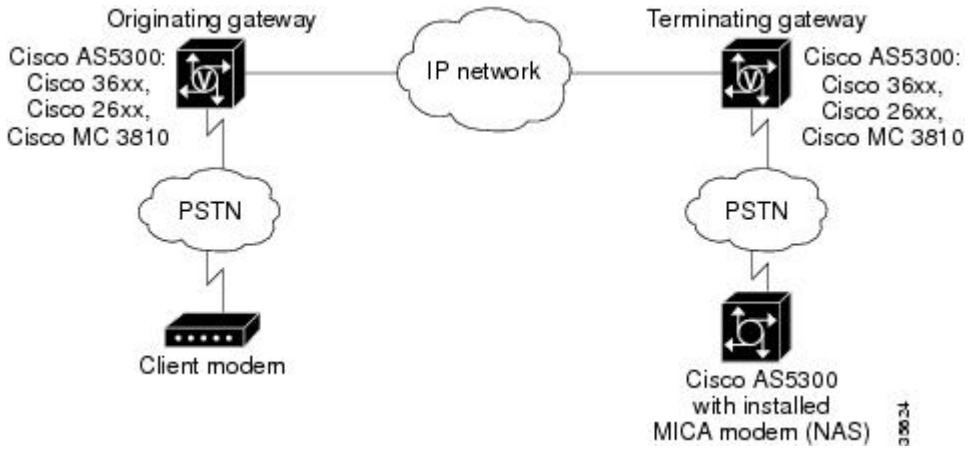
When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

Clock Slip Buffer Management

When the gateway detects a data modem, both the originating gateway and the terminating gateway switch from dynamic jitter buffers to static jitter buffers of 200-ms depth. The switch from dynamic to static is to compensate for Public Switched Telephone Network (PSTN) clocking differences at the originating gateway and the terminating gateway. At the conclusion of the modem call, the voice ports revert to dynamic jitter buffers.

The figure below illustrates the connection from the client modem to a MICA technologies modem network access server (NAS).

Figure 3: Modem Passthrough Connection



How to Configure Modem Passthrough over VoIP

You can configure the Modem Passthrough over VoIP feature on a specific dial peer in two ways, as follows:

- Globally in the voice-service configuration mode
- Individually in the dial-peer configuration mode on a specific dial peer

By default, modem passthrough over VoIP capability and redundancy are disabled.

Tip You need to configure modem passthrough in both the originating gateway and the terminating gateway for the Modem Passthrough over VoIP feature to operate. If you configure only one of the gateways in a pair, the modem call will not connect successfully.

Redundancy can be enabled in one or both of the gateways. When only a single gateway is configured for redundancy, the other gateway receives the packets correctly, but does not produce redundant packets.

See the following sections for the Modem Passthrough over VoIP feature. The two configuration tasks can configure separately or together. If both are configured, the dial-peer configuration takes precedence over the global configuration. Consequently, a call matching a particular dial-peer will first try to apply the modem passthrough configuration on the dial-peer. Then, if a specific dial-peer is not configured, the router will use the global configuration:

Configuring Modem Passthrough over VoIP Globally

For the Modem Passthrough over VoIP feature to operate, you need to configure modem passthrough in both the originating gateway and the terminating gateway so that the modem call matches a voip dial-peer on the gateway.

The default behavior for the voice-service configuration mode is **no modem passthrough**. This default behavior implies that modem passthrough is disabled for all dial peers on the gateway by default.

When using the **voice service voip** and **modem passthrough nse** commands on a terminating gateway to globally set up fax or modem passthrough with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match.

To configure the Modem Passthrough over VoIP feature for all the connections of a gateway, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **voice service voip**
3. **modem passthrough nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**] [**maximum-sessions** *value*]
4. **exit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice-service configuration mode. Configures voice service for all the connections for the gateways.

Step 3	**modem passthrough nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**] [**maximum-sessions** *value*]
	
	Example:
	
	`Device(config)#`
	`Router(conf-voi-serv)# modem passthrough nse payload-type 97 codec g711alaw redundancy maximum-sessions 3`
		Configures the Modem Passthrough over VoIP feature The default behavior is **no modem passthrough**.
		
		The payload type is an optional parameter for the **nse** keyword. Use the same **payload-type** *number* for both the originating gateway and the terminating gateway. The **payload-type** *number*can be set from 96 to 119. If you do not specify the **payload-type** *number*, the *number*defaults to 100. When the **payload-type** is 100, and you use the **show running-config**command, the **payload-type** parameter does not appear.
		
		Use the same codec type for both the originating gateway and the terminating gateway. **g711ulaw** codec is required for T1, and **g711alaw** codec is required for E1.
		
		The **redundancy** keyword is an optional parameter for sending redundant packets for modem traffic.
		
		The **maximum-sessions** keyword is an optional parameter for the **redundancy**keyword. This parameter determines the maximum simultaneous modem passthrough sessions with **redundancy**.

Step 4	**exit** **Example:** `Device(conf-voi-serv)# exit`	Exits voice-service configuration mode.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuring Modem Passthrough over VoIP for a Specific Dial Peer

To enable Modem Passthrough on the VoIP dial peers on both the originating and terminating gateway, configure modem passthrough globally or explicitly on the dial peer.

For modem passthrough to operate, you must define VoIP dial peers on both gateways to match the call, for example, by using a destination pattern or an incoming called number. The modem passthrough parameters associated with those dial peers then will apply to the call.

Note When modem passthrough is configured individually for a specific dial peer, that configuration for the specific dial peer takes precedence over the global configuration.

To configure the Modem Passthrough over VoIP feature for a specific dial peer, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **dial-peer voice** *number* **voip**
3. **modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**}[**redundancy**]}
4. **exit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**dial-peer voice** *number* **voip** **Example:** `Device(config)# dial-peer voice 5 voip`	Enters dial-peer configuration mode. Configures a specific dial peer in dial-peer configuration mode.
Step 3	**modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**}[**redundancy**]} **Example:** `Device(config-dial-peer)# modem passthrough nse payload-type 97 codec g711alaw redundancy`	Configures the Modem Passthrough over VoIP feature for a specific dial peer. The default behavior for the Modem Passthrough for VoIP feature in dial-peer configuration mode is **modem passthrough system**. As required, the gateway defaults to **no modem passthrough**. When the **system** keyword is enabled, the following parameters are not available: **nse**, **payload-type**, **codec**, and **redundancy**. Instead the values from the global configuration are used. The payload type is an optional parameter for the **nse** keyword. Use the same **payload-type** *number* for both the originating gateway and the terminating gateway. The **payload-type** *number*can be set from 96 to 119. If you do not specify the **payload-type** *number*, the *number*defaults to 100. When the **payload-type** is 100, and you use the **show running-config**command, the **payload-type** parameter does not appear. Use the same codec type for both the originating gateway and the terminating gateway. **g711ulaw** codec is required for T1, and **g711alaw** codec is required for E1.

	Command or Action	Purpose
		The **redundancy** keyword is an optional parameter for sending redundant packets for modem traffic.
Step 4	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits dial-peer configuration mode and returns to the global configuration mode.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Troubleshooting Tips

To troubleshoot the Modem Passthrough over VoIP feature, perform the following steps:

- Make sure that you can make a voice call.
- Make sure that Modem Passthrough over VoIP is configured on both the originating gateway and the terminating gateway.
- Make sure that both the originating gateway and the terminating gateway have the same named signaling event (NSE) **payload-type** *number*.
- Make sure that both the originating gateway and the terminating gateway have the same **maximum-sessions** *value* when the two gateways are configured in the voice-service configuration mode.
- Use the **debug vtsp dsp** and **debug vtsp session** commands to debug a problem.

Verifying Modem Passthrough over VoIP

To verify that the Modem Passthrough over VoIP feature is enabled, perform the following steps:

SUMMARY STEPS

1. Enter the **show run** command to verify the configuration.
2. Enter the **show dial-peer voice** command to verify that Modem Passthrough over VoIP is enabled.

DETAILED STEPS

Step 1 Enter the **show run** command to verify the configuration.

Step 2 Enter the **show dial-peer voice** command to verify that Modem Passthrough over VoIP is enabled.

Monitoring and Maintaining Modem Passthrough over VoIP

To monitor and maintain the Modem Passthrough over VoIP feature, use the following commands in privileged EXEC mode:

Command	Purpose
`Device# show call active voice brief`	Displays information for the active call table or displays the voice call history table. The brief option displays a truncated version of either option.
`Device# show dial-peer voice 15 summary`	Displays configuration information for dial peers. The *number* argument specifies a specific dial peer from 1 to 32767. The summary option displays a summary of all dial peers.

Configuration Examples

The following is sample configuration for the Modem Passthrough over VoIP feature:

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
voice service voip
  modem passthrough nse codec g711ulaw redundancy maximum-session 5
!
!
resource-pool disable
!
!
!
!
!
ip subnet-zero
ip ftp source-interface Ethernet0
ip ftp username lab
ip ftp password lab
no ip domain-lookup
!
isdn switch-type primary-5ess
cns event-service server
!
!
!
!
```

```
!
mta receive maximum-recipients 0
!
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 shutdown
 clock source line secondary 1
!
controller T1 2
 shutdown
!
controller T1 3
 shutdown
!
!
!
interface Ethernet0
 ip address 1.1.2.2 255.0.0.0
 no ip route-cache
 no ip mroute-cache
!
interface Serial0:23
 no ip address
 encapsulation ppp
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no peer default ip address
 no fair-queue
 no cdp enable
 no ppp lcp fast-start
!
interface FastEthernet0
 ip address 26.0.0.1 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 duplex full
 speed auto
 no cdp enable
!
ip classless
ip route 17.18.0.0 255.255.0.0 1.1.1.1
no ip http server
!
!
!
!
voice-port 0:D
!
dial-peer voice 1 pots
 incoming called-number 55511..
 destination-pattern 020..
 direct-inward-dial
 port 0:D
 prefix 020
!
dial-peer voice 2 voip
 incoming called-number 020..
 destination-pattern 55511..
 modem passthrough nse codec g711ulaw redundancy
 session target ipv4:26.0.0.2
!
!
line con 0
 exec-timeout 0 0
```

```
 transport input none
line aux 0
line vty 0 4
 login
!
!
end
```

Feature Information for SIP-to-SIP Extended Feature Functionality for Session Border Controllers

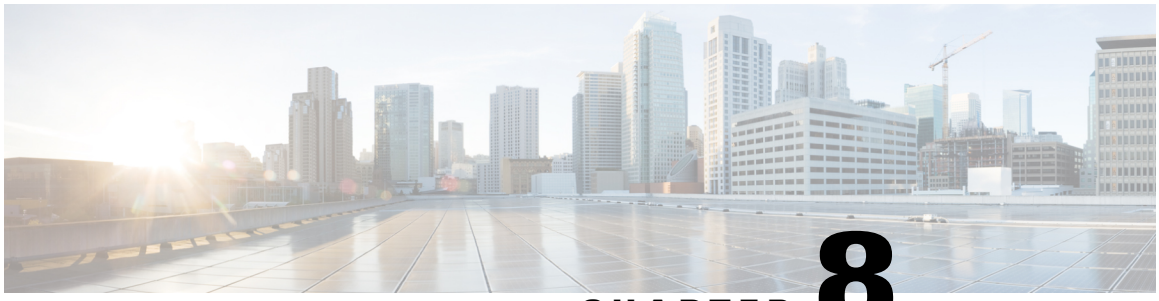
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6: Feature Information for Configuring SIP-to-SIP Extended Feature Functionality for Session Border Controllers

Feature Name	Releases	Feature Information
SIP-to-SIP Extended Feature Functionality for Session Border Controllers	12.4(6)T	The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). In Cisco IOS Release 12.4(6)S, this feature was implemented on the Cisco Unified Border Element The following commands were introduced or modified: **modem passthrough (dial-peer)**; **modem passthrough (voice-service)**; **show call active voice voice**; **show call history voice voice**; **show dial-peer voice**; **voice service**.

Feature Name	Releases	Feature Information
SIP-to-SIP Extended Feature Functionality for Session Border Controllers	Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.3S	The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). In Cisco IOS Release 12.4(6)S, this feature was implemented on the Cisco Unified Border Element (Enterprise). The following commands were introduced or modified: **modem passthrough (dial-peer)**; **modem passthrough (voice-service)**; **show call active voice voice**; **show call history voice voice**; **show dial-peer voice**; **voice service**.



CHAPTER 8

Clearable SIP-UA Statistics

This feature introduces the CISCO-SIP-UA-MIB. The MIB is available by default.

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

http://www.cisco.com/go/mibs

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Clearable SIP-UA Statistics

Cisco Unified Border Element

- Cisco IOS Release 12.3(2)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

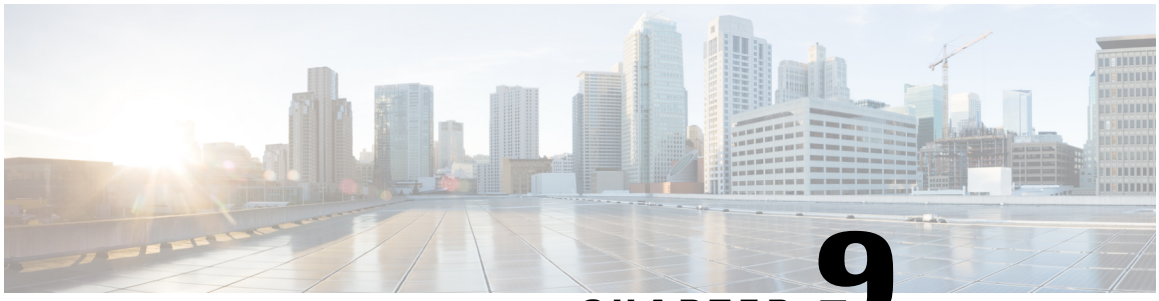
- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Feature Information for Clearable SIP-UA Statistics

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Name	Releases	Feature Information
Clearable SIP-UA Statistics	12.2(13)T 12.2(15)T 12.3(2)T	The Clearable SIP-US Statistics feature adds MIB support. In Cisco IOS Release 12.2(13)T, this feature was implemented on the Cisco Unified Border Element No commands or configurations were introduced or modified in this release.
Clearable SIP-UA Statistics	Cisco IOS XE Release 2.5	The Clearable SIP-US Statistics feature adds MIB support. In Cisco IOS XE Release 2.5, this feature was implemented on the Cisco Unified Border Element (Enterprise) No commands or configurations were introduced or modified in this release.



CHAPTER 9

Additional References

The following sections provide references related to the Cisco Unified Border Element (Enterprise) Configuration Guide.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS Voice commands	*Cisco IOS Voice Command Reference*
Cisco IOS Voice Configuration Library	For more information about Cisco IOS voice features, including feature documents, and troubleshooting information--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm
Cisco IOS Release 15.0	Cisco IOS Release 15.0 Configuration Guides
Cisco IOS Release 12.2	Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2

Related Topic	Document Title
internet Low Bitrate Codec (iLBC) Documents	• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide http://www.cisco.com/en/US/docs/ios-xml/ios/voice/dialpeer/configuration/15-mt/vd-dp-overview.html • Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide http://www.cisco.com/en/US/docs/ios-xml/ios/voice/dialpeer/configuration/15-mt/vd-dp-feat-cfg.html
Related Application Guides	• *Cisco Unified Communications Manager and Cisco IOS Interoperability Guide* • *Cisco IOS SIP Configuration Guide* • Cisco Unified Communications Manager (CallManager) Programming Guides
Troubleshooting and Debugging guides	• Cisco IOS Debug Command Reference, Release 12.4. • *Troubleshooting and Debugging VoIP Call Basics* at http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml • *VoIP Debug Commands* at http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html

Standards

Standard	Title
ITU-T G.711	--

MIBs

MIB	MIBs Link
• CISCO-PROCESS MIB • CISCO-MEMORY-POOL-MIB • CISCO-SIP-UA-MIB • DIAL-CONTROL-MIB • CISCO-VOICE-DIAL-CONTROL-MIB • CISCO-DSP-MGMT-MIB • IF-MIB • IP-TAP-MIB • TAP2-MIB • USER-CONNECTION-TAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

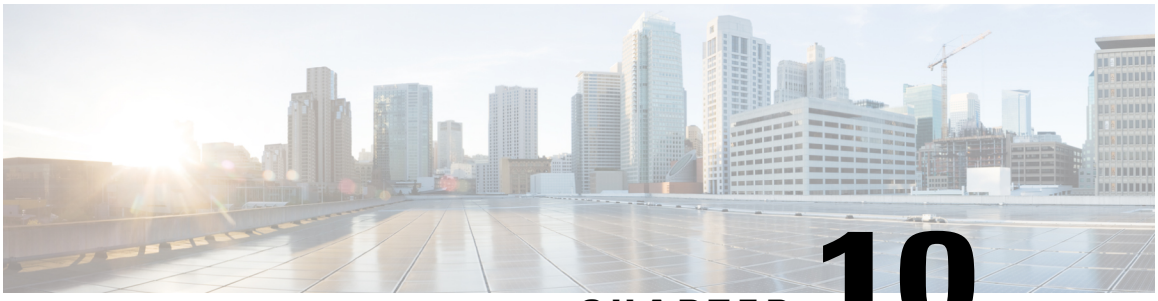
RFCs

RFC	Title
RFC 1889	*RTP: A Transport Protocol for Real-Time Applications*
RFC 2131	*Dynamic Host Configuration Protocol*
RFC 2132	*DHCP Options and BOOTP Vendor Extensions*
RFC 2198	*RTP Payload for Redundant Audio Data*
RFC 2327	*SDP: Session Description Protocol*
RFC 2543	*SIP: Session Initiation Protocol*
RFC 2543-bis-04	*SIP: Session Initiation Protocol, draft-ietf-sip-rfc2543bis-04.txt*
RFC 2782	*A DNS RR for Specifying the Location of Services (DNS SRV)*
RFC 2833	*RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*

RFC	Title
RFC 3203	*DHCP reconfigure extension*
RFC 3261	*SIP: Session Initiation Protocol*
RFC 3262	*Reliability of Provisional Responses in Session Initiation Protocol (SIP)*
RFC 3323	*A Privacy Mechanism for the Session Initiation Protocol (SIP)*
RFC 3325	*Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*
RFC 3515	*The Session Initiation Protocol (SIP) Refer Method*
RFC 3361	*Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers*
RFC 3455	*Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)*
RFC 3608	*Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration*
RFC 3711	*The Secure Real-time Transport Protocol (SRTP)*
RFC 3925	Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 10

Glossary

Glossary

AMR-NB —Adaptive Multi Rate codec - Narrow Band.

Allow header —Lists the set of methods supported by the UA generating the message.

bind — In SIP, configuring the source address for signaling and media packets to the IP address of a specific interface.

call —In SIP, a call consists of all participants in a conference invited by a common source. A SIP call is identified by a globally unique call identifier. A point-to-point IP telephony conversation maps into a single SIP call.

call leg —A logical connection between the router and another endpoint.

CLI —command-line interface.

Content-Type header —Specifies the media type of the message body.

CSeq header —Serves as a way to identify and order transactions. It consists of a sequence number and a method. It uniquely identifies transactions and differentiates between new requests and request retransmissions.

delta —An incremental value. In this case, the delta is the difference between the current time and the time when the response occurred.

dial peer —An addressable call endpoint.

DNS -—Domain Name System. Used to translate H.323 IDs, URLs, or e-mail IDs to IP addresses. DNS is also used to assist in locating remote gatekeepers and to reverse-map raw IP addresses to host names of administrative domains.

DNS SRV —Domain Name System Server. Used to locate servers for a given service.

DSP —Digital Signal Processor.

DTMF —dual-tone multifrequency. Use of two simultaneous voice-band tones for dialing (such as touch-tone).

EFXS —IP phone virtual voice ports.

FQDN —fully qualified domain name. Complete domain name including the host portion; for example, *serverA.companyA.com* .

FXS —analog telephone voice ports.

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

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

iLBC —internet Low Bitrate Codec.

INVITE**—**A SIP message that initiates a SIP session. It indicates that a user is invited to participate, provides a session description, indicates the type of media, and provides insight regarding the capabilities of the called and calling parties.

IP**—**Internet Protocol. A connectionless protocol that operates at the network layer (Layer 3) of the OSI model. IP provides features for addressing, type-of-service specification, fragmentation and reassemble, and security. Defined in RFC 791. This protocol works with TCP and is usually identified as TCP/IP. See TCP/IP.

ISDN —Integrated Services Digital Network.

Minimum Timer —Configured minimum value for session interval accepted by SIP elements (proxy, UAC, UAS). This value helps minimize the processing load from numerous INVITE requests.

Min-SE —Minimum Session Expiration. The minimum value for session expiration.

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

originator —User agent that initiates the transfer or Refer request with the recipient.

PDU —protocol data units. Used by bridges to transfer connectivity information.

PER —Packed Encoding Rule.

proxy —A SIP UAC or UAS that forwards requests and responses on behalf of another SIP UAC or UAS.

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

recipient —User agent that receives the Refer request from the originator and is transferred to the final recipient.

redirect server —A server that accepts a SIP request, maps the address into zero or more new addresses, and returns these addresses to the client. It does not initiate its own SIP request or accept calls.

re-INVITE —An INVITE request sent during an active call leg.

Request URI —Request Uniform Resource Identifier. It can be a SIP or general URL and indicates the user or service to which the request is being addressed.

RFC —Request For Comments.

RTP —Real-Time Transport Protocol (RFC 1889)

SCCP —Skinny Client Control Protocol.

SDP**—**Session Description Protocol. Messages containing capabilities information that are exchanged between gateways.

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

session expiration —The time at which an element considers the call timed out if no successful INVITE transaction occurs first.

session interval —The largest amount of time that can occur between INVITE requests in a call before a call is timed out. The session interval is conveyed in the Session-Expires header. The UAS obtains this value from the Session-Expires header of a 2*xx* INVITE response that it sends. Proxies and UACs determine this value from the Session-Expires header in a 2*xx* INVITE response they receive.

SIP —Session Initiation Protocol. An application-layer protocol originally developed by the Multiparty Multimedia Session Control (MMUSIC) working group of the Internet Engineering Task Force (IETF). Their goal was to equip platforms to signal the setup of voice and multimedia calls over IP networks. SIP features are compliant with IETF RFC 2543, published in March 1999.

SIP URL —Session Initiation Protocol Uniform Resource Locator. Used in SIP messages to indicate the originator, recipient, and destination of the SIP request. Takes the basic form of *user@host* , where *user* is a name or telephone number, and *host* is a domain name or network address.

SPI —service provider interface.

socket listener —Software provided by a socket client to receives datagrams addressed to the socket.

stateful proxy —A proxy in keepalive mode that remembers incoming and outgoing requests.

TCP —Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmissions. TCP is part of the TCP/IP protocol stack. See also TCP/IP and IP.

TDM —time-division multiplexing.

UA —user agent. A combination of UAS and UAC that initiates and receives calls. See **UAS**and **UAC**.

UAC —user agent client. A client application that initiates a SIP request.

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

UDP —User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC-768.

URI —Uniform Resource Identifier. Takes a form similar to an e-mail address. It indicates the user's SIP identity and is used for redirection of SIP messages.

URL —Universal Resource Locator. Standard address of any resource on the Internet that is part of the World Wide Web (WWW).

User Agent —A combination of UAS and UAC that initiates and receives calls. See **UAS and UAC.**

VFC —Voice Feature Card.

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

Glossary